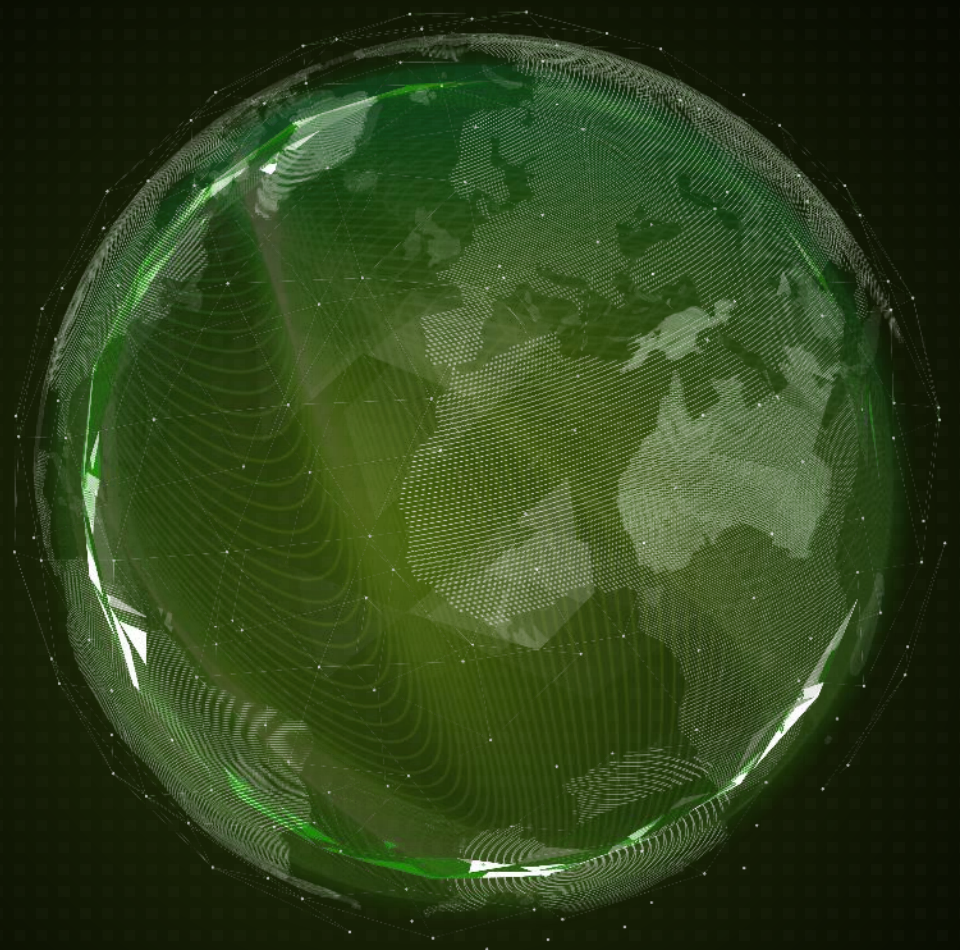
Deloitte.
Legal



Cross-jurisdictional data protection, cybersecurity and AI overview

Recent updates and upcoming developments

December 2025 – Fourth Edition

Index

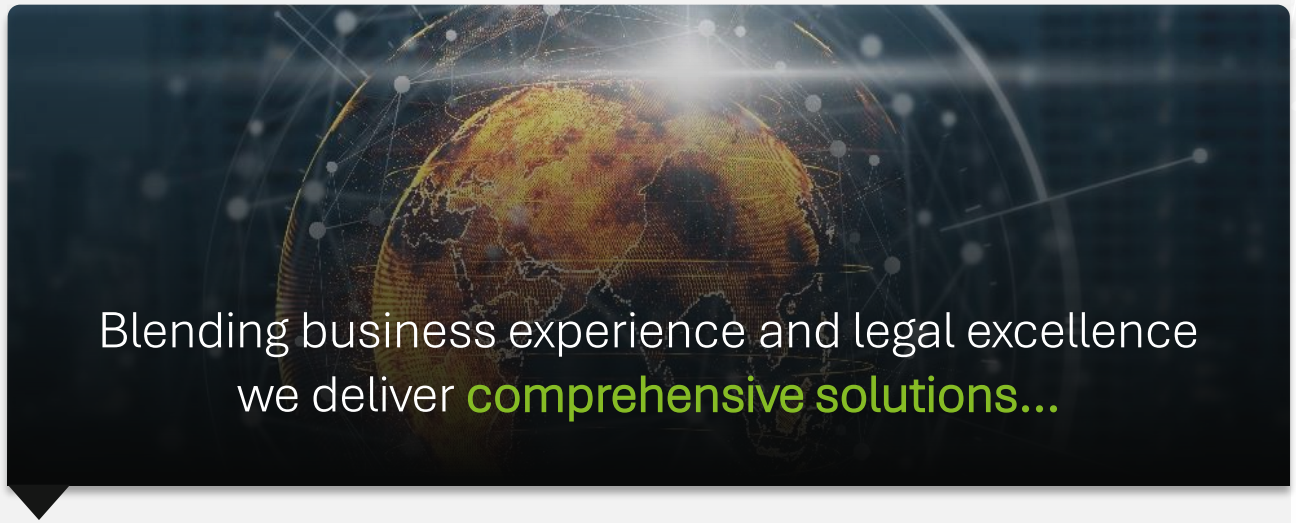
03 Introducing Deloitte Legal
04 Overview
05 National updates and developments

06 European Union
17 Australia
26 Austria
32 Belgium
41 Bulgaria
47 Chile
54 Colombia
59 Costa Rica
64 Croatia
73 Czech Republic
80 Denmark
85 El Salvador
89 France
98 Germany
103 Greece
110 Guatemala
112 Hong Kong
117 Indonesia
123 Italy
131 Ivory Coast
136 Japan
145 Luxembourg
149 Malaysia
160 Malta
168 Mexico
174 Morocco
179 Nigeria
183 Norway
189 Peru
197 Poland
203 Portugal
211 Romania
217 Serbia
222 Singapore
231 Slovenia
239 Spain
249 Sweden
255 Switzerland
265 Taiwan
270 Thailand
273 The Netherlands
280 Turkey
287 Ukraine
292 United Kingdom
300 Contributors

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Introducing Deloitte Legal

Where legal meets business



...designed to address the evolving needs of businesses

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

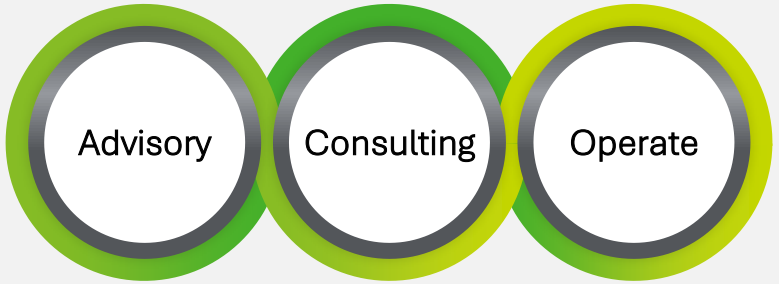
...developed with a business-first approach and methodology

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 Legal 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 *broader*, *global*, *cross-functional*, *industry-informed*, and *technology-enabled*, with a business solution centered approach.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Overview

A complex framework, a cross-jurisdictional approach

In an era where digital transformation accelerates at an unprecedented pace, data remains the fundamental asset driving business innovation and resilience across all sectors and geographies.

As regulatory landscapes around data protection, cybersecurity, and artificial intelligence continue to evolve rapidly, organizations face increasing complexity and heightened expectations. Beyond legal compliance, the effective governance, protection, security, and strategic use of data are critical enablers of a competitive advantage.

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

Since its inception in 2022, Deloitte Legal's cross-jurisdictional annual report has provided a detailed overview of global regulatory developments in these critical areas.

The previous year's edition (third edition) is accessible here.

This fourth edition aims to continue to offer once again up-to-date insights into the latest legal changes, enforcement trends, and forward-looking perspectives on data protection, cybersecurity, and AI governance.

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 AI; and
- Emerging trends: Potential upcoming developments in these fields.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

National updates and developments

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

EU framework

(Institutions, Authorities and Courts)

Contacts

Ida Palombella

Equity Partner, Deloitte Legal Italy

ipalombella@deloitte.it

Pietro Boccaccini

Director, Deloitte Legal Italy

pbocaccini@deloitte.it

(*) This section concerning the European Union has been prepared by the Deloitte Legal Italy team.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

European Data Protection Board released 2024 annual report

On 23 April 2025, the European Data Protection Board (EDPB) published its annual report for 2024, outlining the activities carried out and key achievements. The report highlights, among other things, the following:

- The increasing issuance of consistency opinions pursuant to Article 64(2) of the GDPR;
- The definition of the EDPB's strategy for the 2024-2027 period;
- The adoption of guidelines aimed at providing useful support to organizations in achieving and maintaining GDPR compliance, as well as guidance targeted to small businesses identifying key obligations regarding personal data protection;
- Engagement with stakeholders through the launch of public consultations and the organization of events; and
- Active contribution to ensuring consistency in the combined application of the GDPR and new digital legislation acts, including the Digital Markets Act, the Digital Services Act, the AI Act, the Data Governance Act, and the Data Act, also through collaboration with European and international partners such as the AI Office and the High-Level Group on the Digital Markets Act.

European Data Protection Board published guidelines on pseudonymization

On 17 January 2025, the European Data Protection Board (EDPB) published Guidelines 01/2025 on pseudonymization.

The guidelines aim, among other things, to support data controllers in choosing effective techniques for modifying original data, clarify that the use of pseudonymization – understood as the processing of personal data intended to render the data no longer attributable to a specific data subject without the use of additional information (but still considered personal data) – contributes to:

- Reducing risks for data subjects arising from potential unauthorised access to data;
- Meeting GDPR requirements, such as compliance with the data minimization principle, implementing privacy by design and by default principles, and ensuring the security of processing, including in the context of international data transfers; and
- Justifying the use of the legitimate interest as legal basis and demonstrating the compatibility of further purposes with the original one.

The guidelines will probably undergo a review in the upcoming months, following the decision of the Court of Justice of the European Union in the case EDPS vs. SRB (C-413/23 P).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

European Commission issued guidelines to enhance privacy, security, and online protection of minors under Digital Service Act

On 10 October 2025, the European Commission (the Commission) published the Guidelines on measures to ensure a high level of privacy protection pursuant to Article 28(4) of the Digital Services Act (DSA). The guidelines primarily aim to support providers in adopting appropriate and proportionate measures to ensure a high level of protection for minors, particularly to prevent their exposure to content such as the sale of alcohol, pornographic material, and gambling.

According to the Commission, the most reliable age verification measures depend on the specific context and purpose and can be classified as follows:

- Self-declaration, where individuals state their age;
- Age estimation, which involves methods to determine whether the user meets a certain age threshold; and
- Age verification, a system based on physical identifiers or other sources of identification.

In all cases, the adopted method must meet requirements of accuracy, reliability, robustness, and non-discrimination.

The Commission also provides guidance on how to ensure a suitable environment for minors from the moment of account registration, offering advice on online interface design, the actions an account can perform, methods for monitoring various accounts, and content moderation.

General Court dismissed actions against the EU-US Data Privacy Framework

In September 2025, in Case T-553/23, the General Court of the European Union dismissed a case in which the applicant was seeking annulment of the Commission Implementing Decision (EU) 2023/1795 which had designated the United States as a third country that ensures an adequate level of protection of personal data in relation to US organisations included in the 'Data Privacy List.'

Thus, conversely from the two well known cases in which the CJEU had declared the invalidity of the previous EU-US adequacy decisions (Commission Decision 2000/520/EC, "Safe Harbour," and Commission Implementing Decision (EU) 2016/1250, "Privacy Shield"), this time the new framework for the transfer of personal data between the European Union and the United States has held its validity.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Court of Justice judgment redefined the criteria to distinguish between pseudonymized and anonymous data

On 4 September 2025, in the case EDPS vs. SRB (C-413/23 P), the Court of Justice of the European Union (CJEU) ruled on a central issue in data protection: the classification of pseudonymised data as "personal data."

Pseudonymization involves processing personal data in a manner that prevents the data from being attributed to a specific data subject without access to additional information.

According to the principle expressed by the CJEU, whether pseudonymized data is considered personal depends on the entity processing it:

- For the entity that holds the additional information necessary to link the pseudonymized data to the data subject, such data must be considered personal; and
- For the recipient of the data to whom technical and organizational measures (legally available) effectively prevent identification, the data cannot be considered personal.

The CJEU highlighted that, when assessing a person's identifiability, it is necessary to consider "all means" reasonably accessible to the controller for identification. The data recipient lacked the technical means to re-link the pseudonymized data to the data subjects. Therefore, such data should not have been considered personal data.

Interestingly, the CJEU interpreted that such recipient would have to be listed among the recipients provided in the privacy information notice made available to the data subjects.

EU Court of Justice ruled on data controller status without legal personality

With the decision of 27 February 2025 in Case C-638/23, the Court of Justice of the European Union ruled that an entity without legal personality can also be recognized as a data controller.

The case originated from a preliminary ruling request submitted by the Austrian Administrative Court concerning the definition of "data controller" under Article 4(7) of the GDPR. In this regard, the CJEU established that a data controller can be not only a natural or legal person but also a public authority, service, or body, even if such entities do not have legal personality under national law.

Therefore, the court ruled that an entity may be considered a "data controller" even in the absence of legal personality. Furthermore, the court clarified that the controller must always be capable of fulfilling the obligations established by the GDPR, regardless of whether the entity has legal personality or capacity.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

EU Commission issued Implementing Regulation for the application of NIS2 requirements and European Union Agency for Cybersecurity (ENISA) published the Technical Implementation Guidelines

The EU Commission approved the Implementing Regulation (EU) 2024/2690, which lays down rules for the application of EU Directive 2022/2555 (NIS2 Directive) as regards technical and methodological requirements for cybersecurity risk management measures along with additional clarification of the cases in which an incident is considered to be significant with regard to providers of digital infrastructures and ICT service management sectors due to their cross-border nature.

In particular, such requirements apply to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers.

Following such Implementing Regulation, in June 2025 the European Union Agency for Cybersecurity (ENISA) published an operational technical implementation guidance by providing:

- Guidance, that is, indicative and actionable advice on parameters to consider when implementing a requirement;
- Examples of evidence, that is, the types of evidence that a requirement is in place; and
- Mappings from security requirements to industry good practices, European and international standards, and national frameworks.

European Union Agency for Cybersecurity launched new interactive map of national cybersecurity strategies

On 4 June 2025, the European Union Agency for Cybersecurity (ENISA) announced the update of its "interactive map of national cybersecurity strategies."

Specifically, this digital platform provides a detailed overview of the cybersecurity strategies adopted by each EU member state, outlining their strategic objectives, implementation measures, and best practices.

The map thus serves as a useful tool to monitor each EU member state's progress in its national cybersecurity agenda in order to meet new legislative requirements, including the NIS2 Directive.

The platform will continue to be updated in line with the progress made by EU countries.

European Union Agency for Cybersecurity published a guidance document on the skills and roles for the cybersecurity professionals

The European Union Agency for Cybersecurity (ENISA) published a guide on the skills and roles that cybersecurity professionals must possess to meet the requirements of the NIS2 Directive.

This guide, based on the European Cybersecurity Skills Framework (ECSF), links the obligations of the NIS2 Directive to the professional roles defined by the ECSF, aiming to help essential and important entities understand which professional roles and skills are required to fulfil their obligations as well as which step-by-step approach can guide an organization in implementing the necessary organizational, workforce and strategic planning.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

European Union Agency for Cybersecurity published its Threat Landscape 2025

The European Union Agency for Cybersecurity (ENISA) published in October 2025 its "Threat Landscape 2025," which provides an overview of the cyberthreats that affected the European Union during the period from July 2024 to June 2025, analyzing approximately 4,900 previously identified incidents.

The report highlights how the threat landscape is continuously evolving, with an increase in the exploitation of vulnerabilities alongside the growing complexity of tracking the attackers.

Among the main threats detected, phishing remains the most common, accounting for 60% of all attacks. This is followed by the exploitation of vulnerabilities, representing 21.3% of the attacks, which often lead to the introduction of malware into targeted networks.

The report also focuses on the increased use of AI tools to facilitate network attacks, particularly with reference to large language models (LLMs) used to make phishing emails increasingly credible. It is highlighted that 80% of phishing emails identified between September 2024 and February 2025 used AI in some way, for example, in cases of vishing and online scams, through the creation of deepfakes to impersonate "credible" individuals.

An interesting trend is also the use of AI itself as bait, with the proliferation of fraudulent websites presenting themselves as legitimate AI tools.

In the analysis of nearly 4,900 selected incidents, ENISA reported that the most targeted sector was public administration, accounting for 38.2%. This sector is followed by transport (7.5%), infrastructure and digital services (4.8%), finance (4.5%), and manufacturing (2.9%).

The increase in attacks on public administration is attributed to the rise in distributed denial-of-service (DDoS) attacks carried out during hacktivism operations, which mainly affected the public administration sectors in France (27%), Italy (26.3%), and Germany (16.2%), followed by Spain and the Netherlands.

As for cybercrime, although it represents only 13.4% of the total incidents analyzed in the report, cybercrime activities continue to be a prevalent threat against EU organizations, particularly with regard to ransomware (81.1%) and data breaches (15.2%), which have been documented as consequences of ransomware incidents.

CER entities will be identified during 2026: The EU Commission published a communication with guidelines on the resilience of the critical entities under the CER Directive

On 16 January 2023 the Critical Entities Resilience (CER) Directive entered into force. Such directive had to be transposed into national legislation by EU member states by 17 October 2024. Pursuant to the CER Directive, EU member states shall adopt a national strategy for enhancing the resilience of critical entities and carry out a risk assessment by 17 January 2026 and hence, taking into account the outcomes of the risk assessment, EU member states shall identify critical entities by 17 July 2026.

During 2025, the EU Commission issued a communication offering EU member states recommendations and practical guidance to help identify critical entities in key sectors, including energy, transport, drinking and wastewater, food, banking, and digital infrastructure.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The AI Act gradually continues to become applicable

Although the AI Act was adopted on 1 August 2024, some of its obligations already came into effect. From 2 February 2025 chapters in general provisions and prohibited AI practices come into effect.

This obligation prohibits providers and deployers from placing on the market, using, or putting into service AI systems that employ prohibited AI practices. These practices, listed in Article 5 of the AI Act, include, among others, AI systems that:

- Use subliminal or deceptive manipulation techniques and exploit vulnerabilities related to age, disability, etc.;
- Evaluate individuals based on social behavior or personal characteristics (so called social scoring);
- Carry out real-time biometric identification or categorization to deduce sensitive attributes (e.g., political and religious beliefs); and
- Conduct assessments to evaluate the likelihood that an individual may commit a crime based on their traits or personality.

From the 2 of August 2025, further sections became applicable:

- Section on notified authorities and notified bodies in high-risk AI systems chapter;
- Chapter on general-purpose AI (GPAI) models;
- Chapter on governance;
- Chapter on penalties without the fines for GPAI models; and
- Article on confidentiality in the chapter on post-marketing monitoring.

EU Commission published Guidelines on prohibited AI practices

On 4 February 2025, the European Commission approved the Guidelines on prohibited AI practices under the AI Act.

The guidelines aim to ensure a consistent, effective, and uniform application of the AI law across Europe by providing legal explanations and practical examples to help stakeholders understand and comply with the AI regulation requirements.

The guidelines, after listing the areas excluded from the scope of the AI Act, analyze each prohibited AI practice listed in Article 5 of the regulation, highlighting:

- The motivations and purposes (e.g., in the case of manipulative techniques, the rationale behind the prohibition is to protect individuals' autonomy and well-being);
- The definition of key concepts and components of the prohibition (e.g., in the case of manipulation, the system must employ subliminal techniques aimed at materially distorting a person's behavior, and such behavior must be capable of causing significant harm); and
- Any exceptions to the prohibition and interactions with other European Union laws.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

European Commission published Q&A on AI literacy

On 7 May 2025, the European Commission published the Q&A on the AI literacy obligation set out in Article 4 of the AI Act, aiming to clarify its scope and compliance methods.

This obligation requires the adoption of measures to ensure a sufficient level of knowledge, skills, and awareness of AI among all personnel within organisations – entities such as providers or deployers of AI systems – who use, manage, or interact with an AI system.

Compliance with this obligation, which also has been in effect since 2 February 2025, will be supervised by the market surveillance authority. The authority will ensure compliance starting from 2 August 2026, including through the application of sanctions.

In particular, the Q&A:

- Clarifies the minimum content that an AI literacy program should include and the elements to consider (e.g., risks);
- Specifies that the national market surveillance authority is responsible for enforcing Article 4, including imposing sanctions; and
- Suggests specific training initiatives for SMEs, also referring to the literacy practices repository established under the AI Pact, and EU support programmes such as the European Digital Innovation Hubs (EDIH) network.

European Commission released final Code of Conduct for GPAI models

On 10 July 2025, the European Commission presented the final version of the Code of Conduct for general-purpose AI models (GPAI).

The GPAI Code of Practice (the Code) is a voluntary tool, prepared by independent experts in a multi-stakeholder process, designed to help industry comply with the AI Act's obligations for providers of general-purpose AI models.

The EU Commission and the AI Board have confirmed that the code is an adequate voluntary tool designed to help the industry demonstrate compliance with the AI Act. The Code was developed by 13 independent experts with input from over 1,000 stakeholders (providers, SMEs, academics, civil society).

The objective of the Code of Conduct is to ensure safety and transparency in GPAI models placed on the European market.

The Code is structured into three chapters:

- Transparency: The first chapter of the Code provides an easy-to-use "Model Documentation Template" that helps providers fulfil the obligation to document the required information effortlessly.
- Copyright: The second chapter offers GPAI model providers useful guidance to ensure compliance with European copyright law.
- Safety and protection: The third chapter, aimed only at providers of more advanced models, contains a series of best practices for managing so-called "systemic risk."

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

European Commission's guidelines on general-purpose AI models

On 18 July 2025, the European Commission published its guidelines on general-purpose AI models, providing clarifications on the following aspects:

- The definition of "general-purpose AI models";
- The subjects that should be considered "providers" of GPAI models;
- The meaning of a GPAI model being "placed on the market";
- When downstream modifiers become providers of general-purpose AI models;
- Cases of exemption from certain obligations for providers of GPAI models; and
- Enforcement of the obligations for providers of general-purpose AI models.

The EU Commission also clarified that compliance with the AI Act obligations by GPAI models' providers can be demonstrated by voluntarily following a code of good practices recognized as adequate by the AI Office and the European Artificial Intelligence Board.

Failure to voluntarily adhere to one of these codes will impose the responsibility on the provider to demonstrate compliance of the model through alternative means, which must be notified to the AI Office, which may also request additional information and access to the model's documentation.

EDPS published and updated guidance to EU institutions on the processing of personal data when using AI systems

On 28 October 2025, the European Data Protection Supervisor (EDPS) updated its guidance on "Orientations for ensuring data protection compliance when using Generative AI systems" to provide practical advice and instructions to EU institutions, bodies, offices and agencies (EUIs) on the processing of personal data when using generative AI systems, to facilitate their compliance with their data protection obligations as set out, in particular, in Regulation (EU) 2018/1725 (EUDPR).

On 11 November 2025, the EDPS published a Guidance for Risk Management of Artificial Intelligence Systems. The purpose of this guidance is to facilitate a systemic assessment of risks from a data protection perspective when adopting an AI system, providing an analytical framework for identifying and treating risks that may arise in AI systems, structured according to the data protection principles potentially affected. The guidance focuses in particular on two specific aspects of risk management process, namely risk identification and risk treatment, listing specific risk scenarios and suggesting a non-exhaustive list of technical countermeasures to illustrate how risks can be managed in practice.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

"Digital Omnibus" and "Digital Omnibus on AI" proposals

On 19 November 2025, the EU Commission published a proposal for major reforms of the digital acts of the EU, known as the "Digital Omnibus" proposal. The Digital Omnibus proposal is a step to optimize the application of the digital rulebook; it includes a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens, and to stimulate competitiveness. The immediate objective is to reduce compliance costs, adapting the EU's regulatory framework to a more volatile world.

In particular, among the main aspects included in the Digital Omnibus proposal we highlight the following:

- Amendments to the 2023/2854 (Data Act), to consolidate into it the provisions of the Regulation (EU) 2018/1807 (the Free Flow of Data Regulation), Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive); and
- Amendments to the data protection and cybersecurity framework, including Regulation (EU) 2016/679 (GDPR), 2018/1725 (EUDPR) Directive 2002/58 (ePrivacy Directive) and targeted amendments that impact the Directive (EU) 2022/2555 (NIS2 Directive), 2022/2557 (CER Directive), Regulation 2022/2554 (DORA) and Regulation (EU) 910/2014 (eIDAS Regulation).

Furthermore, the EU Commission also published the Digital Omnibus on AI proposal, proposing the amendment of Regulation (EU) 2024/1689 (AI Act) and Regulation (EU) 2018/1139.

The AI Act will gradually continue to become applicable

The general date of application will be the 2 August 2026, which includes the enforcement rules. Without any amendment, the AI Act will be fully applicable by 2027.

"Apply AI Strategy": A roadmap for the future of AI and strengthening Europe's competitiveness

The European Commission has launched the "Apply AI Strategy", designed to promote the practical adoption of AI in key economic sectors and the public sector through targeted funding, thereby enhancing Europe's competitiveness.

The strategy is based on three fundamental pillars:

- The first pillar involves the launch of a series of sector-specific initiatives designed to introduce and promote AI solutions in strategic areas such as healthcare, robotics, manufacturing, defense, energy, agriculture, transport, telecommunications, culture, and public administration.
- The second pillar addresses cross-cutting challenges, as common obstacles that slow down AI adoption, especially for SMEs. It includes strengthening digital skills, professional training and upskilling programs, and creating a clear and reliable regulatory framework through the implementation of the AI Act.
- The third pillar aims to establish a unique governance mechanism that fosters dialogue among the various stakeholders, such as institutions, businesses, and researchers, through a new "ApplyAI Alliance" and a dedicated observatory to monitor AI progress, impacts, and trends. All of this will be coordinated by the European AI Council.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Proposal for the simplification of the GDPR for SMEs and SMCs and other possible proposals to simplify EU data protection laws

The European Commission plans to simplify some EU laws, including the GDPR, in particular for the benefit of small and medium-sized enterprises (SMEs) and small mid-cap enterprises (SMCs). We can expect that a reform of the GDPR could be approved during the next year.

In particular, the EU Commission has issued a proposal – on which the EDPB and EDPS provided a joint opinion – which aims to modify Article 30(5) GDPR, with the aim to expand the derogation to the obligation to keep a record of data processing operations. Specifically, under the proposal, the derogation to the obligation to keep a record of processing operations would apply to an enterprise or organization employing fewer than 750 people, unless the processing operation carried out is likely to result in a high risk to individuals' rights and freedoms, within the meaning of Article 35 GDPR.

Update of the guidelines on pseudonymization

Following the ruling of the European Union Court of Justice in the in the case EDPS vs. SRB (C-413/23 P), we may expect that during 2026 the EDPB may want to update the Guidelines 01/2025 on Pseudonymization.

Proposed regulation to prevent and combat child sexual abuse

During the vote on 14 October 2025, EU member states failed to reach an agreement on "Chat Control," the proposed regulation aimed at preventing and combating child sexual abuse (known as CSAR – Child Sexual Abuse Regulation).

The proposed regulation, introduced in 2022, seeks to protect minors online from serious abuse by mandating messaging and email platforms to scan all messages, images, or videos prior to sending and encryption, in order to detect child sexual abuse material or grooming attempts aimed at minors.

To this end, these platforms would need to implement a proactive scanning system that analyzes all content using an algorithm which, if it detects matches with child sexual abuse material, reports it to the authorities.

The proposal has generated intense debate, with contrasting views among EU member states; on one side, concerns about violations of privacy rights and data protection, with risks of potential "mass surveillance" and, on the other, Chat Control is seen as an essential tool to limit the spread of child sexual abuse material and protect minors.

The EDPB and EDPS had already expressed concerns in 2022 regarding data protection and respect for privacy.

The vote has been postponed to December 2025.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Australia

Contacts

Rachel Sciascia

Partner, Deloitte Legal Australia

rsciascia@deloitte.com.au

Celeste Bennett

Director, Deloitte Legal Australia

cebennett@deloitte.com.au

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Privacy reforms: Raising expectations for data protection and transparency

The Privacy and Other Legislation Amendment Bill 2024 (Cth) (Privacy Bill 2024), reported in the 2024 Cross-jurisdictional report, has been enacted and includes significant changes to the privacy landscape in Australia, raising expectations for data protection and transparency. These reforms include:

- Individuals can now sue for serious privacy breaches directly without proving damage. Previously any privacy breaches required Office of Australian information Commissioner (OAIC) involvement;
- Criminalizing doxing, with offenders facing a maximum of seven years in jail if found guilty;
- Enhancing OAIC enforcement powers including to issue infringement notices and compliance notices. Failing to comply with an infringement or compliance notice could result in a maximum pecuniary penalty of AUD 330,000;
- Clarifying that for organizations subject to the Privacy Act 1988 (Cth) (Privacy Act), taking "technical and organizational measures" are reasonable steps to protect personal information; and
- Allowing for countries with substantially similar privacy protections to Australia to be identified in regulations to make it easier for businesses in Australia to transfer personal information to recipients in those countries. To date, no countries have been designated, however the legislation is only new, and this may change in the future.

Productivity Commission's Interim Report "Harnessing data and digital technology"

The Productivity Commission's Interim Report released in August 2025, considers that individuals and businesses can increase value from products and services by accessing and sharing data. Implementing "new lower-cost and flexible pathways" will let data holder obligations and government functions change according to each sector's "structural characteristics and digital maturity." Data access and sharing pathways can be rolled out among sectors, starting with sectors "where the benefits of sharing data clearly outweigh the costs, and the costs are relatively low."

The pathways could include industry-led data access codes for consumers to periodically export nonsensitive data or standardized data transfers with technical standards for "high-frequency data transfers and interoperability."

While the types of accessible data will vary, the data should be "identified with the consumer or business," held or controlled digitally by the provider, and collected or created through interactions.

However, this type of data access and data use may be burdened by the obligations in the Privacy Act creating an "excessive regulatory burden without improving outcomes for individuals." The Interim Report recommends amending the Privacy Act to include an outcomes-based privacy compliance pathway targeted at outcomes, rather than compliance with "controls-based rules."

Further, the Interim Report recommends against including a "right to erasure" in the Privacy Act due to the "high compliance burden" it would impose on businesses and the "uncertain privacy benefits" it would provide to individuals.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Privacy and the use of biometric information

The Commissioner initiated investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025) examined Kmart Australia Limited's (Kmart) deployment of facial recognition technology in 28 retail stores in Australia over a two-year period. The facial recognition technology was collecting biometric information of every shopper who entered 28 of its retail stores and those shoppers who presented at a product returns counter in that store.

Biometric information falls within the subset of "sensitive information" in the Privacy Act and its collection and use is restricted to individuals who have consented to collection, unless an exemption applies.

Kmart claimed it used the biometric information to detect and prevent fraudulent refunds and "assist in identifying individuals who had previously engaged in refund fraud or theft." Kmart argued consent was not required because of an exemption in the Privacy Act that allows for organizations to collect personal information if they:

- Have "reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in"; and
- "Reasonably" believe "that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter."

The Australian Information Commissioner accepted that refund fraud was unlawful activity relating to Kmart's "functions and activities in respect of the sale of goods and loss prevention." However, the Australian Information Commissioner considered that there was not reasonable belief including because:

- The value of the fraud prevented as a result of the biometric data being collected was minimal compared to Kmart's annual revenue of AUD 9.2 billion;
- Kmart was collecting the biometric data of all customers entering the stores, not just suspected individuals;
- The facial recognition technology appeared to have limited effectiveness in detecting and preventing refund fraud; and
- There were "less privacy intrusive methods" Kmart could have implemented.

While Kmart had an entry notice at the relevant stores noting the use of facial recognition technology in that store, the Privacy Act requires individuals to be notified of the collection of their personal information at or before the time the personal information is collected or if that is not practicable, as soon as practicable after collection. Kmart had a notice at store entries stating "[t]his store has 24-hour CCTV coverage, which includes facial recognition technology" and a privacy poster displayed at the entry points of certain stores directing shoppers to Kmart's privacy policy. However, the entry notice and poster did not:

- Adequately notify or make shoppers aware their personal information was being collected, or the consequences of their personal information not being collected;
- Specify the purpose for collecting personal information was to prevent and detect refund fraud; and
- Specify that its privacy policy contained information about how shoppers could access their personal information and seek corrections.

Further, there were instances of the entry notice not being displayed in stores when the facial recognition technology was in use, and there were no signs at the returns counter.

Kmart's privacy policy also did not reference the use of facial recognition technology to collect personal information and the purpose of this collection, which also breached the requirements in the Privacy Act for having a clear and up to date privacy policy containing the information stipulated by the Privacy Act.

This decision reflects a broader concern about the proportionality of using invasive technologies in retail settings without robust justification or safeguards and underscores the need for organizations to priorities privacy when adopting emerging technologies, particularly those involving sensitive information.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

eSafety Commissioner – Introduction of new industry codes

Australia's eSafety Commissioner has registered the following codes, each one of which is to be read in accordance with the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Term:

- Schedule 1 - Hosting Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 2 - Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 4 - Social Media Services (Core Features) Online Safety Code (Class 1C and Class 2 Material)
- Schedule 4A - Social Media Services (Messaging Features) Online Safety Code (Class 1C and Class 2 Material)
- Schedule 5 - Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 6 - Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 7 - App Distribution Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 8 - Equipment Online Safety Code (Class 1C and Class 2 Material)

The above codes and Head Terms (Codes) aim to restrict children accessing or being exposed to viewing Class 1C and Class 2 material and provide Australian end-users with "information, tools and options to limit access and exposure" to these materials.

Class 1C material includes films, publications, computer games and other material classified as or which would likely be classified as, Refused Classification (RC) and which describes or depicts specific fetish practices or fantasies (excluding child sexual exploitation, pro-terror and extreme crime or violence material). RC material is content outside "generally accepted community standards" and cannot be provided, advertised or legally imported into Australia.

Class 2 material includes films, publications, computer games and other material classified as or which would likely be classified as, X 18+ or R 18+. Content classified as X 18+ is restricted to people 18 years and older and contains "sexually explicit activity." Content classified as R 18+ is restricted to people 18 years and older and contains content "that may be offensive to sections of the adult community."

The Codes identify compliance measures for each industry. For example, the Social Media Services (Core Features) Online Safety Code specifies that a social media service provider must implement access control measures and age assurance measures where feasible and practicable before providing access to online pornography or self-harm material.

Compliance with the Codes requires industry entities "to identify and implement" reasonable compliance measures, taking into account various factors including human rights and the industry participant's risk profile, the product or service, whether the steps are proportionate to the risk and the nature of the material classified as Class 1C or Class 2 material.

These Codes complement the existing codes and standards issued by the eSafety Commissioner for Class 1A material (which includes child sexual exploitation material, pro-terror material advocating for committing terrorist acts, including terrorist manifestos, extreme crime and violence material dealing with extreme crime, cruelty or violence without justification (including sexual violence)) and Class 1B material (which includes unjustified depictions, description, promotion or instructions in crime or violence and unjustified description, promotion, instruction or dealing with drug misuse or addiction).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cyber Security Act – Mandatory cybersecurity standards for consumer IoT devices and ransomware reporting

The Cyber Security Act 2024 (Cth) (Cyber Security Act) institutes:

- Mandatory cybersecurity standards for smart devices, and
- Mandatory ransomware payment reporting for entities.

Cybersecurity standards for smart devices

The Cyber Security Act and the Cyber Security (Security Standards for Smart Devices) Rules 2025 introduce cybersecurity standards for consumer smart devices which are intended for personal use and are not a desktop computer, laptop or tablet computer, smartphone, therapeutic good, road vehicle or road vehicle component. The security standards include requirements regarding passwords, reporting security issues and publishing the period for which security updates will be provided for the product.

Ransome payment reporting

The Cyber Security Act and the Cyber Security (Ransomware Payment Reporting) Rules 2025 implement mandatory ransomware payment reporting obligations where a payment or benefit has been made for an imminent, occurring or occurred cybersecurity incident of:

- An entity carrying on a business in Australia with an annual turnover of AUD 3 million and which is not a Commonwealth or State body; or
- A responsible entity for a critical infrastructure asset to which Part 2B of the Security of Critical Infrastructure Act 2018 (Cth) applies.

A cybersecurity incident is defined in the Cyber Security Act as:

- Involving a critical infrastructure asset;
- Involving activities of a corporation subject to Parliament's corporation powers in the Australian Constitution;
- Effected by a telegraphic, telephonic or similar service subject to Parliament's powers under the Australian Constitution, including the internet;
- Impeding or impairing a computer connecting to such a service; or
- Seriously prejudicing the social or economic stability of Australia or Australians, national security or Australia's defense.

The timeframe for making the report to the Department of Home Affairs and the Australian Signals Directorate is within 72 hours of making the ransomware payment or becoming aware that the ransomware payment has been made.

Reforms to Security of Critical Infrastructure Act

The Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act), which contains obligations for owning, operating or having direct interests in critical infrastructure assets in Australia, has been amended to:

- Expand critical infrastructure assets to include data storage systems storing business-critical data used in relation to a critical infrastructure asset;
- Expand government powers from "serious cybersecurity threats" to "serious incidents" on a critical infrastructure asset;
- Grant the government power to compel an entity to vary its critical infrastructure risk management program to address "serious deficiencies"; and
- Allow the government to compel risk management improvements and consolidate telecommunications security under the SOCI Act.

Businesses operating critical infrastructure must reassess risk programs, data storage compliance, and readiness for expanded government intervention.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Scams Prevention Framework

The Australian government has introduced the Scams Prevention Framework (SPF) establishing a scams prevention regime.

For the purposes of the SPF a scam is a "a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt: (i) involves deception ... and (ii) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF's consumer's associates."

A scam attempt involves deception if the scam:

- "Deceptively represents something to be (or to be related to) the regulated service";
- "Impersonates a regulated entity in connection with the regulated service";
- "Is an attempt to deceive the SPF consumer into: (i) performing an action using the regulated service; or (ii) facilitating another person to perform an action using the regulated service"; or
- "Is an attempt to deceive the SPF consumer that is made using the regulated service."

The SPF protects natural persons and small businesses in Australia and extends beyond Australia to natural persons who ordinarily reside in Australia and entities providing services outside of Australia, but where the entity is an Australian resident or has a permanent establishment for income tax purposes.

Banking services, digital platform services and telecommunication services have been identified as possible regulated sectors.

Regulated sectors will need to comply with the following overarching principles, in addition to any designated codes applying to them:

- Governance: Documenting and implementing governance policies and procedures and performance metrics in relation to scams, maintaining records of this, and annual certifications of compliance;
- Preventing scams: Taking reasonable steps to prevent scams, which requires more than acting on actionable scam intelligence provided by another person;
- Detecting scams: Taking reasonable steps to detect a scam as or after it happens, investigating whether an activity is a scam, taking reasonable steps in a reasonable time to identify consumers who may have been impacted by the activity;
- Reporting scams: Reporting on actionable scam intelligence;
- Disrupting scams: Taking reasonable steps in a reasonable time to disrupt the scam activity or prevent loss or harm; and
- Reporting and dispute mechanisms: Having accessible reporting mechanisms for reporting actual or potential scams and accessible and transparent internal dispute resolution mechanisms for complaints.

Maximum penalties for breaching the SPF are:

- For individuals: AUD 2,636,700; or
- For companies: The maximum of AUD 52,715,850, or three times the value of the benefit obtained or 10% of the turnover during the period in breach.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Productivity Commission's Interim Report "Harnessing data and digital technology" – AI perspective

The Productivity Commission's Interim Report released in August 2025, considers that most of the risks AI pose are not new issues, and therefore "[t]he regulatory response should focus on mitigating the *additional risk* of these harms occurring, rather than treating them as wholly new problems." The Interim Report recommends that:

- The Australian government undertake "gap analyses" to understand AI risks and whether these risk are dealt with by "existing regulatory frameworks," and pause the introduction of AI regulations until this occurs; and
- AI regulations are a last resort where the existing framework is not adaptable and "technology-neutral regulations are not feasible."

The Interim Report noted that there was an option to expand the "fair dealing" regime in copyright to include training for AI models without obtaining consent from the copyright holders. However, the Australian government has "no plans" to introduce this exemption.

New model AI clauses for Australian government contracts

The Australian government published model clauses to assist government buyers procuring AI systems or in circumstances where the seller is using AI systems in the delivery of their services.

These model clauses address a range of AI matters including no use of banned AI systems, notifications of AI hazards and incidents, disengaging the AI system, the AI system operating ethically and complying with a range of legislation and principles and policies and complying with new laws and policies as they are introduced, human oversight of the AI system, steps to be taken regarding AI datasets and compliance with AI risk management systems.

These clauses can be amended to the specific AI requirements the government buyer, and government buyers have been using and enforcing compliance with these clauses.

Copyright and Artificial Intelligence Reference Group (CAIRG) – Responses to transparency discussion paper

In September 2024, the Attorney General's Department circulated the Copyright and AI Reference Group Transparency paper to obtain feedback from CAIRG participants on "copyright-related transparency issues."

The responses received from CAIRG participants advocate for clear disclosure requirements for AI developers and operators to identify when copyright material has been used to develop AI models. The CAIRG participants also support the use of AI tools in the creation of some content being identified. The CAIRG participants also overall supported implementing these requirements in a new piece of legislation, instead of amending the *Copyright Act 1968* (Cth).

While CAIRG participants considered the EU regulatory approach, however:

- Participants from the creative and broadcasting sector generally supported "imposition on general purpose AI (GPAI) providers of copyright-related transparency obligations and the need to comply with EU copyright law, no matter the jurisdiction in which the GPAI model was developed"; and
- Participants from technology and other sectors "urge caution" due to key differences between EU and Australian copyright frameworks, including "that the EU's copyright-AI transparency measures are explicitly tied to compliance with the opt-out condition of its generally-applicable text and data mining exception."

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Australian Senate Select Committee on AI

The Australian Senate Select Committee on Adopting Artificial Intelligence released its final report calling for consultation and new legislation to regulate high-risk AI uses. The final report contains the following recommendations to the Australian government:

- Introduction of a piece of legislation regulating "high-risk uses of AI"
- Adopting a "principles-based approach to defining high-risk AI uses" accompanied "by a non-exhaustive list of explicitly defined high-risk AI uses" which includes "general-purpose AI models";
- Increasing financial and nonfinancial "support of sovereign AI capability in Australia" concentrating on "Australia's existing areas of comparative advantage and unique First Nations perspectives";
- The final definition of high-risk AI includes AI use impacting workers' rights and that existing workplace health safety legislation extends to "workplace risks posed by the adoption of AI";
- Workers, employers and worker and employer organizations are "consulted on the need for, and best approach to, further regulatory responses to address the impact of AI on work and workplaces";
- "Creative workers, rightsholders and their representative organizations" are consulted on "appropriate solutions to the unprecedented theft of their work by multinational tech companies operating within Australia";
- Transparency by AI product developers on the use of copyright materials in their training datasets, and that these materials are "appropriately licensed and paid for";
- Urgent "consultation with the creative industry to consider an appropriate mechanism to ensure fair remuneration is paid to creators for commercial AI-generated outputs based on copyrighted material used to train AI systems";
- Amending legislation to include a "right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made";
- Managing AI infrastructure in Australia using a "a coordinated, holistic approach" for sustainable growth.

Office of Australian Information Commissioner – Guidelines on privacy and AI

In October 2024, OAIC released guidelines to assist organizations to comply with Australian privacy requirements while using commercially available AI products or developing and training Generative AI models.

The guidelines for using AI note:

- Organizations should conduct due diligence on AI systems since privacy requirements apply to personal information entered into the AI system and in the AI system's outputs if they contain personal information;
- Privacy policies will need to be updated to account for the use of AI;
- AI systems generating or inferring personal information must comply with the requirements for collecting personal information;
- Organizations can only input personal information into an AI system if it is for the primary purpose for which it was collected, unless there is consent, or the person providing the personal information would reasonably expect it to be used in this way and this use relates to the primary purpose the information was collected.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Transparency rules for automated decision-making

New transparency rules for automated decision-making (ADM) will take effect on 10 December 2026, requiring entities subject to the Privacy Act to include in their Privacy Policy if:

- The entity is using an ADM system "to make, or do a thing that is substantially and directly related to making, a decision" or refusing or failing to make a decision (noting that a decision can affect an individual beneficially or adversely);
- The decision or refusal or failure to make a decision "could reasonably be expected to significantly affect the rights or interests of an individual"; and
- An individual's personal information is used in the ADM system "to make the decision or do the thing" or refusal or failure to do the thing.

Here, the information includes:

- The types of personal information used by the ADM system;
- The types of decisions the ADM system is solely making; and
- The types of decisions "for which a thing, that is substantially and directly related to making the decision" is completed by the ADM system.

If an entity fails to update its Privacy Policy as required, they could face maximum penalties of:

- For companies: The maximum of AUD 50 million, or three times the value of the benefit obtained or 30% of the turnover during the period in breach; or
- For individuals: A maximum penalty of AUD 2.5 million.

Social media minimum age laws

From December 2025, "age-restricted social media platforms" must take reasonable steps to prevent Australian children under 16 years from having accounts.

An "age-restricted social media platform" is an electronic service:

- With the sole, or significant, purpose of enabling online social interaction between at least two end users. This includes enabling end-users to "share material for social purposes";
- Allowing end-users "to link to, or interact with, some or all of the other end-users"; and
- Allowing "end-users to post material on the service."

Breaching the requirement to restrict access to social media platforms to children under 16 years, could result in maximum penalties of:

- For companies: A maximum of AUD 49.5 million; or
- For individuals: A maximum of AUD 9.9 million.

On 16 September 2025, the eSafety Commissioner published eSafety Social Media Minimum Age Regulatory Guidance to assist age-restricted social media platforms to meet their legislative requirements.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Austria

Contacts

Sascha Jung

Partner, Deloitte Legal - Jank Weiler Operenyi Attorneys at Law

s.jung@jankweiler.at

Christian Kern

Senior Manager, Deloitte Legal - Jank Weiler Operenyi Attorneys at Law

c.kern@jankweiler.at

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Legislation – Farewell to official secrecy

Freedom of Information Act (Informationsfreiheitsgesetz (IFG))

The Austrian Freedom of Information Act (Informationsfreiheitsgesetz (IFG)) came (mostly) into force on 1 September 2025. On this day, official secrecy was replaced by the right of access to information. Additionally, the proactive duty to provide information came into effect.

Administrative, legislative, judicial, and state oversight bodies must, as a matter of principle, proactively publish information of "general interest" that they have created or commissioned on the internet free of charge.

Furthermore, every person has a constitutionally guaranteed right to access information and can request it from certain governmental (administrative bodies of the federal government, states, and municipalities) or quasi-governmental bodies (foundations, funds, institutions, and enterprises subject to the control of the Federal Audit Office (Rechnungshof) or a State Audit Office (Landesrechnungshof)).

If the right to data protection within the meaning of the GDPR is affected, this constitutes "grounds for confidentiality" under the IFG, which may prevent information from being disclosed. The body responsible for providing information must weigh up the interests in each individual case and may only disclose information if the right to provide information prevails.

According to Article 15 paragraph 1 IFG the Austrian Data Protection Authority (DSB) "advises and supports the bodies and institutions subject to information requirements by providing guidelines and training opportunities on data protection issues relating to the enforcement of freedom of information."

New data protection supervisory authority

The Parliamentary Data Protection Committee

The Parliamentary Data Protection Committee was established in 2025 as the supervisory authority which decides on data protection complaints against legislative bodies, including their administrative affairs.

The Parliamentary Data Protection Committee is responsible for the areas of work of the National Council, Federal Council, Court of Auditors, and Ombudsman.

The Parliamentary Data Protection Committee is now one of two supervisory authorities in Austria, alongside the Austrian Data Protection Authority.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Legislation – Access to data

Data Access Act (Datenzugangsgesetz (DZG))

The new Data Access Act (Datenzugangsgesetz (DZG)) came into force on 24 July 2025. The law implements the EU Regulation on Data Governance (EU 2022/868) and makes a significant contribution to the European Data Strategy.

The Data Access Act establishes central structures for data access:

- **Competent authority**: The Federal Chancellery is responsible for supervising new players in the data economy, such as data brokerage services and data altruistic organizations.
- **Central information point**: Together with Statistics Austria and the Federal Computing (data.gv.at) is being expanded into a one-stop shop for protected public data – with an interface to the EU portal (data.europe.eu).
- **Responsible bodies**: Institutions such as Statistics Austria make protected data available for research and innovation under clearly defined conditions in secure processing environments.

The DZG provides regulated access to "protected data" (i.e., personal data, trade secrets) in strict compliance with legal requirements and technical security standards. This opens up new opportunities for research institutions and companies for data-based developments – from health research to sustainable mobility.

In addition, the law establishes data brokerage services – i.e., neutral data intermediaries – in law for the first time and places them under supervision. At the same time, it creates a legal framework for so-called "data altruism": individuals or organizations can voluntarily make data available free of charge for charitable purposes – such as scientific studies or combating climate change.

Legislation – Messenger surveillance

Messenger Surveillance Act

The State Security and Intelligence Service Act (Staatsschutz- und Nachrichtendienst-Gesetz) and the Security Police Act (Sicherheitspolizeigesetz) are to be amended to allow the Directorate for State Security and Intelligence (DSN) to **monitor encrypted and unencrypted digital communication** in the future.
To defend against particularly serious attacks that threaten the constitution, it should be possible to read messages sent via messenger services, although surveillance should only be used as a last resort and be subject to strict legal and technical controls. An independent legal protection officer and the Federal Administrative Court are to be given central review and approval tasks.
The **proposal** has already been approved by the National Council as well as the Federal Council, but the law itself has not come into force yet.
The opposition has voiced strong criticism – one party has even announced that it will be filing a lawsuit before the Constitutional Court. Particularly controversial is the fact that, in case of encrypted messages, the usage of **spyware** is necessary. Written inquiries regarding the procurement of said spyware have already been submitted by several members of Parliament.

EU Project

Project to improve data protection compliance among small and medium-sized enterprises (SMEs)

Since February 2025, the Austrian Data Protection Authority has been working with the Austrian Federal Economic Chamber on a new EU project. The aim of the project (provisional name: GDPR4SMEs) is to develop an online self-audit tool that SMEs can use to assess their company's data protection maturity level. In addition, various tools, checklists, and videos will be provided to help companies comply with the GDPR.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

NIS2 Implementation

Austrian NIS Act 2025 – The wait continues

Since the rejection due to lack of a two-thirds majority in the Austrian National Council, there have been no changes with regard to the national implementation of the NIS2 Directive. When exactly implementation will take place in Austria depends on the parliamentary legislative process and is currently still unclear. However, it is currently expected that the regulations could come into force in 2025.

CER Directive Implementation

Austrian Resilience Act for critical facilities (Resilienzgesetz für kritische Einrichtungen (RKEG))

The Critical Entities Resilience Directive EU 2022/2557 (CER) is the counterpart to the NIS2 Directive and refers solely to physical security risks. The Resilience Act for critical entities (RKEG) explicitly excludes matters relating to cybersecurity that fall under the NIS2 Directive.

However, the RKEG requires the establishment of a coordination procedure between the authorities regarding the CER and the NIS2 for the purpose of exchanging information on cybersecurity risks as well as non-cyber-related risks.

The RKEG will enter into force on the 1 March 2026.

CSA Implementation

Cybersecurity Certification Act

With the adoption of the **Cybersecurity Certification Act** (Bundesgesetz, mit dem ein Bundesgesetz über Daten-Governance, Anbieter von Datenvermittlungsdiensten und datenaltruistische Organisationen nach der Verordnung (EU) 2022/868 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Datenzugangsgesetz (DZG)) and the establishment of a **national authority for cybersecurity certification**, Austria is implementing an EU regulation on cybersecurity (Cybersecurity Act (CSA)), which requires EU member states to designate national authorities for cybersecurity certification.

The aim is to ensure appropriate security standards for ICT products, services, and processes across the EU. The new authority will be based at the Federal Chancellery (Bundeskanzleramt). It will be responsible for monitoring and enforcing the rules of a cybersecurity certification scheme.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The Austrian Data Protection Authority on the relationship between data protection law and the AI Act

On the adoption of the AI Act on 21 May 2024, the Austrian Data Protection Authority (DSB) provided initial information on the relationship between data protection regulations and the AI Regulation on its website (FAQ on AI and data protection and circular letter to public and private sector controllers; only available in German).

The essential aspects of this information are summarized as follows:

- The work of the DSB and the obligations of providers and operators of AI systems in their role as controllers or processors according to the GDPR remain unaffected by the AI Regulation.
- The GDPR remains applicable in parallel with the AI Regulation insofar as the processing of personal data is concerned.
- In connection with AI systems, Article 22 of the GDPR is particularly considerable.
- The AI Regulation also supplements the data protection obligations in some respects. For example, Article 10(5) of the AI Regulation is used as an exception to the prohibition on processing sensitive personal data.
- A market surveillance authority for the supervision and enforcement of the AI Regulation has not yet been established in Austria. In preparation for the implementation of the AI Regulation, an AI service center has been set up at RTR GmbH to serve as a point of contact and information hub on the subject of AI. The DSB is responsible for data protection issues relating to AI systems.

The Austrian RTR GmbH on the AI Act

On the occasion of the adoption of the AI Regulation, Austrian RTR GmbH has also published FAQ with regard to the applicability and implementation of the AI Act in Austria.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Budget cuts lead to reductions in the activities of the DSB

The budget for the DSB for 2025 and 2026 has been reduced compared to the previous year, which will have an impact on the DSB's activities.

In detail, this means:

- The focus will be on treating complaints. However, according to the DSB, delays in treatment are inevitable;
- Official investigation procedures will only be initiated if the submission gives rise to sufficiently concrete suspicion of a serious violation of the GDPR or the Data Protection Act, with particular attention being paid to vulnerable groups (e.g., children, employees);
- Announcement of the (annual) audit focus (topic: e.g., data security) in the sense of an annual strategy without disclosing the industry in January of each year, with simultaneous announcement of the actual start of the audit (e.g., in May);
- Reports pursuant to Article 33 GDPR are reviewed in terms of content. However, a notification is only sent to the controller if the DSB is of the opinion that follow-up measures are necessary, or the report is incomplete;
- Availability by phone will be limited;
- Written legal information will only be provided with a reference to the detailed information on the DSB website;
- The participation of DSB employees in events, including as speakers, will be restricted;
- The DSB will only participate in meetings of the EDSA subgroups if the topic under discussion is of significant interest to the DSB;
- Business trips will be reduced to the absolutely necessary minimum; and
- Statements in the legislative and regulatory review process will only be made if the project touches on fundamental data protection issues.

In its statement, the DSB expressed its hope that there will be a sustainable increase in the DSB's staffing levels in the future so that it can once again fully meet all its responsibilities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Belgium

Contacts

Matthias Vierstraete

Partner, Deloitte Legal Belgium

mvierstraete@deloitte.com

Julie Van Com

Senior Manager, Deloitte Legal Belgium

jvancom@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Market Court decision 2022/AR/292 – IAB case

Market Court decision

In the 2024 edition, we discussed the IAB Europe case (IAB). The IAB is an association of digital advertising undertakings which developed a well-known mechanism facilitating the management of users' preferences for online personalized advertising. They 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 replied to the questions by concluding that "the TC String constitutes personal data where those data may, by reasonable means, be associated with an identifier (including the IP address)." Additionally, the CJEU ruled that: "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."

The Market Court has ruled on the case, taking into account the ruling of the CJEU. The Market Court concluded that the TC string fulfills all conditions to be considered personal data.

It is information that can be used to identify a natural person. Furthermore, the court concluded that IAB possess the necessary resources to identify natural persons regardless of the fact that they had to require third parties to help them.

Recommendation 01/2025 regarding the processing of personal data for direct marketing

The Belgian Data Protection Authority (DPA) has updated its Guidelines on Direct Marketing (the Guidelines) – originally published in 2020 – to account for evolving legal interpretations, case law and industry practices.

This recommendation aims to aid controllers in fulfilling their obligations regarding the protection of personal data. As the GDPR falls short in defining this concept of "direct marketing," the Belgian DPA defined it as "all activities that result in the direct communication of messages with promotional content to one or more identified or identifiable natural persons." There are multiple elements to the definition:

- It doesn't just relate to the communication as such, but to all the activities supporting the communication;
- It relates both to wanted and unwanted communications;
- There is processing of personal data;
- The identity of the natural or legal person whose services, goods, or activities are promoted in the direct marketing message is not relevant;
- The term 'promotional content' has to be understood broadly; and
- The means used to send the direct marketing communication is not relevant.

The recommendation discusses in greater detail the processing of personal data, GDPR principles such as the proportionality principle and the grounds for legitimate processing, the purpose and transparency. Additionally, it mentions the rights of natural personals such as the right of objection and the right to access.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Dispute committee decision 61/2025 of 25 March 2025 case nr.: DOS-2023-03455 and DOS-2023-03186

Dispute committee decision

Facts

This case relates to the installation of a geolocation tracking system by an employer in an employee's company car. The employee disputes the fact that the employer informed him thereof. Additionally, it was no possible for the employee to turn the geolocation device off during vacations of after work. In its capacity of controller, the employer invoked Article(6)(1)(f) GDPR (necessary for the purposes of the legitimate interest) as legal ground for the processing.

Dispute committee decision

The dispute committee assessed the validity to base the processing on Article(6)(1)(f) and concluded that:

- The employer indeed had a legitimate interest;
- The necessity criterion was met. However, the committee does highlight that a suspicion of fraud is not enough of a reason to install a geolocation tracking device; and
- After performing the balancing test, the employer could legitimately rely on Article(6)(1)(f) GDPR.

Nevertheless, the committee did determine multiple other infringements, including an infringement of:

- Principle of purpose limitation;
- Principle of transparency; and
- Access to information.

Guidance and warning of the Flemish Supervisory Commission to cities and municipalities regarding ANPR cameras

Guidance and warning Flemish Supervisory Commission

The Flemish Supervisory Commission (FSC) has, in the year 2024, received multiple complaints from citizens regarding the use of ANPR cameras, which triggered the FSC to issue a guidance and warning, including some critical remarks.

- It has been confirmed that the cities and municipalities qualify as controllers, even if (as was argued) they just receive the information.
- The FSC is of the opinion that ANPR cameras are too easily considered the ‘best solution,’ without taking into account less invasive measures.
- The purpose of the use of ANPR cameras must be specific and clear. References to public order alone are insufficient. There is a risk that purposes are expanded without a new assessment (function creep), resulting in residents being constantly monitored. Furthermore, enforcement must never be used as a source of financial income but should aim to prevent violations and protect public order.
- Another remark is about transparency. There must be transparency about the potential risks to citizens, whereby a public debate is necessary. Data protection impact assessments must include all affected parties and not just residents of that city or municipality. Additionally, the purpose has to be communicated, alongside other elements such as the contact details of the controller and the data protection officer.
- The fifth remark mentions that the controller, thus the city and municipality, must make an assessment of the risks according to the GDPR. The FSC mentions some risks that the city and municipality have to take into account such as unclear purposes, registrations and monitoring of citizens. The risks for the persons involved are considered severe and are insufficiently detected. Thus, there are also not enough protective measures put in place.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Publication of Guidance on the NIS2 Act

Belgium has taken up a leading role with regard to NIS2 implementation. As introduced by this publication last year, Belgium was the first to transpose the NIS2 Directive including a concurring Royal Decree.

The authority ensuring NIS2 compliance in Belgium is the for Cybersecurity Belgium (CCB). The CCB has been very active over the past year to support businesses with regard to NIS2 compliance. Publishing guidelines, implementation documents based on the risk level and most importantly the Frequently Asked Questions on the NIS2 Act. In 2025, the CCB published two versions of their FAQ, with the second one incorporating and addressing specific queries and issues coming from the private sector.

The CCB's FAQs address a wide range of questions including:

- General queries regarding the scope of the NIS2 Act such as, the territorial scope of the NIS2 Act, clarification on the sector interpretations, group structures and intra-group service providers and the calculation of the size of an entity;
- Questions relating to (the concept of) the public sector;
- Clarifications regarding the obligations for essential and important entities subject to the NIS2 Act. This ranges from simple registration obligations to supply chain obligations imposed by the NIS2 Act;
- Illustrating the enforcement of the NIS2 Act, including the competent authorities, conformity assessment bodies, possible administrative measures; and
- Other miscellaneous questions relating to the NIS2 Act.

SafeonWeb launches national prevention campaign against investment fraud

The CCB has prioritized launching an awareness campaign against online investment fraud via its SafeonWeb platform, following the alarming €15 million lost by Belgian investors in the first half of 2025. The two primary sources of these fraudulent losses were fake trading platforms and cryptocurrency scams, which together accounted for over €12 million, three times the amount lost through these channels during the same period last year.

This sharp increase in losses is particularly concerning. Additionally, 1,289 complaints were filed with the Financial Services and Markets Authority (FSMA), although this figure likely underrepresents the actual cases. The average loss per victim was approximately €37,777, with over two-thirds of victims being men aged 50 and above. Emerging fraud trends include scams conducted via recovery rooms, where fraudsters falsely promise to help previously scammed victims recover lost funds, and through social media platforms.

The awareness campaign will be rolled out across cinemas, linear television, and online channels, aiming to raise public vigilance and educate citizens about the risks of online investment fraud. The campaign's message is further amplified through partnerships with public services, schools, banks, and other institutions.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Clarification on intra-group service providers

Belgium positioned itself as a frontrunner in NIS2 implementation. As the CCB implemented the NIS2 Act and published its NIS2 Act Frequently Asked Questions, the CCB received a lot of questions on the practical implementation of the NIS2 Act.

Under the NIS2 Act, every legal entity must independently assess whether it falls within scope, based on its activities, headcount, and financial thresholds. While size assessments can consolidate data from linked or partner entities, the core analysis of sectoral designation remains entity-specific. However, there was uncertainty regarding the designation of intra-group managed/IT service providers who provided services falling in the scope of NIS2. In its second FAQ the CCB provided clarity on this matter.

For intra-group IT service providers, such as those offering cloud hosting, IT support, or cybersecurity services exclusively within the corporate group, the NIS2 obligations still apply if the entity meets size thresholds, and the services fall within the NIS2 Act's definitions. The CCB clarifies that providing IT services to another legal entity qualifies as an activity under NIS2, regardless of whether the services are limited to group members. Such providers must implement risk management, incident notification, and supply chain security measures as required by their designated risk-level.

The CCB also introduced an exception in case group entities jointly share infrastructure, networks, or systems without a clear provider-customer relationship. Here, costs and resources are pooled, and the group functions collaboratively rather than hierarchically. However, practical guidance regarding this specific exception remains limited.

As such, the CCB obliged intra-group service providers to abide by the same rules as companies providing the same services as external providers. This had an important ripple effect on large conglomerates and corporate groups relying on intra-group IT service providers.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Charter for the responsible use of artificial intelligence in public services when providing services to individuals, companies and organizations

On 11 July 2025, the Belgian government introduced a Charter for the Responsible Use of Artificial Intelligence (AI) in public services. The charter aims to guide the ethical deployment of AI in interactions by governmental organizations with individuals, businesses, and other stakeholders, ensuring respect for fundamental rights and public trust.

The charter applies to all endorsing public services and aligns with the AI Act, GDPR, and administrative transparency laws. The charter states that AI systems are complex and not limited to the algorithms *an sich* rather they are complex systems involving data, hardware, human input, and context. However, the charter also recognizes the value it could bring to public services.

Public authorities who sign the charter will commit to using AI responsibly in administrative decision-making and direct user interactions. The key message of the charter is transparency. Citizens must be informed when they engage with AI, and AI-supported decisions must comply with legal requirements, including the right to appeal.

The charter confirms the human oversight obligation with regard to high-risk AI systems. It also recognizes data quality and risk assessments as essential before deployment. The charter also promotes ongoing monitoring to address ethical, legal, and security risks. Furthermore, the charter codifies training for public servants to ensure responsible use of AI, tackling issues like bias and transparency and fulfilling AI literacy obligations.

Lastly, sustainability is also taken into consideration by encouraging attention to AI's environmental impact. Through the adoption of this charter, Belgium aims to lead in ethical AI adoption in the public sector, balancing innovation with responsibility.

(In)Action with regard to the EU AI Act

https://economie.fgov.be/nl/themas/online/artificiele-intelligentie

In the context of AI Act obligations and more specifically AI Act enforcement, each European government will have to designate a notifying authority, market surveillance authority and an authority in charge of fundamental rights' protection relating to high-risk AI systems.

Belgium has failed to designate the national competent authorities, both the Notifying Authority and the Market Surveillance Authority, pursuant to Article 50 of the AI Act. Surpassing the deadline of 2 August 2025.

Nevertheless, the Belgian and local governments have taken action with regard to the designation of public authorities or bodies who will ensure the protection of fundamental rights in the context of high-risk AI systems. The Belgian government has designated over 21 public authorities or bodies who will monitor the respect for fundamental rights pursuant to article 77 AI Act. The link to the full list of respective public authorities or bodies can be found here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Artificial intelligence systems and the GDPR: A data protection perspective

By the General Secretariat of the Belgian Data Protection Authority

The Belgian Data Protection Authority's has published a brochure on Artificial Intelligence Systems and the GDPR. The brochure aims to provide essential guidance on harmonizing AI system development with key data protection laws. It highlights the complementary roles of the GDPR and the newly enforced AI Act in ensuring that AI systems processing personal data operate lawfully, fairly, and transparently.

The brochure clarifies the definition of AI systems and illustrates their use through practical examples. It emphasizes core GDPR principles, such as purpose limitation, data minimization, accuracy, storage limitation, and data subject rights, applied specifically to AI contexts. Accountability is a central theme, with detailed requirements under both the GDPR and AI Act for demonstrating compliance.

Security measures receive particular focus, stressing the need for robust technical and organizational safeguards to protect personal data from risks unique to AI, including bias and manipulation. The brochure also underscores the importance of meaningful human oversight, especially for high-risk AI systems, to ensure responsible development and decision-making.

Targeted at legal professionals, data protection officers, and technical stakeholders, this brochure aims to bridge legal and technical perspectives and links GDPR concepts to AI Act obligations. Furthermore, it offers practical insights and user-centric examples to help organizations embed data protection-by-design principles in AI projects, mitigate ethical and legal risks, and comply effectively with evolving regulatory requirements.

AI strategy in the federal coalition agreement

The Belgian federal coalition agreement outlines a comprehensive AI strategy aimed at responsibly integrating artificial intelligence across public services. It emphasizes a unified, data-driven approach that prioritizes transparency, ethical use, and compliance with European regulations such as the AI Act. Central to this strategy is the establishment of clear governance frameworks, supported by competent authorities like the Belgian Institute for Postal Services and Telecommunications (BIPT), to oversee AI implementation and ensure alignment with data protection and privacy standards.

The federal coalition agreement highlights the importance of balancing innovation with safeguards, particularly in sensitive areas such as healthcare and law enforcement, where AI can enhance efficiency, however, due to the sensitivities of the respective sector, always with fundamental rights at the top of mind. It also promotes collaboration between government departments through standardized policies and a "comply or explain" principle, fostering accountability and flexibility.

By embedding AI within a broader digital transformation agenda, the government aims to improve public service delivery, boost trust in digital platforms, and stimulate economic growth. This strategy fits in Belgium's broader commitment to harnessing AI's potential responsibly, ensuring that technological advancement goes hand in hand with legal and ethical considerations.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Cybersecurity: Awaiting the new National Strategy for Cybersecurity

The for Cybersecurity (CCB) has adopted a leading role with regard to the NIS2 Directive's national adoption. As such, Belgium became the first country to transpose the NIS2 Directive and the CCB has developed a framework, including the necessary support, to guide entities in scope of NIS2 towards NIS2 compliance, namely, the CyberFundamentals Framework. Furthermore, it has also taken active steps to support non NIS2 entities to take steps towards cybersecurity. Lastly, the CCB has also focused on raising cybersecurity awareness of the general public. All of these elements were reflected by the CCB's National Strategy for Cybersecurity for the period from 2021 to 2025.

As 2025 comes to an end, it remains to be seen when an updated National Strategy for Cybersecurity will be adopted. However, we believe it is expected that the CCB will aim to retain its position as one of the leading authorities with regard to NIS2 implementation. In this context, it is to be expected that their will be shift from raising awareness and supporting companies implementing NIS2 obligations, towards compliance enforcement with regards to the most critical entities.

Furthermore, with other European cybersecurity regulation entering into force, such as the Cyber Resilience Act and Cyber Solidarity Act, it is expected that these regulations will be part of further guidance provided by the CCB.

Lastly, it is expected that the CCB will remain focused on raising awareness to the general public, as it did this year through its awareness campaign regarding online investment fraud.

AI: Appointment of Market Surveillance and Notifying Authorities

As previously mentioned in this publication, the Belgian government is lagging behind in its appointment of Market Surveillance and Notifying Authorities as required by the AI Act.

Therefore, we expect that the Belgian government will focus on the appointment of the relevant authorities in the upcoming months so that when the bulk of obligations come into force, Belgium is ready to provide guidance and to raise awareness regarding the AI Act. In a following phase, these authorities will play a key role in enforcement of the AI Act.

Furthermore, the Belgian Data Protection Authority has identified technological progress, of which AI is a key aspect, as one of the most important challenges for the enforcement of data protection rules in its draft strategic plan for 2026-2028 (which will be further discussed on the next page).

The strategic plan also indicates the possible assignment of the Belgian DPA as (one of) the Belgian Market Surveillance Authority(ies). As such, it is expected that the Belgian DPA will also play a role in AI Act enforcement.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection: Draft strategic plan of the Belgian Data Protection Authority for 2026-2028

The Belgian Data Protection Authority (DPA) has published its draft strategic plan for 2026 through 2028. The draft strategic plan aims to provide insight in the priorities of the Belgian DPA and it is an important to document to gain an understanding of the activities of the Belgian DPA, the challenges it expects to face over the upcoming years, to ensure transparency regarding the use of its resources and to provide insights regarding the decision-making process of identifying priorities and enforcement decisions.

The Belgian DPA has set four strategic goals:

- Inform and raise awareness: The Belgian DPA has set out to remain the center of expertise regarding data protection in Belgium. As such it wants to remain the key actor that informs and raises awareness amongst citizens, data protections officers, politicians, companies and other stakeholders;
- Recommendations: The Belgian DPA aims to follow sectoral, regulatory and technological evolutions closely with the aim of quickly providing guidance where necessary;
- Advise, approve and authorize: Provide advice to lawmakers on data protection aspects of new regulation, provide approval to binding corporate rules and certification schemes; and
- Mediation, treating complaints and enforcement: The Belgian DPA aims to remain as accessible as possible while also focusing on the most societally impactful data protection violations. By focusing on the most relevant infringements, the Belgian DPA aims effectively allocate its resources where they are most impactful. As such, the most strategically important cases will be assigned the most resources. Lastly, the Belgian DPA also aims to adopt a more proactive approach where possible.

The draft strategic plan also identifies the following key challenges for the Belgian DPA:

- More and increased complexity of the cases brought before the Belgian DPA;
- Technological and regulatory evolutions; and
- Hiring freeze until 2029.

Nevertheless, the draft strategic plan also aims to address these challenges. Through prioritization both on the level of the tasks and processes within the Belgian DPA as on a substantive level, the Belgian DPA hopes to address these challenges in the most effective manner possible without having to compromise on quality. The substantive focus of the Belgian DPA for the period of 2026-2028 will be:

- Large-scale data processing, both in the private sector as in the public sector which may pose a high risk for the rights and freedoms of those concerned; and
- Processing of minors' personal data.

These substantive focuses will be further developed in the yearly management plan of the Belgian DPA.

Furthermore, the Belgian DPA makes it clear throughout its strategic plan that it does not see data protection in isolation from other relevant regulation. Data protection rules are part of the broader EU Digital Strategy and, as such, the Belgian DPA is aware and will take its responsibility where required with regard to the AI Act, Data Act, Data Governance Act, ...

Finally, cooperation will remain a key focus in the upcoming years as the Belgian DPA aims to improve its involvement in the EDPB, wants to cooperate more closely with other authorities, both focusing on data protection and other digital regulations, at the national level and to improve cooperation with stakeholders and lawmakers where relevant.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Bulgaria

Contacts

Miglena Micheva

Senior Manager, Deloitte Legal Bulgaria

mmicheva@deloittece.com

Irena Koleva

Manager, Deloitte Legal Bulgaria

ikoleva@deloittece.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Opinions of the Bulgarian Commission for Personal Data Protection

Opinion on the use of facial recognition functionality in retail outlets

The Bulgarian Commission for Personal Data Protection (CPDP) issued an Opinion № ПНМД-01-52/2025 related to the admissibility of the processing of personal data through a video surveillance system with facial recognition functionality in retail outlets (shops).

According to the CPDP, the entry and subsequent processing of facial images of customers, who have attempted or committed theft or exhibited other illegal behavior, for the purpose of facial recognition by the video surveillance system during future visits to retail outlets, does not constitute a matter of significant public interest under Article 9(2)(g) of the GDPR.

None of the conditions under Article 9(2) of the GDPR for the admissibility of processing biometric data for identifying natural persons are applicable and cannot justify the planned processing of such data for the purposes specified by the applicant. In particular, the consent of the data subjects is not applicable. This leads to the conclusion that the planned processing does not comply with the requirements of the GDPR and is therefore deemed inadmissible.

The processing of biometric data by means of facial recognition technology may be carried out based on a reason of important public interest, where it is established in EU or national law, considers the nature of the data controller's activity and is a necessary, appropriate and proportionate measure in a democratic society that guarantees an objective of important public interest.

According to the CPDP, such a reason of important public interest may include ensuring security in national security facilities or elements of the country's critical infrastructure.

Guidelines of the CPDP

Guidelines on the use of video recorders in private vehicles

The CPDP points out that the need for such guidelines is justified by the increased use of technical means of recording installed in cars (the so-called video recorders) and the resulting risk of complicating consequences for the rights to protect the privacy and personal data of other road users.

According to the CPDP, when personal data is processed and the exception for "purely personal or domestic activities" is not applicable, the person responsible for recording with a dashcam should be considered a "data controller.“ In this case, the following requirements must be observed:

- Personal data must be processed in a transparent manner;
- Personal data must only be stored for as long as necessary to achieve the purpose for which it was collected;
- Personal data must be kept secure;
- Individuals have the right to access their data; and
- The publication of filmed material, e.g., on social networks, is an additional processing operation that may pose a risk of violating the data protection rights of the filmed persons.

The full text of the guidelines is published here: https://cpdp.bg.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Recommendations, instructions and advice from the CPDP

Recommendations for personal data controllers when assigning the processing of personal data

The Bulgarian Commission for Personal Data Protection (CPDP) has published recommendations for data controllers due to a significant number of instances involving a formal approach to defining the conditions for regulating relationships when assigning activities to personal data processors, in accordance with the requirements of Article 28 of the GDPR. The recommendations cover the actions that the data controller should take before selecting a data processor, the actions required prior to concluding a contract for processing personal data with the data processor, as well as the legal basis for managing the relationship between the controller and the processor – Article 28 of the GDPR.

The full text of the recommendations is published here: https://cpdp.bg.

CPDP advice related to unintentional or thoughtless disclosure of personal data

The CPDP has published advice on unintentional or thoughtless disclosure of personal data. The need for this advice is explained by the wide scope and sensitivity of personal data and the increasing number of situations where personal data is inadvertently disclosed. In this regard, the CPDP has noted an increase in inquiries and reports of cases where individuals (data subjects) have inadvertently disclosed personal data – either their own or that of their relatives.

The full text of the advice is published here: https://cpdp.bg.

Instructions to data controllers

According to the published announcement from the CPDP, data controllers are encouraged to clearly and distinctly indicate the contact information for the competent supervisory authority – the CPDP – to avoid misleading individuals seeking contact with the data controller itself.

The announcement is published here: https://cpdp.bg.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Amendments to the Cybersecurity Act transposing the NIS2 Directive

On 12 December 2024, the Council of Ministers submitted a Bill on Amendments and Supplements to the Cybersecurity Act (the Bill) to the Bulgarian National Assembly. This Bill aims to shape the regulatory framework for cybersecurity by introducing the requirements of the NIS2 Directive.

The adoption of the Bill is intended to provide high guarantees and opportunities for better resilience of cyberspace and more effective measures to counter cyberattacks, especially concerning major economic entities and state authorities.

The key change is a significant expansion of the sectors affected, which now include energy, transport, the banking sector, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, ICT governance (between businesses), public administration, and space. Critical sectors have also been identified, including postal and courier services, waste management, production, preparation and distribution of chemicals, food production, processing and distribution, manufacturing, digital service providers, and scientific research.

The adoption of the amendments would result in the assignment of additional powers to the competent authorities in the field.

It is expected that the amendments to the Cybersecurity Act will simplify and accelerate the process of interaction and resolution of cross-border and national incidents within the EU.

The Bill has passed its first reading in the National Assembly, and the second (final) reading is anticipated* by the end of 2025/ beginning of 2026

*As of 12 November 2025, the second reading has not passed yet.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Bill on the Use and Development of Artificial Intelligence

On 8 October 2025, a group of members of the Bulgarian National Assembly submitted a Bill on the Use and Development of Artificial Intelligence (the Bill). The purpose of the Bill is to create a framework for the implementation of the EU AI Act, the use of AI in the public sector, including for the provision of electronic administrative services. The adoption of the Bill is expected to stimulate the development of employees' skills for using AI in their work and foster investments in the development and use of AI. The Bill includes draft provisions to minimize risks to national security that could arise from the malicious use of AI.

It is envisaged that the government policy regarding artificial intelligence aimed at public administration will be led by the Bulgarian Minister of Electronic Governance. The Bulgarian Minister of Innovation and Growth shall lead government policy aimed at encouraging the use and development of artificial intelligence in the private sector.

Competent state bodies are determined by sector. For example, the Bulgarian National Bank shall oversee the use of AI by credit institutions.

The Prime Minister, upon proposal by the Minister of Electronic Government, shall appoint a National Coordinator for the use and development of AI. The National Coordinator will be responsible for the adoption of the National AI Strategy and will coordinate projects under various programs.

The Bill is intended to introduce a ban on the use of certain high-risk AI systems, such as those used in remote biometric identification. AI systems that can be considered threats to national security are identified in the Bill, which also introduces restrictions on the use of third-party AI services that pose a risk to national security. The publication of deep fake content created by artificial intelligence systems on online platforms is regulated in the Bill.

The Bill provides for administrative sanctions for failing to comply with its provisions, with fines varying depending on the nature and extent of the violations committed.

The Bill will be reviewed by the competent parliamentary commissions and then voted on by the National Assembly.

Decision of the Council of Ministers for the designation of national bodies for the protection of fundamental rights, including the right to nondiscrimination, pursuant to Article 77 of the EU AI Act

On 19 June 2025, the Council of Ministers made a decision designating national bodies to supervise or ensure compliance with obligations under EU law for the protection of fundamental rights, including the right to nondiscrimination, in relation to the use of high-risk artificial intelligence systems listed in Annex III of Regulation (EU) 2024/1689 of the European Parliament and the Council of 13 June 2024, establishing harmonized rules on artificial intelligence (AI Act).

The authorities designated according to their legal powers are as follows:

- Ombudsman;
- Central Election Commission;
- Commission for Protection against Discrimination;
- Commission for Personal Data Protection;
- Commission for Consumer Protection;
- State Agency for Child Protection; and
- Executive Agency "General Labor Inspectorate."

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

Draft rules amending the Rules on the Activities of the CPDP and its Administration

The CPDP is opening a procedure for public discussion of draft Rules amending the Rules on the Activities of the CPDP and its Administration.

The proposed changes aim to address difficulties that have arisen over time in the functioning of the administration and seek to achieve greater efficiency in organizing work and ensuring supervisory activities. Additionally, they aim to overcome gaps identified in the implementation of the Rules on the Activities of the CPDP and its Administration.

Strategy of the CPDP for Development in the Fields of Personal Data Protection and Protection of Whistleblowers (horizon 2024-2029)

The CPDP's strategy for development in the field of personal data protection, which set strategic goals for the period 2017-2022, has already expired. The CPDP is expected to finalize the review of its strategic goals, a process that began in 2022. The new CPDP strategy should identify priorities for development in its 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 the national law by the deadline of 17 October 2024.

The Bill on Amendments and Supplements to the Cybersecurity Act has passed its first reading in the National Assembly, and the second (final) reading is anticipated* by the end of 2025/beginning of 2026.

*As of 12 November 2025, the second reading has not passed yet.

National Cybersecurity Strategy

The National Cybersecurity Strategy of Bulgaria expired in December 2023, and a new one shall be adopted. 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.

AI

A Bill on the Use and Development of Artificial Intelligence has been submitted to the National Assembly. It is expected to be reviewed by the competent parliamentary commissions and then voted on by the National Assembly.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Chile

Contacts

Ruby Soteras

Partner, Deloitte Legal Chile

rsoterasf@deloitte.com

Oliver Ortiz

Senior Manager, Deloitte Legal Chile

oortizq@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Personal Data Protection Act

Law N°21,719 or the Personal Data Protection Act amends the 1999 Chilean Private Life Protection Act (Law N°19,628).

- The Chilean Congress has approved the new Personal Data Protection Act (the Act), elevating the standard of data privacy rights for citizens.
- Although it has already been published, its full entry into force shall be as of 1 December 2026.
- As it bears similarities with the European GDPR, the new Act strengthens the data protection ecosystem in the country and thus brings Chile closer to international standards on the matter.
- The Act establishes the right of individuals to know, rectify, delete, block and oppose the processing of their personal data.
- It creates the Personal Data Protection Agency (APDP), an autonomous authority responsible for supervising and enforcing data protection regulation and establishes a series of new obligations for data controllers and processors, introducing significant sanctions for violations, including fines of up to US$1.5 million.
- The new regulation applies to both public and private entities that process personal data.
- The law emphasizes transparency, security, and the responsible use of personal data.
- It also includes provisions for the protection of sensitive personal data and the obligation to report data breaches.
- The approval of this law is considered a milestone for the protection of citizens' rights in the digital era in Chile.

Consolidated Debt Registry Act

Law N°21,680 or the Consolidated Debt Registry Act creates an official registry of information on credit obligations and contains some personal data dispositions.

- The Consolidated Debt Registry Act (the Act) was enacted as of July 2024, and will fully enter in effect as of 1 April 2026, and aims to create an official registry of information related to credit obligations, in order to improve the credit evaluation system of individuals and to provide the Financial Market Commission (FMC) with more information for the exercise of its regulatory and supervisory powers and the fulfillment of its legal functions.
- It contains some articles regarding personal data protection that interact with the Chilean Private Life Protection Act No. 19,628, and its 2024 Amendment, the Personal Data protection Act NO. 21,799.
- In particular, the Act indicates that the treatment of personal data for the creation and maintenance of the registry must always ensure data privacy in the terms of the Chilean Private Life Protection Act No. 19,628.
- The FMC shall regulate, by means of a general rule, the operational functioning of the registry, the periods for updating the information online, and the access procedures for reporting entities, their representatives, debtors, and third parties authorized by the latter.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cybersecurity Framework Act

Law N°21,663 on Cybersecurity and Critical information Infrastructure

- Enacted in March 2024, Law No. 21,663 or the Cybersecurity Framework Act (CFA) sets out to regulate Chile's national cybersecurity ecosystem, creating a new institutional framework for dealing with issues related to the topic, setting out new responsibilities and categories of obligated entities, and establishing graduated sanctions in case of noncompliance with the law.
- The Act created the National Cybersecurity Agency (Agencia Nacional de Ciberseguridad (ANCI)) as the country's central authority on cybersecurity.
- The CFA creates a national coordination framework for cybersecurity policy, crisis response, and information sharing.
- The CFA applies to both public and private sectors, creating the categories of essential services providers (PSE), and operators of vital importance and critical infrastructure (OIV).
- The CFA:
  - Sets new cybersecurity standards, introduces mandatory incident reporting, and enforces sanctions for noncompliance, with potential fines up to US$3 million. These are graduated sanctions for noncompliance, including administrative, financial, and reputational penalties;
  - Imposes mandatory cybersecurity incident notification to the National CSIRT within specified deadlines, for certain operators;
  - Requires implementation of risk management frameworks, business continuity plans, and security audits; and
  - Defines and regulates OIVs – entities whose disruption could significantly impact national security, the economy, or essential public services, and which either work with digital services or provide them to others.

Essential services providers (PSE) and operators of vital importance (OIV)

- PSEs are public or private entities designated by the ANCI that provide services essential to the continuity of critical social or economic activities, amongst others.
- On the other hand, OIVs are those entities which depend on digital or networked systems for essential operations, provide those digital or networked services, and whose disruption would cause major consequences for national security, public order, or economic stability.
- Includes sectors such as energy, telecommunications, healthcare, finance, transport, and water supply.
- The legal requirements set forth by the CFA are highly more stringent on OIVs, entities which are required to: (i) implement an Information Security Management System (ISMS) aligned with international standards (e.g., ISO 27001), (ii) maintain business continuity and disaster recovery plans to ensure resilience, (iii) report cybersecurity incidents promptly to the ANCI and the National CSIRT, (iv) undergo regular audits, risk assessments, and emergency simulations, and (v) ensure coordination with sectoral authorities and other critical infrastructure operators.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Relationship with the Personal Data Protection Act (Law N°21,719)

- While Law N°21,663 (CFA) governs cybersecurity and infrastructure, Law N°21,719 (Personal Data Protection Act) regulates **personal data handling**.
- **Intersection:** OIVs often process large volumes of personal or sensitive data (identity, financial, or health information).
- Compliance with **both laws** is essential:
  - Law N°21,663 ensures network and system security; and
  - Law N°21,719 ensures privacy and lawful processing of personal data.
- The CFA reinforces a unified national approach to cyber resilience, data governance, and digital trust, and strongly complements Law N°21,719 on Data Protection, creating a dual legal shield for both system security and information privacy.
- For critical entities, compliance with both frameworks is strategic, mandatory, and of national importance.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Overview

- The Chilean government has taken significant steps in AI governance, focusing on ethics, transparency, data protection, innovation and risk-based regulation.
- Major milestones include the update of the national AI policy, public consultations, and a draft bill to legally regulate AI systems.
- These developments are important for any organization operating or using AI in Chile, especially with respect to rights protection, system governance and regulatory preparedness.

National AI Policy 2024 – Consultation and update

- On 15 January 2024, the Ministry of Science, Technology, Knowledge and Innovation opened a public consultation on the update of Chile's National Artificial Intelligence Policy 2024.
- The consultation closed on 15 March 2024.
- Key areas included: ethics and governance; international collaboration; AI's role in climate change; children and workforce implications; gender, equity, nondiscrimination; cultural heritage; secure digital ecosystems; and regulation.
- The updated policy reflects alignment with international norms such as UNESCO's Recommendations on AI Ethics and OECD work.
- The most significant Implication is that organizations must align AI strategies with ethical and governance frameworks, anticipate regulatory changes.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Draft Bill for Regulation of AI Systems – Bill No. 16,821-19/15,869-19

- On 7 May 2024, a bill was introduced in the Chilean Chamber of Deputies entitled "Bill regulating Artificial Intelligence Systems (No. 16821-19)."
- The draft proposes a risk-based classification of AI systems: unacceptable risk (prohibited), high risk, limited risk, no-evident risk.
- Requirements include system documentation, human oversight, transparency, liability, notification of serious incidents, data protection obligations.
- As of October 2025, the Chamber of Deputies approved the bill and forwarded it to the Senate.
- The AI bill emphasizes compliance with data protection laws (such as the Personal Data Protection Act) and cybersecurity obligations.
- The policy and draft legislation embed value-based aspects: nondiscrimination, equity, transparency, accountability, and heavily focuses on fundamental rights considerations.
- The bill aims to "promote the creation, development, innovation and implementation of AI systems **in service of human beings**, respectful of democratic principles and the rule of law."
- It targets **systems of AI** whose output information is used in Chile – so even if the system is located abroad, if its output reaches Chile it may fall under the draft's scope.
- The bill is structured around 10 chapters (titles) including: general provisions, classification of AI systems by risk, prohibited uses, high-risk systems, limited risk systems, incidents, governance, innovation support, consumer rights, and sanctions.

Classification of AI systems by risk and principles

The bill adopts a **risk-based approach**, classifying AI systems into four categories:

- **Unacceptable risk:** Systems that pose unacceptable threats to fundamental rights; these would be banned;
- **High risk**: Systems that could significantly impact fundamental rights, safety, environment, or consumer rights; subject to stricter obligations;
- **Limited risk**: Systems with lower risk; subject to lighter obligations (e.g., transparency, user notification); and
- **No-evident risk:** Systems assessed as having minimal risk; lowest regulatory burden.

The draft bill lays out a set of **governance and ethical principles**, including:

- Human oversight/supervision of AI systems;
- Technical robustness, safety and security;
- Privacy, data governance and protection of personal data;
- Transparency and traceability;
- Nondiscrimination, equity (social and gender) and fairness;
- Social and environmental well-being;
- Accountability/responsibility of those who deploy or use AI; and
- Consumer protection and rights when interacting with AI-driven decisions.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Governance and institutional framework

- The bill foresees the involvement of the Agencia de Protección de Datos Personales (APDP) as the supervisory authority for many obligations under the law.
- Entities subject to the proposed law include providers of AI systems, implementers, and importers or distributors located in or whose output reaches Chile.

Obligations, sanctions and innovation support

- Providers/implementers of AI must document their systems, classify them according to risk, implement safeguards (especially for high-risk systems).
- The bill draft includes **reporting obligations** for serious incidents involving AI systems.
- The draft sets fines up to **US$1.5 million** for grave violations, among other administrative or reputational consequences.
- The bill also includes **innovation support measures**: regulatory sandboxes/spaces for controlled testing of AI systems, especially for SMEs; promotion of infrastructure enabling AI.

Relevance and next steps

- If approved, this law would place Chile among the first in Latin America with a comprehensive, binding AI regulatory law modelled after global practices (e.g., the EU's AI Act).
- Organizations operating in or entering Chile should monitor developments and prepare for obligations around: system documentation, classification, transparency, incident reporting, and data protection alignment.
- The legislative process continues; amendments may refine obligations, institutional responsibilities and timelines.
- Final approval timeline is not yet fixed – the bill is now in the Senate stage.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Colombia

Contacts

Jose Luis Jerez

Partner, Deloitte Legal Colombia

jjerez@deloitte.com

Andrés Felipe Salazar

Senior Associate, Deloitte Legal Colombia

andsalazar@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Guidelines for the Protection of Personal Data in Artificial Intelligence Systems

External Circular No. 003 of 2024 dated 18 September 2025, Superintendency of Industry and Commerce

This circular is intended to provide legal certainty to data controllers regarding the lawful processing of personal data in the context of the development, deployment, and use of AI systems. It also aims to ensure that data subjects can trust that their personal data will be handled responsibly and transparently within such systems, which are commonly used for autonomous decision-making or to support human decision-makers through predictive analytics and recommendations.

In processing personal data through AI systems, data controllers are required to implement appropriate mechanisms to identify, evaluate, and mitigate associated risks, thereby ensuring compliance with applicable data protection laws and regulations.

Furthermore, during the design and development of AI systems, a data protection impact assessment must be conducted to determine the potential effects of such technologies on personal data. This is essential to ensure that data subjects are adequately informed of their rights in relation to the use of AI tools. As stated by the Superintendence of Industry and Commerce, AI systems must incorporate relevant, effective, and demonstrable strategies to uphold and guarantee the rights of data subjects.

Guidelines for the Processing of Personal Data within the Framework of Fintech Operations

Circular 001 of 2025 dated 18 September 2025, Superintendency of Industry and Commerce

On 18 September 2018, the Superintendency of Industry and Commerce, the data protection authority in Colombia, issued a circular containing instructions regarding the processing of personal data in the context of offering products and providing services related to financing, low-value deposits, and other similar activities aimed at promoting financial inclusion through the use of digital technologies (fintech).

Within this framework, the entity established that fintech companies, although supervised by the Financial Superintendency of Colombia, must comply with all constitutional principles and duties, as well as those set forth in Law 1581 of 2012, in relation to the processing of personal data they collect.

The circular also includes an express prohibition against accessing the device's image gallery or contact list for debt collection purposes. Additional specific obligations are included, such as informing the data subject about which purposes are necessary for the provision of the service and which are ancillary, as well as requesting authorization for various functionalities of web applications, such as access to the camera and microphone.

In general, this circular reinforces the obligations of data controllers and processors that provide services in the Fintech sector and adds certain requirements specific to their activities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

National Digital Security Strategy of Colombia 2025-2027

National Strategy March 2025

The National Digital Security Strategy of Colombia 2025-2027 represents a comprehensive and forward-looking initiative designed to address the challenges and opportunities arising within a constantly evolving digital environment. This strategic framework aims to enhance Colombia's digital security posture by effectively responding to emerging threats and leveraging technological innovation to foster a more secure, resilient, and trustworthy cyberspace.

This strategic framework prioritizes four core pillars deemed critical to reinforcing Colombia's cybersecurity posture:

- Strengthening digital security governance to address institutional fragility and improve inter-agency coordination;
- Advancing national cyber resilience to mitigate exposure to increasingly sophisticated cyberthreats;
- Cultivating a skilled and sustainable cybersecurity workforce to close the gap in specialized talent; and
- Updating and aligning the cyber legal and regulatory framework to effectively respond to emerging technological and security challenges.

Through targeted strategic actions across key focus areas, the strategy aims to reshape Colombia's digital security landscape by enhancing national capabilities, fostering cross-sector and international cooperation, and promoting an inclusive digital security culture. This holistic approach positions the country to effectively counter current and future cyberthreats, safeguarding national interests and the digital well-being of its citizens.

Resolution 02277 of 2025 – MinTIC's Update to the Information Security Model

Resolution 02277 of 2025

In 2025, Colombia's Ministry of Information and Communications Technologies (MinTIC) issued Resolution 02277, updating the national Information Security and Privacy Model (MSPI). This reform aligns the model with the international standard ISO/IEC 27001:2022, reflecting Colombia's commitment to global best practices in cybersecurity and digital governance. The resolution aims to enhance the protection of digital assets across public sector entities.

One of the key impacts of the resolution is the repeal of over 10 outdated technical documents, streamlining the regulatory framework and reducing implementation complexity. By modernizing the MSPI, MinTIC facilitates more agile and effective adoption of cybersecurity protocols, especially in government institutions that manage sensitive citizen data and critical infrastructure.

The updated model also introduces simplified compliance mechanisms, making it easier for public entities to meet security requirements without compromising robustness. This initiative supports Colombia's broader digital transformation strategy, reinforcing institutional resilience and trust in public digital services. Resolution 02277 marks a significant step toward harmonizing national cybersecurity efforts with international standards.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

CONPES 4144 – Colombia's National AI Policy

CONPES 4144 February 14, 2025

In February 2025, Colombia approved CONPES 4144, a strategic document that defines the country's national policy on AI through 2030. The policy aims to foster ethical, inclusive, and sustainable AI development, positioning Colombia as a regional leader in responsible innovation. It outlines 106 specific actions across six strategic pillars: ethics and governance, data and infrastructure, research and innovation, digital talent, risk mitigation, and sectoral adoption.

The policy was developed through a multi-stakeholder approach involving key government entities such as MinTIC, MinCiencias, DNP, and MinEducación. It emphasizes the importance of cross-sector collaboration, institutional capacity building, and the integration of AI into public services and productive sectors. A total budget of COP 479 billion was allocated to implement the policy, reflecting the government's commitment to long-term digital transformation.

CONPES 4144 also introduces mechanisms to ensure transparency, human oversight, and algorithmic accountability. It promotes the responsible use of AI while safeguarding fundamental rights, including privacy, nondiscrimination, and access to technology. The policy serves as a foundational framework for future regulatory developments and international cooperation in AI governance.

Law 2502 of 2025 – Criminal Code Reform on AI Identity Fraud

Law 2502, 2025

In August 2025, Colombia enacted Law 2502, introducing a specific criminal aggravating factor for identity fraud committed through AI. This includes the use of deepfake technologies and digital impersonation tools to deceive, manipulate, or harm individuals. The reform updates Article 296 of the Criminal Code, reflecting the growing risks posed by AI-driven deception.

The law provides legal definitions for emerging technological concepts such as "deepfake" and "digital image," establishing a clearer framework for judicial interpretation and enforcement. These definitions are designed to support prosecutors and judges in identifying and sanctioning AI-related offenses, especially those involving falsified audiovisual content or unauthorized digital representations.

Beyond punitive measures, Law 2502 outlines public policy guidelines for prevention and response. It calls for ethical standards in AI development, enhanced cybersecurity protocols, and international cooperation to combat cross-border digital crimes. Additionally, it mandates the creation of rapid response mechanisms to address technological incidents, reinforcing Colombia's commitment to digital justice and citizen protection.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Bill 043 of 2025 – AI Legal Framework Proposal

Bill 043 July 28, 2025

Bill 043 of 2025 was introduced in the Colombian Congress to establish a comprehensive legal framework for the development and deployment of AI systems. The bill proposes a risk-based classification of AI technologies, distinguishing between low, medium, and high-risk systems. It sets out guiding principles such as transparency, ethical design, human supervision, and technological sovereignty.

The proposed law defines legal responsibilities for all actors involved in the AI lifecycle, including developers, deployers, and users. It introduces administrative, civil, criminal, and ethical liabilities, ensuring that AI systems operate in alignment with constitutional rights and democratic values. The bill also mandates impact assessments and public disclosure for high-risk AI applications.

Bill 043 complements the national AI policy by translating strategic goals into enforceable legal standards. It seeks to balance innovation with regulation, fostering trust in AI technologies while protecting citizens from potential harms. If enacted, the bill would place Colombia at the forefront of AI governance in Latin America, aligning its legal system with emerging global norms.

Bills for the Modernization of the Personal Data Protection Law

Bills No. 214 and 274 of 2025 Congress of the Republic of Colombia

The bills aim to update and strengthen the regulatory framework for personal data protection in Colombia, adapting it to the challenges of the digital economy.

The scope of the law is expanded to include any data processing linked to Colombian territory, regardless of the data controller's location. Additionally, key definitions are introduced, such as automated processing and profiling, acknowledging the use of technologies without human intervention.

The prohibition on processing minors' data is relaxed, allowing it for individuals over 14 years of age with their consent, while maintaining state and societal obligations for their protection. The legal bases for data processing are also broadened, including contract performance, and supervisory functions are reinforced, promoting better coordination between the data protection authority and the Office of the Inspector General (Procuraduría General de la Nación).

Overall, these legislative initiatives represent a significant step toward a more robust, adaptive, and rights-based data protection regime in Colombia, capable of responding to the challenges posed by digital innovation and cross-border data processing.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Costa Rica

Contacts

Ricardo Güell

Partner, Deloitte Legal Costa Rica

riguell@deloitte.com

Estefanía Ramírez

Manager, Deloitte Legal Costa Rica

esteramirez@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Personal Data Protection Law (Bill No. 23,097)

Costa Rica's data protection framework is currently governed by Law No. 8968. However, there are significant amendments being are underway to align with international standards such as the GDPR and Convention 108.

- Bill No. 23,987 proposes modernization of the law, introducing rights such as data portability, erasure (right to be forgotten), and restriction of processing. It also establishes a stronger Data Protection Agency with independent funding and enhanced enforcement powers.
- Active legislative debate on a comprehensive amendment of Law No. 8968 to address emerging technologies like AI and blockchain.
- Privacy Forum 2025 highlighted challenges posed by AI and cybersecurity, issuing recommendations for impact assessments and robust incident response protocols.

Status: The bill is under discussion in the Legislative Assembly and expected to advance in 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

National Cybersecurity Law (Under Legislative Review)

Introduced in 2025, this Bill responds to severe ransomware attacks suffered in 2022.

Costa Rica has made significant progress in advancing discussions on the **Cybersecurity Law**, which aims to establish a comprehensive legal framework for protecting critical infrastructure and managing cyberthreats. The proposed law outlines several key measures, including:

- Creation of the **National Cybersecurity Agency (ANC)** under MICITT;
- Establishment of specialized centers:
  - **CSIRT-CR** (Incident Response Center);
  - **CIMR-CR** (Network Monitoring Center); and
  - **CID-CR** (Cybersecurity Intelligence Center).
- Declaration of critical information infrastructure as a matter of **national security**;
- Mandatory compliance with international standards (ISO/IEC 27001, NIST); and
- Obligations for public and private operators of critical ICT infrastructure:
  - Business continuity plans;
  - Risk management and incident reporting to CSIRT; and
  - Certification of Information Security Management Systems (ISMS).

Status: Under legislative debate; controversial due to cost and technical challenges.

National Cybersecurity Strategy 2023-2027

Launched by MICITT, this strategy sets five pillars:

- Governance and coordination;
- Protection of critical infrastructure;
- Legal modernization and resilience;
- Education and awareness; and
- International cooperation.

Includes **Directriz N° 133-MP-MICITT** for public sector cybersecurity improvements and **Decree N° 44196-MSP-MICITT** on security measures for 5G networks.

Guidelines and technical standards

- Adoption of **cloud-first policy** for public institutions (Decree N° 46-H-MICITT);
- Mandatory accessibility and network security measures for government websites; and
- Strengthening CSIRT-CR protocols for incident response and coordination.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Costa Rica launched its National AI Strategy (2024-2027) to promote ethical and secure adoption of AI technologies

The strategy focuses on governance, infrastructure, and talent development.

Highlights:

- Seven strategic pillars including ethical AI, smart government, digital infrastructure, and workforce training;
- Costa Rica ranks among the top in Latin America for AI readiness, excelling in governance and open data initiatives; and
- Research centers and universities are actively developing AI capabilities and regulatory sandboxes.

Status: Implementation is ongoing with strong institutional support.

Global leadership in AI governance

Costa Rica is co-leading an intergovernmental initiative within the United Nations to establish an International Scientific Panel on Artificial Intelligence and a Global Dialogue on AI Governance. Launched in 2025, this effort seeks to develop a comprehensive global framework for AI governance, addressing both challenges and opportunities in AI development while ensuring alignment with the UN Sustainable Development Goals.

Costa Rica has introduced several draft bills aimed at regulating AI:

- Bill No. 23,771: Presented in May 2023, this proposal focuses on AI auditing and accountability. It requires developers to implement measures to mitigate algorithmic bias and prevent discriminatory outcomes. The bill emphasizes compliance with human rights principles and calls for independent oversight of AI systems.
- Bill No. 23,919: This initiative promotes the responsible adoption of AI as a matter of public interest. While it encourages ethical use and innovation, it does not include specific provisions on AI auditing.
- Bill No. (unassigned): This draft underscores the importance of auditability and due diligence throughout the AI system lifecycle, advocating for robust governance mechanisms.

These legislative efforts remain under review, with ongoing consultations involving technology experts, legal professionals, and human rights advocates.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

- A **pending bill** in Congress seeks to **fully amend Law No. 8968** to align with GDPR principles (lawfulness, transparency, accountability, data subject rights). This amendment has been under discussion since 2021 and is expected to gain traction by 2026.
- Stronger **cross-border data transfer rules** and **explicit consent requirements** for sensitive data.
- Integration with AI governance: AI systems will need **privacy-by-design** and **bias audits**, especially under ENIA (AI Strategy).

Cybersecurity

- **National Cybersecurity Strategy 2023-2027:** Aiming to become a trustworthy digital ecosystem by 2027 through governance, regulatory updates, infrastructure protection, capacity building, and international cooperation.
- **SOC-CR (National Security Operations Center):** Fully operational for real-time threat monitoring and incident response.

AI

- **Landmark AI Regulation Bill** advanced in late 2025, aiming for a **principles-based framework**:
  - Transparency and accountability for AI systems;
  - Prohibitions on exploitative AI uses; and
  - Risk-based approach for high-impact sectors (health, justice, finance).
- Full enactment of AI law with **mandatory algorithmic audits**, **human-in-the-loop requirements**, and **data privacy integration**.
- Establishment of **National AI Center of Excellence** and **regulatory sandboxes** for testing AI applications.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Croatia

Contacts

Zrinka Vrtarić

Director, Vrtaric & Partners (member of the Deloitte Legal network)

zvrtaric@kip-legal.hr

Ana Romić

Associate, Vrtaric & Partners (member of the Deloitte Legal network)

anromic@kip-legal.hr

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

AZOP's 2024 annual report on personal data protection

In March 2025, the Croatian Personal Data Protection Agency (AZOP) published its annual report on personal data protection for the year 2024. The report provides an overview of AZOP's main activities, achievements, and enforcement actions in the field of data protection during 2024.

The year 2024 was marked by record numbers across AZOP's core areas of operation – enforcement, supervision, and education.

Key themes of 2024 included AI and its interaction with GDPR. The EDPB's work, in which AZOP participated, focused heavily on large language models (LLMs) and the adoption of guidelines on legitimate interest, pseudonymization, and the ongoing development of guidance on anonymization and the AI Act-GDPR interplay.

Key figures for 2024: (i) 1,257 complaints/requests for determination of data protection violations, a 290% increase compared to 2023, (ii) 698 inspections conducted, an increase of 28% year-on-year, (iii) 206 corrective measures issued, including 38 administrative fines, the highest number in AZOP's history, and (iv) 3,171 cases resolved, representing a 32% increase compared to 2023.

Major focus areas:

- Artificial intelligence: Oversight of data processing in AI systems, particularly large language models;
- Cybersecurity incidents: An increase in data breaches and cyberattacks across Croatia prompted several ex officio investigations; and
- Education and awareness: AZOP organized 48 free educational events and 30 workshops reaching over 3,500 SMEs and launching the "Olivia" online compliance tool to help companies align with data protection laws.

Croatian energy utility provider fined €320,000 for password security failure and serious GDPR breaches

AZOP imposed an administrative fine of €320,000 on the energy utility provider, a state-owned district heating company, for multiple violations of the GDPR, primarily related to the failure to implement adequate technical and organizational measures and noncooperation with the supervisory authority.

An individual complained that, when requesting a password reset on provider's online portal "Moj račun" (My Account), users received by email a "temporary password" that was actually their previous password.

AZOP's investigation found that the company stored passwords of nearly 16,000 users in plain text within its database; the password reset mechanism re-sent the existing password instead of generating a new one; no encryption, hashing, or other basic safeguards were in place; the controller had not conducted any risk assessment nor applied security measures required under Article 32(2) GDPR.

Despite being aware of these risks, the provider deliberately chose a system design lacking fundamental safeguards and later failed to cooperate with AZOP during the inspection.

The company did not provide the requested documentation or evidence of remedial measures, nor did it notify affected users after discovering the security flaw, violating Articles 31 and 32 GDPR.

AZOP emphasized that storing passwords in readable form exposed users to serious risks of unauthorized disclosure and misuse and that the controller's refusal to cooperate aggravated the infringement.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Sports betting operator fined €175,000 for poor data security and improper retention of customer data

AZOP imposed an administrative fine of €175,000 on a sports betting company for failing to implement adequate technical and organizational measures to protect personal data and for unlawful data retention practices.

AZOP initiated the investigation after receiving a complaint that the betting operator required users to send copies of their ID cards via unencrypted email for account verification on its website.

This method posed a high risk to users' rights and freedoms.

The investigation revealed multiple serious deficiencies:

- Users' personal data (including names, ID numbers, addresses, OIBs, and copies of ID cards) were stored and accessed without sufficient safeguards;
- Weak employee passwords, in some cases only three characters long, allowed potential access to mailboxes containing ID scans of thousands of users; employees accessed the administrative platform via insecure HTTP connections;
- The controller failed to delete personal data after the legally required retention period, breaching Article 5(1)(e) GDPR (storage limitation); and
- The company refused to implement data backups, citing cost, despite processing data of over 70,000 users; this further violated its duty to ensure data integrity and availability under Article 32 GDPR.

AZOP concluded that the betting operator had systematically neglected data protection obligations and prioritized cost-saving over compliance.

Parking operator fined €80,000 for unlawful processing of vehicle owner data

AZOP imposed an administrative fine of €80,000 on a private company managing parking services for the unlawful processing of personal data of vehicle owners obtained from the Ministry of the Interior (MUP) database without a valid legal basis.

AZOP's investigation revealed that the company:

- Accessed and used personal data from the MUP Vehicle Register – originally obtained under an agreement allowing access for a different purpose and a different city;
- Used that data to collect parking fees for shopping centers and a general hospital, activities outside its authorized purpose;
- Had no valid legal basis under the GDPR;
- Did not conclude a data processing agreement with the hospital as required by the GDPR; and
- Failed to implement appropriate technical and organizational measures to secure the data.

The company had obtained a local government concession for on-street parking enforcement and based on that, an agreement with the Ministry of the Interior for limited data access. However, it misused those access rights for unrelated private contracts, thus engaging in unauthorized data processing.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

ICT company fined €50,000 for inadequate technical data protection measures

AZOP fined an information and communications technology (ICT) company €50,000 for failing to implement appropriate technical and organizational security measures to protect personal data, in breach of Article 32 GDPR.

The case originated from a data breach report submitted by the company after a hacker attack exposed users' personal data.

AZOP's investigation revealed that the company had not ensured adequate protection against unauthorized access, alteration, or destruction of data.

Once the attacker gained entry, they were able to move freely across the entire IT system, compromising all personal data stored on its servers.

Although the company acted promptly after detecting the breach, it was found to have multiple systemic weaknesses in the design and maintenance of its processing systems – including the absence of regular testing, evaluation, and risk assessment procedures.

AZOP concluded that the company's failure to maintain the confidentiality, integrity, availability, and resilience of its systems constituted a serious violation of GDPR security obligations, warranting the administrative fine.

AZOP marked European Data Protection Day with AI-focused conference and launch of "Olivia" GDPR compliance tool

On 28 January 2025, AZOP celebrated the 19th European Data Protection Day by organizing a national conference titled "What Does Artificial Intelligence Bring Us?", emphasizing both the opportunities and risks of AI development and use.

The interconnection between the GDPR and the EU Artificial Intelligence Act was highlighted, and it was noted that GDPR compliance is the foundation for developing AI that is ethical, lawful, and human-centric.

The conference gathered representatives of the Croatian government, Parliament, the European Commission, academia, and the private sector, who agreed that responsible AI governance requires cross-sector collaboration.

Speakers underlined that effective regulation should enable innovation while safeguarding fundamental rights and privacy. A panel discussion explored how AI systems routinely process vast amounts of personal data, making compliance with the GDPR essential throughout all stages of AI system design, testing, and deployment. Panelists emphasized the need for transparent, accountable, and human-controlled AI systems that uphold democratic values.

In line with the AI Act, AZOP also announced preparations for establishing a national AI regulatory sandbox by August 2026 – a controlled environment to safely test innovative AI solutions under regulatory supervision.

AZOP also presented "Olivia," a free web-based GDPR compliance platform developed under the EU co-funded ARC II project. Olivia is specifically designed to help small and medium-sized enterprises (SMEs) understand and meet their GDPR obligations. The platform combines: educational modules on key GDPR topics and compliance principles; practical templates for privacy documentation and security policies; and knowledge tests and certificates to strengthen internal awareness.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

New Cybersecurity Regulation

On 21 November 2024, Croatia adopted the Cybersecurity Regulation (the Regulation) based on the Cybersecurity Act.

The Regulation represents a key step in transposing the EU NIS2 Directive into Croatian law.

The Regulation establishes:

- Criteria for classifying entities (key and important) under cybersecurity requirements and for maintaining a national register of entities;
- National risk management measures, including 13 specific cyber risk control measures, each detailing goals, sub-measures, IT/OT applicability, and implementation levels;
- Procedures for self-assessment of cybersecurity maturity, incident notification, and information exchange between national authorities;
- Obligations for both public and private entities to provide data for classification and maintain designated contact points for cybersecurity communication; and
- Three levels of cybersecurity maturity (basic, intermediate, and advanced) tied to assessed national cyber risk levels.

The Regulation designates the Security and Intelligence Agency (SOA) as the authority maintaining the national cybersecurity register, and the central state body for cybersecurity as responsible for developing national risk assessments and implementation guidelines.

Secondary acts and guidelines to implement the Cybersecurity Act and Regulation

Throughout 2025, Croatia adopted and published a series of bylaws and technical guidelines to operationalize the Cybersecurity Act and the Cybersecurity Regulation ensuring effective implementation of the national cybersecurity framework in line with the EU NIS2 Directive.

Key developments include:

- National Taxonomy of Cybersecurity Incidents: Introduces a standardized national framework for the consistent classification, recording, and information exchange of cybersecurity incidents.
- General Guidelines on Reporting Significant Cybersecurity Incidents: Define structured procedures and reporting templates for notifying significant incidents to the competent authorities.
- Guidelines on Cyber Risk Management for Categorized Entities: Provide practical support for key and important entities in implementing comprehensive risk management processes, including risk identification, assessment, mitigation, monitoring, and continuous improvement for network and information systems.
- Guidelines for Correlation Review of Cybersecurity Measures: Offer a reference framework that correlates national cybersecurity measures with international standards and best practices, enabling entities to ensure alignment and interoperability with globally recognized security frameworks.
- Security Certification Rules for Cybersecurity Audits: Establish a national certification framework for managed security service providers authorized to perform cybersecurity audits, requiring providers to hold a national or EU-recognized security certificate.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cybersecurity Exercise Implementation Plan through 2027

On 26 September 2025, the Government of the Republic of Croatia adopted the Cybersecurity Exercise Implementation Plan for the period until 2027, in accordance with the Cybersecurity Act.

The plan establishes a comprehensive schedule of national and international cybersecurity exercises for 2025-2026, aimed at strengthening national capabilities, testing procedures and communication tools, and enhancing coordination and crisis response mechanisms across public institutions and critical infrastructure operators.

It includes:

- Four national exercises focused on technical, procedural, and strategic readiness of public bodies and educational institutions; and
- Five international exercises conducted with ENISA, NATO, and other EU partners to test cross-border crisis management and defense coordination.

Participating institutions are required to prepare post-exercise analyses and reports identifying lessons learned and areas for improvement, which are submitted to the National Cybersecurity Center (NCSC-HR) within the Security and Intelligence Agency (SOA).

Categorization of entities under the Croatian Cybersecurity Act

In September 2025, Croatian authorities responsible for implementing the Cybersecurity Act completed the initial categorization process of entities subject to cybersecurity obligations.

As of Q3 2025, 713 entities have been categorized: 125 key entities and 588 important entities. These organizations have begun implementing cybersecurity measures and reporting incidents in line with requirements.

All categorized entities across relevant sectors have been notified by their competent authorities and received guidelines on further compliance steps.

Organizations operating in listed sectors listed, which believe they meet the criteria but have not yet received categorization notices, are invited to contact the relevant competent authority.

In October 2025, the NCSC-HR also issued a call for voluntary implementation of cybersecurity measures for noncategorized legal entities.

This voluntary initiative targets:

- Noncategorized private sector entities operating in the sectors covered by the Act; and
- Public sector bodies not falling under mandatory categorization.

Interested organizations are encouraged to apply, providing basic company data and an overview of their IT infrastructure and services.

Together, these measures mark a significant milestone in the nationwide rollout of Croatia's new cybersecurity framework, ensuring broad participation and preparedness across both mandatory and voluntary sectors, and supporting the gradual alignment with the EU NIS2 Directive.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Designation of competent authorities under the EU Artificial Intelligence Act

In October 2024, the Ministry of Justice, Administration and Digital Transformation of Croatia submitted to the European Commission the official list of competent authorities designated under Regulation (EU) 2024/1689 – the Artificial Intelligence Act (AI Act).

Under Article 77(2) of the AI Act, EU member states were required to designate and publish the public authorities responsible for monitoring and enforcing obligations related to the protection of fundamental rights in connection with the use of high-risk AI systems.

Croatia has designated the following bodies:

- Ombudsperson;
- Ombudsperson for Children;
- Ombudsperson for Gender Equality;
- Ombudsperson for Persons with Disabilities;
- Croatian Personal Data Protection Agency (AZOP); and
- State Electoral Commission Agency for Electronic Media.

While these authorities have been formally designated, their specific supervisory and enforcement roles under the AI Act are yet to be defined. Further details are expected once the implementation framework is adopted.

Croatia has not yet designated the national competent authorities required by Article 70, specifically the Market Surveillance Authority and the Notifying Authority.

Preparatory Phase for the Croatian Law Implementing the EU Artificial Intelligence Act

In 2025, the Ministry of Justice, Public Administration and Digital Transformation initiated a public consultation on the Legislative Activity Form for the forthcoming Law on the Implementation of the EU AI Act.

This consultation marks the preparatory phase before the drafting and adoption of the full implementing law.

The proposal is currently under governmental procedure, with the public consultation planned for the third quarter of 2025.

The next steps include drafting the legislative text and its submission to the Croatian Parliament for adoption.

According to the explanatory notes of the Legislative Activity Form, the proposed law will aim to:

- Ensure the implementation of the EU AI Act by establishing the legal framework for the development, placing on the market, and use of reliable and safe artificial intelligence systems within the EU.
- Improve the functioning of the EU internal market through a harmonized regulatory framework for AI systems, promoting anthropocentric and trustworthy AI that guarantees a high level of protection of health, safety, and fundamental rights, in line with the EU Charter of Fundamental Rights.
- Support innovation and the free cross-border movement of AI-based goods and services by preventing Member States from imposing disproportionate national restrictions on AI development and deployment, unless expressly allowed under the regulation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Croatia begins drafting National Artificial Intelligence Development Plan 2032 and accompanying 2026-2028 Action Plan

In May 2025, the Minister of Justice, Administration and Digital Transformation presented the Decision to initiate the drafting of the National Artificial Intelligence Development Plan (to 2032) and the related Action Plan for 2026-2028.

Under this decision, the Ministry of Justice, Administration and Digital Transformation is tasked with preparing both documents, which will be based on three strategic pillars:

- Formulating and implementing public policies in the field of AI;
- Encouraging investment in the AI sector; and
- Creating conditions for the effective application of AI across society and the economy.

The National Plan will cover key thematic areas such as education and AI skills development, digital transformation, economic and industrial growth, promotion of research, innovation and start-ups, and the protection of citizens' privacy and security.

The minister stressed the importance of balancing innovation and technological progress with safety and data protection.

The working group responsible for drafting the plans will include not only the existing AI Act transposition team, but also representatives of the academic community, the private sector, and experts from ministries and other state bodies, ensuring a comprehensive, cross-sectoral approach to shaping Croatia's long-term AI development strategy.

Criminal offence for AI-related endangerment

Croatia is proposing amendments to its Criminal Code that, for the first time, introduce a new criminal offence related to artificial intelligence.

The offence, titled "endangering life, property or bodily integrity through an AI system," aims to address risks arising from rapidly developing technologies.

The legal definition of an AI system is taken directly from the EU AI Act to ensure full alignment with European law.

The Ministry of Justice, Public Administration and Digital Transformation emphasized that the provision is intentionally broad, anticipating future technological developments and the need for further updates.

These amendments form part of a wider legislative package intended to modernize Croatia's criminal law framework and respond to new EU obligations, particularly in the areas of technology-related risks, organized crime and procedural efficiency.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

- AZOP is expected to intensify its enforcement activities, continuing its trend of stronger supervision and the imposition of administrative fines, particularly in sectors with recurring compliance issues.
- Closer alignment between the GDPR and the AI Act is anticipated. AZOP has emphasized the complementarity of both frameworks, and it is expected that the Agency will issue guidance and opinions on the application of the GDPR in the context of AI.

Cybersecurity

- The operational rollout of the Cybersecurity Regulation continues, with all entities classified under the Cybersecurity Act expected to conduct self-assessments, report significant incidents, and implement robust technical and organizational measures to enhance resilience.
- The implementation of the national plan of cybersecurity exercises for 2025-2027 will introduce a structured program of national and international drills designed to test readiness, strengthen incident response capabilities and improve cross-institutional communication.
- Ransomware remains the most serious short-term threat to government and critical sectors. Progressive implementation of Cybersecurity Act measures is expected to improve the resilience of categorized entities.

AI

- The drafting and adoption of a national implementation law for the AI Act is underway, with the proposal progressing through governmental procedure and expected to provide the core legal framework for Croatia's AI governance regime.
- The development of a comprehensive national AI strategy is anticipated to set clear policy, investment and deployment priorities, ensuring Croatia's long-term alignment with the AI Act and EU digital objectives.
- The establishment of AI regulatory sandboxes is anticipated to create controlled testing environments for AI systems, particularly high-risk ones, enabling safe innovation, accelerating market readiness and supporting responsible technological development.
- The designation and operationalization of national competent authorities for the AI Act will form a central pillar of Croatia's implementation architecture, ensuring effective oversight, enforcement and coordination in line with EU requirements.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Czech Republic

Contacts

Jaroslava Kračúnová

Partner, Deloitte Legal Czechia

jkracunova@deloitteCE.com

Edita Bolková

Senior Associate, Deloitte Legal Czechia

ebolkova@deloitteCE.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Czech Office for Personal Data Protection celebrates 25 years of activity

The Czech Office for Personal Data Protection (the Office) is commemorating its 25th anniversary of supervising compliance with personal data protection laws in the Czech Republic. Established by Act No. 101/2000 Sb. on 1 June 2000, the Office has evolved from modest beginnings into an institution with significant regulatory responsibilities within the country's governance framework.

Over the years, additional key pillars of its activities have been added – participation in eGovernment through operating the ORG information system and especially the agenda of free access to information. According to the current chairman, Jiří Kaucký, the Office's role in protecting privacy has never been more important as society has moved from paper forms and analog video cameras to a digital world of hybrid wars, mass identity theft, artificial intelligence, and attempted manipulation of public opinion.

In 2025, the Office addresses key personal data protection challenges across both public and private sectors. Priority inspections include monitoring the use of data from public administration registers by private entities, such as banks, examining loyalty programs where discounts depend on consent with processing personal data, and reviewing data handling in freedom of information request procedures. The Office will also focus on camera systems in public transportation vehicles and commercial communication practices by online comparison platforms.

Czech Office for Personal Data Protection warns against email invoice “catalog” scams

The Czech Office for Personal Data Protection issued a warning about companies that send invoices via email demanding payment for allegedly ordered services. This practice constitutes what is known as a "catalog scam," a deceptive business practice aimed at tricking business entities into unintentionally entering into a contractual relationship by misleading them and subsequently exploiting this confusion for fraudulent enrichment.

The Office strongly advises companies and individual entrepreneurs who receive such communications not to pay these invoices. Such conduct can be considered an offense under Act No. 480/2004 Coll. on certain information society services, as amended, and may potentially amount to a criminal offence. The Office has received several hundred complaints from business entities, all stating they never ordered any services from the sending companies. The accused companies defended themselves by claiming they obtained contact information for business entities from publicly published company directories.

However, the Office clearly states that commercial communications may only be sent after obtaining prior consent from the recipient or based on an existing customer relationship, and publicly available catalogs cannot be used for sending commercial communications to contacts listed in them. The Office considered it a highly aggressive practice when companies not only sent proforma invoices but also various payment reminders, information about unpaid invoices or due dates, and even notices about debt collection and violation of general business terms.

For these catalog scams involving the distribution of unsolicited commercial communications containing proforma invoices for unordered services, the Office imposed fines on three totaling more than 5 million CZK. All these fines are now final, and investigations into additional companies are currently being conducted by the Office.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Recommendation on the use of camera systems in schools

The Czech Office for Personal Data Protection issued Recommendation No. 1/2025 regarding the use of camera systems in schools and educational facilities. The guidance follows public consultation and builds on the general methodology for deploying and operating camera systems. It responds to the need for more detailed rules in settings where children and young people spend a significant part of their daily lives, and where the impact on privacy can be particularly sensitive.

The recommendation outlines when and how camera systems may be justified, mainly for property protection or evidence purposes, while stressing that surveillance should not disproportionately intrude on privacy. It discourages the use of cameras for monitoring issues such as bullying, given limited effectiveness, and calls for a balancing test to weigh legitimate interests against fundamental rights. The document highlights factors such as camera placement, scope of footage, storage duration, and use of advanced technologies, encouraging schools to consider less intrusive alternatives and ensure compliance with GDPR principles.

New camera surveillance regulations in healthcare facilities

The Czech Ministry of Health has prepared an amendment to Decree No. 92/2012 Coll. that introduces regulations for camera systems in healthcare facilities, addressing a previously specifically unregulated area. The amendment, effective January 2026, requires camera systems to enable two-way audio-visual transmission, feature on/off mechanisms, display camera status indicators, and secure feeds against unauthorized access. The new rules prohibit surveillance in sanitary facilities and mandate clear marking of monitored areas. Healthcare providers will have until 31 December 2026, to bring their existing camera systems into compliance, while any newly installed systems must comply as of January 2026. This regulation aims to balance patient safety with privacy protection, responding to concerns raised by the Public Defender of Rights regarding excessive monitoring in medical facilities.

The Czech Office for Personal Data Protection and the Office for the Protection of Competition signed a memorandum of mutual cooperation

On 13 March 2025, Jiří Kaucký, Chairman of the Czech Office for Personal Data Protection, and Petr Mlsna, Chairman of the Office for the Protection of Competition, signed a memorandum of cooperation focused on digital services. The two authorities will jointly organize workshops and training sessions on new business models, artificial intelligence, and data use, while also sharing expert consultations and support in cases overlapping both data protection and competition law.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

NÚKIB and intelligence services warn of Russian cyber campaign against Ukraine supporters

The Czech National Cyber and Information Security Agency (NÚKIB), together with Czech intelligence services and partners from the United States, the United Kingdom, Germany, Poland, Australia, Canada, Denmark, Estonia, France, and the Netherlands, issued a joint cybersecurity advisory on 21 May 2025 warning about a long-term cyber campaign conducted by Russian-supported actors. These attacks specifically target logistics and technology companies involved in foreign aid to Ukraine.

The campaign is attributed to Unit 26165 of Russian military intelligence (GRU), known as APT28 (also Fancy Bear or Forrest Blizzard), which has been conducting espionage operations against defense and transportation sectors for more than two years. The attackers employ tactics such as password spraying, targeted phishing emails, changes to email box settings in Microsoft Exchange environments, and exploitation of vulnerabilities in software like Outlook (NTLM) or WinRAR. They have also actively monitored aid shipments to Ukraine by accessing IP cameras at border crossings, railway hubs, and other strategic points.

The advisory warns that these activities will likely continue, urging technology, logistics, and transportation organizations to strengthen monitoring, actively hunt for signs of compromise, and implement appropriate protective measures against these sophisticated threats.

Czech government approves new national cybersecurity strategy

The Czech government approved a new National Cybersecurity Strategy (NSKB) effective from 2026, which sets long-term priorities and goals for the state in this area. The strategy replaces the previous document from 2021 and responds to the deteriorating global security situation and technological changes of recent years, emphasizing the need for more intensive cooperation at both national and international levels.

The strategy, developed by the National Cyber and Information Security Agency (NÚKIB) with input from dozens of organizations from both public and private sectors and through public consultations, establishes three main strategic areas: secure strategic infrastructure, societal preparedness and development, and international cooperation and promotion of interests.

According to the strategy, the Czech Republic will need to more intensively use new technologies for organizational security, prepare for potential transitions to crisis situations, improve working conditions for cybersecurity experts in public administration, and develop alternative solutions to risky technologies, new platforms for information sharing, and an internationally coordinated position to deter malicious state actors.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

NÚKIB issues warning against data transfer and remote management from certain foreign countries or territories

The Czech National Cyber and Information Security Agency (NÚKIB) issued on 3 September 2025 a warning about cybersecurity threats related to the transfer of system and user data to certain foreign countries and remote management of technical assets from such jurisdictions. The warning must be addressed by entities obligated under the Cybersecurity Act.

NÚKIB derived the security threat from three key factors: the increasing share of complex technological solutions in critical sectors that transfer data to or are remotely managed from these jurisdictions; confirmed malicious activities by actors linked to certain states directed against the Czech Republic, the EU, and NATO; and the political and legal environments in some countries that enable government authorities to access data stored in their territories, significantly interfere with private companies' operations, or provides these authorities with tools to enforce cooperation from private firms in state-sponsored espionage activities.

The threat is assessed as "high" (probable to very probable), and while the warning does not unconditionally prohibit data transfers or remote management from these countries and territories, obligated entities must consider this threat in their risk analysis and respond with appropriate security measures.

NÚKIB releases report on the state of cybersecurity in the Czech Republic for 2024

On 22 August 2025, the National Cyber and Information Security Agency (NÚKIB) published its annual report on the state of cybersecurity in the Czech Republic for 2024. The agency recorded an all-time high of 268 cybersecurity incidents, though this represents only a slight increase from 2023. More significantly, the severity of incident impacts has decreased for the third consecutive year, with only one very significant incident and 18 significant incidents recorded in 2024 – more than 50% fewer significant incidents compared to the previous year.

Distributed denial-of-service (DDoS) attacks constituted a substantial portion of the recorded incidents, primarily attributed to certain hacktivist groups, especially NoName057(16), though these activities generally resulted only in short-term website outages. The report highlights new trends including an increase in hacktivist groups targeting poorly secured operational technology and SCADA systems in Western industrial enterprises.

Despite sophisticated campaigns by state actors comprising only a small percentage of total incidents, their severity is typically high. The report also notes a concerning spike in ransomware attacks in late 2024, with October recording a monthly high of seven attacks.

A positive development is the three-year trend of increased organizational cybersecurity budgets, though a shortage of qualified cybersecurity professionals remains problematic. The report also details NÚKIB's legislative progress with a new cybersecurity law set to take effect on 1 November 2025, and engagement in EU-level cybersecurity resilience regulations.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The Government of the Czech Republic approved the Action Plan of the National Artificial Intelligence Strategy of the Czech Republic for 2025

On 2 April 2025, the Czech government approved the Implementation Plan of the Digital Czechia program for 2025, which presents a collection of specific projects focused on supporting digitalization in the Czech Republic, including artificial intelligence. This plan is part of the Czech government's broader effort to increase the efficiency of state administration, public services, and improve citizens' quality of life through advanced digital technologies such as artificial intelligence.

The implementation plan incorporates project proposals from the Action Plan of the National Artificial Intelligence Strategy of the Czech Republic 2030 (NAIS) for 2025. The Ministry actively coordinates the implementation of projects within the Action Plan to create an environment that fosters innovation and technological development.

An important part of this effort will be strengthening cooperation with experts and companies in the field of artificial intelligence development, which will contribute to maintaining the Czech Republic's competitiveness on the international stage.

The NAIS Action Plan allocates 19 billion Czech crowns for project proposals. Under the approved plan, specific projects will be implemented focusing on the development and implementation of artificial intelligence in key areas, including AI in research, development and innovation, education and expertise in AI, AI skills and impacts on the labor market, ethical and legal aspects of AI, security aspects of AI, and AI in public administration and public services.

Czech government approves plan for implementation of EU AI Act with Ministry of Industry and Trade as new coordinator

On 28 May 2025, the Czech government approved a nonlegislative document addressing the national implementation of the EU AI Act, development of a national AI law, and creation of necessary supervisory infrastructure, with oversight transferring from Deputy Prime Minister Marian Jurečka to the Ministry of Industry and Trade. The government also appointed Deputy Minister Jan Kavalírek as AI Commissioner, with Minister Lukáš Vlček emphasizing AI's potential to position the Czech Republic among world leaders in advanced technologies, improving both business processes and public administration.

The ministry is making significant resource commitments, including creating an eight-person AI department and allocating 24 million Czech crowns from its budget for implementation. Multiple authorities will oversee rule enforcement, including the Czech Telecommunication Office, Standards and Metrology Office, Personal Data Protection Office, Czech National Bank, Standardization Agency, and Public Defender of Rights. A regulatory sandbox will allow businesses and researchers to test innovative AI solutions in a controlled environment. With the AI Act coming into force in August 2026, timely implementation is crucial to avoid potential EU sanctions.

However, as the government is currently undergoing a change, it remains uncertain whether the plan will ultimately be implemented in its present form.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

The new EU Regulation (EU) 2024/900 on the transparency and targeting of political advertising, together with national law No. 234/2025 Coll., will become effective from October 2025. The legislation seeks to strengthen trust in democratic processes by ensuring that political advertisements are clearly identifiable and include information about their sponsors, campaign context, and targeting methods. It also introduces strict data protection safeguards, allowing personal data to be used for political advertising only with explicit consent, prohibiting the use of sensitive data, and banning targeting of minors.

The Office for Personal Data Protection (ÚOOÚ) will oversee compliance with these rules, establish supervisory practices, and cooperate with EU institutions to ensure transparent, fair, and responsible handling of political advertising, particularly in the online environment.

Cybersecurity

The Czech cybersecurity landscape in the coming year will be primarily shaped by the gradual implementation of the new Cybersecurity Act and subsequent decrees, which have transposed the EU's NIS2 Directive and took effect on 1 November 2025. Starting on 1 November 2025, organizations have 60 days to register their regulated services through the portal of the Czech National Cybersecurity Agency.

The new legislation expands the scope of entities subject to cybersecurity requirements compared to the current law (Act No. 181/2014 Coll.). Organizations should expect adjustments to compliance obligations, including enhanced security measures and revised incident reporting procedures. This regulatory development coincides with ongoing cybersecurity challenges such as ransomware threats and the continuing shortage of qualified professionals, though many organizations have already been progressively increasing their security investments over recent years.

The implementation will be supported by the newly approved National Cybersecurity Strategy for 2026-2030, which provides a balanced framework for improving infrastructure security, societal readiness, and international cooperation.

AI

The Czech Republic is expected to advance the implementation of the EU Artificial Intelligence Act through a minimalist national adaptation law prepared by the Ministry of Industry and Trade (MPO). The proposal, currently undergoing interdepartmental consultation, focuses on ensuring user safety while fostering innovation and minimizing administrative burdens for businesses. The law, consisting of just ten pages, will fine-tune only the essential provisions of the EU regulation, aiming to create a pro-innovation environment and strengthen the competitiveness of Czech companies.

In the coming year, the Czech government plans to finalize and submit the bill to Parliament, set up the necessary supervisory structures, and establish a national regulatory sandbox to allow firms and startups to safely test AI applications before market launch. Oversight will be shared among several institutions, including the Czech Telecommunication Office, the Czech National Bank, and the Office for Personal Data Protection. Through these measures, the Czech Republic aims to position itself among the EU’s top 10 countries in AI readiness and regulation, preparing for the law’s expected entry into force in 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Denmark

Contacts

Jeanette Vallat

Partner, Deloitte Legal Denmark

jvallat@deloitte.dk

Simone Mai Flindt

Manager, Deloitte Legal Denmark

smpetersen@deloitte.dk

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Decision of the Danish Western High Court (in Danish: Vestre Landsret) regarding breach of personal data retention obligations

ILVA

On 2 September 2025, the Danish Western High Court ruled that ILVA A/S was liable to pay a fine of DKK 1.5 million for breaching data protection regulations concerning the retention of personal data. This judgment represents a landmark decision, as it establishes a new approach to the calculation of fines under the GDPR.

The central issue in the case concerned the basis for calculating the fine, specifically whether it should be determined by reference to the company's individual revenue or the group's total worldwide annual turnover for the preceding financial year. In 2021, the City Court ruled that the fine should be based on ILVA's own revenue, resulting in a penalty of DKK 100,000.

However, the case was subsequently appealed to the High Court, which referred questions to the CJEU concerning the interpretation of the term "undertaking" as defined in Article 83 of the GDPR (Case C-383/23). The CJEU held that the term "undertaking" must be construed in accordance with competition law principles and the definitions provided in Articles 101 and 102 TFEU. Consequently, the amount of the fine is to be determined on the basis of the undertaking's total worldwide annual turnover in the preceding financial year.

In accordance with the CJEU's ruling, the High Court subsequently increased ILVA's fine to DKK 1.5 million, basing the calculation on the annual turnover of the Lars Larsen Group.

This ruling is of particular significance for companies, as it establishes that the level of fines for breaches of data protection regulations is to be determined on the basis of the group's total worldwide annual turnover rather than solely on the revenue of the individual legal entity.

The Data Protection Agency (Datatilsynet) and Agency for Digital Government (Digitaliseringsstyrelsen) have published a joint guideline regarding the use of cookies and similar technologies

Guidance for compliance with the Cookie Statutory Order and General Data Protection Regulation

The guideline is addressed to the owners and providers of, inter alia, websites and apps. The guidelines examines the legal requirements established under the Danish Cookie Statutory Order and the General Data Protection Regulation (GDPR), whilst providing practical guidance and concrete examples to ensure compliance with the requirements. Further, it addresses some common issues to be aware of.

Updated guideline from the Danish Data Protection Agency (Datatilsynet) concerning handling of data breaches

In continuation of the input provided in the previous year, the Danish Data Protection Agency has updated the remaining sections of the guideline, including those addressing reporting obligations to the Data Protection Agency and the notification of affected data subjects.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

The Danish NIS2 Act has entered into force

Denmark has completed the implementation of the Network and Information Security Directive 2 (NIS2)

As of 1 July 2025, the NIS2 Act is effective in Denmark, introducing enhanced cybersecurity requirements, encompassing risk management, incident response procedures, and supply chain security measures. The Danish Emergency Management Agency (Styrelsen for Samfundssikkerhed) has published guidelines for compliance with the regulation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The Agency for Digital Government (Digitaliseringsstyrelsen) has published a so-called “Guidance Package” regarding prohibited use of AI

Pursuant to the AI Act, the initial provisions entered into force on 2 February 2025, establishing prohibitions on certain use of AI. The Agency for Digital Government has accordingly prepared a comprehensive guidance package to support compliance. The guidance package can be accessed via the links below:

- Main Guidance on Prohibited Forms of AI Practices under Article 5 of the AI Act
- Guidance on the Prohibition of AI Using Harmful Manipulative Techniques
- Guidance on the Prohibition of AI Exploiting Specific Vulnerabilities
- Guidance on the Prohibition of AI Conducting Social Scoring
- Guidance on the Prohibition of AI Conducting Non-Targeted Collection of Facial Images
- Guidance on the Prohibition of AI Inferring Emotions in Workplaces and Educational Institutions

The Agency for Digital Government (Digitaliseringsstyrelsen) has been designated as supervisory authority for the AI Act

Accordingly, the Danish Agency for Digital Government, the Data Protection Agency (Datatilsynet) and the Courts Administration (Domstolsstyrelsen) share a joint supervisory responsibility related to the AI Act.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Appealed ruling on compensation for breach of the GDPR

On 20 August 2025, a ruling was rendered concerning compensation under Article 82 of the GDPR, after a municipality mistakenly shared a citizen's health information with a third party. The ruling has been appealed to the Danish Supreme Court (Højesteret), and if the ruling is upheld, there will be a shift in practice.

Additional guidelines for private companies' use of AI

Following the completion of the regulatory AI sandbox projects with the involvement of the Danish Data Protection Agency (Datatilsynet), additional guidance material from the agency is expected.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

El Salvador

Contacts

Estuardo Paganini

Partner, Deloitte Legal El Salvador

egpaganini@deloitte.com

Rita Camila Vega

Manager, Deloitte Legal El Salvador

ritvega@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Law on promotion of AI and technologies

The Personal Data Protection Law came into effect on 23 November 2024.

This law aims to guarantee the right to privacy and informational self-determination and regulates the legitimate and informed processing of personal data. Its scope of application includes all natural and legal persons, whether public or private, who carry out activities related to or connected with the processing of personal data.

Among the principles governing this law are the principles of data accuracy, loyalty, consent and purpose limitation, data minimization, transparency, data security, and lawfulness, among others.

ARCO-POL rights

These are the highly personal and independent rights of access, rectification, cancellation, opposition, portability, erasure and limitation; through which the holders can exercise control over the processing of their data.

The main requirements of the obligated parties with respect to this law are listed as follows:

- Guarantee data subjects the exercise of their ARCO-POL rights;
- Appoint a data protection officer;
- Guarantee data subjects' access to information within the legal timeframes;
- Have a privacy notice, whether physical, electronic, or digital, to inform data subjects of the terms under which their personal data will be processed;
- Maintain security measures and apply technological, regulatory, and procedural mechanisms that guarantee security, as well as notify data subjects of personal data security breaches within a maximum of 72 hours;
- Obtain the prior consent of data subjects, especially for sensitive personal data; and
- Process personal data only for the purposes previously informed and with direct relationship with the nature of the services to be provided.

Supervisory entity

The Cybersecurity Agency (ACE) will be responsible for controlling, inspecting, supervising and exercising sanctioning power in matters of personal data protection.

From the first three months of its implementation (until February 2025), the ACE must issue the policies, measures, guidelines, or provisions necessary for the application of the law, so that, three months after its issuance (March to May 2025), the obligated parties can adapt and implement the regulations. This means that the obligations should be fulfilled by approximately the end of May 2025; however, this will depend on the ACE.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cybersecurity and Information Security Law

This law came into effect on 23 November 2024.

Compliance with this law is mandatory for government bodies, their agencies, autonomous official institutions, municipal authorities, as well as any other entity or organization, regardless of its form, nature, or legal status, through which public resources or state assets are managed, acts of public administration are carried out in general, or that have an impact on the nation's critical infrastructure.

State Cybersecurity Agency

Through this law, the State Cybersecurity Agency (ACE) was created, which will have the following responsibilities:

- Draft the National Cybersecurity and Information Security Policy, which will include the guidelines, plans, and action programs to be applied for its compliance, and submit it for approval by the president;
- Create and implement the necessary action programs to respond to cybersecurity and information security threats or incidents involving obligated parties; and
- Monitor and review the cybersecurity and information security measures and actions implemented by obligated parties, to establish mechanisms for improvement and risk prevention; among others.

Infractions and penalties

The law classifies infractions as minor, serious, or very serious.

- Minor infractions will result in a written warning or a fine ranging from one to 10 monthly minimum wages.
- Serious infractions will result in dismissal or removal from office, along with a fine ranging from 11 to 50 monthly minimum wages.
- Very serious infractions will result in dismissal or removal from office, along with a fine ranging from 50 to 100 monthly minimum wages.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Law for the Promotion of Artificial Intelligence and Technologies

This law has been in force since 12 March 2025, and aims to contribute to the country's technological advancement and economic growth by promoting the development, research, and application of artificial intelligence or similar technologies.

The provisions of this law apply to any natural or legal person, regardless of the latter's nature, degree of autonomy, or incorporation regime, that engages in activities or provides services related to the development, research, and application of technologies related to AI, machine learning, generative models, and similar technologies, as well as those who carry out or participate in the collection, storage, processing, and application of data for the aforementioned activities.

National Artificial Intelligence Agency

This law creates the National Artificial Intelligence Agency (ANIA), which will be responsible for:

- Coordinating and supervising compliance by obligated parties with the obligations established in the law, in order to report to the relevant regulatory institutions, if any;
- Establishing technical assistance programs and training for the general population regarding the activities contemplated in the law; and
- Coordinating state activities to promote the development, research, and application of AI and similar technologies, among others.

National Registry for AI Development, Innovation, and Application

Entities that carry out activities using open-domain or proprietary data and whose projects are not intended for commercial purposes or for public use must register.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

France

Contacts

Benjamin Balensi

Partner, Deloitte Legal France

bbalensi@avocats.deloitte.fr

Tony Baudot

Director, Deloitte Legal France

tbaudot@avocats.deloitte.fr

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Regulation of cookies

On 1 September 2025, the CNIL (French Data Protection Authority) has fined Google €325 million and Shein €150 million, notably for failing to comply with rules regarding trackers.

These fines are part of the ongoing actions led by the CNIL to regulate noncompliant practices related to the tracking and targeting of internet users. The CNIL pays attention to noncompliant practices such as placing trackers (i.e., cookies) without the user's consent, as well as emerging practices like the use of "cookie pay walls."

Regarding this practice, the restricted formation (enforcement committee of the CNIL) reminded in its decision against Google that, while cookie walls are not inherently illegal, they are only permissible if **consent is freely given**. This means that all alternatives offered to users must be presented in a balanced way, without nudging them towards one option over another (for example, by making one choice more complicated than the other).

Additionally, as in a recent decision against Orange (14 November 2024), the enforcement committee also found Google to have violated Article L. 34-5 of the French Postal and Electronic Communications Code for displaying advertising messages in the form of emails within Gmail (in the "Promotions" and "Social" tabs) without obtaining prior user consent.

The two fines issued against Google and Shein by the restricted committee – the CNIL body responsible for imposing sanctions – are part of the CNIL's broader compliance strategy regarding trackers, which has been underway for more than five years. This strategy specifically targets operators of highly visited websites and services.

Data brokers

The CNIL pronounced sanctions for soliciting prospects without their consent and for transmitting their data to partners without a valid legal basis.

As part of its priority control theme on commercial prospecting, the CNIL focused on the practices of professionals in the sector, particularly those who resell data, including the many intermediaries in this ecosystem known as data brokers.

The CNIL inspected a company which acquires prospect data mainly from data brokers, contest website publishers, and product testing sites and uses this data to contact the individuals concerned by SMS or email on behalf of its advertiser clients. It may also transmit some of this data to its clients so that they can carry out prospecting themselves by phone or by post.

Based on the findings made during the inspection, the CNIL considered that the company had **failed to meet its obligations under the French Postal and Electronic Communications Code and the GDPR regarding the collection and proof of consent**. It imposed, on 15 May 2025, a fine of €900,000, made public; and an order to cease carrying out electronic commercial prospecting operations without valid consent.

The amount of this fine takes into account, in particular, the very large number of people concerned (several million), the company's long-standing position in the market, the financial benefit derived from the violations, as well as the measures the company has taken since the inspections to comply with some of its obligations.

The CNIL has imposed other sanctions on such companies on the same date.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Pixel trackers

The CNIL has launched in June 2025 a public consultation on its draft recommendation concerning the use of tracking pixels in emails.

Tracking pixels (also known as "tracking pixels" in English) are an alternative tracking method to trackers/cookies. They take the form of a one pixel by one pixel image, embedded in a website or an email, but are invisible to the user. When this image is loaded, its filename contains a user identifier, which allows the tracker to know that the tracked user has visited a page or read an email.

The goal of this recommendation would be to help stakeholders who use these trackers to better understand their obligations, particularly regarding the collection of user consent. It complements the guidelines and recommendation on "cookies and other trackers" by specifying how these rules apply to tracking pixels in emails, due to the specific technical and practical characteristics of this environment.

In this draft recommendation, the CNIL establishes that:

- Some purposes are subject to the user's prior consent such as individual assessment and analysis of emails to assess the performance of campaigns, creating profiles of recipients based on their expressed preferences and interests, detecting and analyzing suspected fraud, etc.
- Some purposes can be exempt from consent such as implementing user authentication security measures (in this context, the use of tracking pixels may serve the sole purpose of helping to secure authentication (for example, by ensuring that an email containing a password reset link is opened on a device known to belong to the intended user), measuring the overall email open rate, etc.).

Digital death, uses and issues of post-mortem data

The CNIL's Innovation Lab (LINC) published a report on digital death.

The GDPR does not apply to the data of deceased individuals. However, French law (loi informatique et libertés) allows people to decide what happens to their personal data after death. Two types of instructions are possible:

- General instructions: Like a data will, registered with a trusted third party and changeable at any time; and
- Specific instructions: For a particular service, sent directly to the provider and not based on general terms of use.

Through this report, the CNIL explores different aspects of digital legacies – from practices related to digital death, such as commemoration and grieving, to new possibilities enabled by the rise and spread of artificial intelligence systems.

Nowadays, some tools promise a digital afterlife or even digital immortality by allowing users to feed and train conversational agents with the data of the deceased. Sometimes called "deadbots," these tools claim to enable post-mortem interactions with lost loved ones.

This report provides an overview of current practices and explores ways to raise awareness about the legal and ethical issues surrounding post-mortem data.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Protection of minors

The CNIL has published different types of guidelines and documentation relating to the protection of the personal data of minor.

- Geolocation of children: Geolocation devices (AirTags, GPS trackers, smartwatches or connected toys, apps or built-in smartphone features, etc.) are sometimes used to track children. The CNIL highlights key points to be mindful of in order to protect their privacy such as keeping misuse in mind, minimizing the impact on the child's privacy, communicating with a child whenever their privacy is impacted and how to choose a geolocation device wisely.
- The CNIL and the AFCDP (the French Association of Data Protection Officers) have published a ready-to-use toolkit for offer companies and public administrations to distribute in the workplace. This toolkit provides parents with useful resources for managing digital technology and preventing cyber risks within the family.
- Video surveillance systems in schools: There are several types of video surveillance systems, but not all of them can be used in a school setting (i) **video protection cameras**: located outside of schools and require authorization, (ii) **video surveillance cameras**: installed inside a school and subject to specific provisions, and (iii) **"augmented" cameras**: which add software (artificial intelligence) to traditional camera systems and are not permitted within schools, unless a specific law authorizes it.
- Sharing information of children of social media which can be misused for malicious purposes and affect children in the long term.

Political elections and digital communications

The CNIL has published six practical guides on elections and political communication in the digital age, in line with Regulation 2024/900 which is fully applicable since 10 October 2025 and complements the GDPR by providing a framework for the growing use of digital tools in the political sphere.

The CNIL is designated as the competent authority by Regulation 2024/900 to ensure the application of certain articles (Articles 18 and 19 of the Regulation), which strictly regulate the use of personal data for political communication purposes. The practical guides published aim to inform candidates, parties, and citizens about the responsible use of personal data in political contexts, more specifically they address:

- Political communication tools, and detail the rules regarding the use of targeting techniques and distribution of political ads online, and the use of other political canvassing techniques, both online and offline;
- Political communication contact files and describe the regulations for creating contact files, such as for primary elections or party membership lists;
- The use of electoral lists for political communication;
- The files prohibited for political communication;
- The precautions needed when using files originating from private companies; and
- The responsibility of political actors in order to remind them of their obligations regarding data protection and responsible communication practices.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Ensuring the compliance of the annotation process and the security of AI system development

In its new recommendations, the CNIL offers practical solutions to ensure that using the model does not involve the processing of personal data, such as implementing robust filters at the level of the system encapsulating the model.

The CNIL has also published two practical guides regarding:

- Annotating data: The data annotation phase for training is crucial to guarantee the quality of the trained model and the protection of individuals' rights, while also developing more reliable and efficient AI systems.
- Ensuring the security of AI system development: The CNIL details the risks and measures to be considered during the development of an AI system to ensure that such systems are developed in a secure environment. In practice, for the development of an AI system – including the fine-tuning of a pretrained model used in the system – it is necessary to combine:
  - A "classic" security analysis (which focuses in particular on the security of the environment, including infrastructure, authorizations, backups, and physical security); and
  - The security of software development and maintenance (such as the implementation of development best practices, vulnerability management, and updates) with an analysis of risks specific to AI systems and large training databases.

The CNIL issues guidelines to strengthen the security of large databases

2024 was marked by an increase in massive data breaches, affecting several million people. The growing frequency of these incidents justifies the need to reinforce the security of processing operations involving large volumes of personal data.

The CNIL details the necessary measures to achieve this goal and draws the attention of data controllers to security measures that it considers generally required under Articles 5(1)(f) and 32 of the GDPR whenever large databases are involved, particularly in view of the risks of massive data exfiltration. These measures go beyond and strengthen basic security precautions. Furthermore, they must be adapted to the specific architecture of the data processing.

- **Secure external access to the information system through multi-factor authentication**: This type of measure should be part of a broader identity and access management policy that the organization must implement and maintain over time, according to the different user profiles (employees, service providers, developers, administrators, etc.).
- **Log, analyze, and set limits on data flows transiting through the information system**. To achieve this, the organization must have appropriate human resources and an adequate organizational structure in place to analyze alerts and respond to them as quickly as possible.
- **Consider humans as key actors in security**: Organize regular awareness and training sessions tailored to different user profiles (employees, developers, managers, subcontractors, etc.).
- **Supervise data security with subcontractors** and enter into a contracting agreement with each subcontractor.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Public consultation on web filtering gateway

The CNIL has submitted a draft recommendation for public consultation to support data controllers implementing web filtering gateways and their providers.

A web filtering gateway, often referred to as a web filtering proxy, is a device or service used to control and monitor internet access by filtering web content according to predefined policies. Its main role is to block access to certain websites or categories of content for security and compliance reasons.

These filtering solutions aim to address crucial cybersecurity challenges, notably by:

- Preventing access to illicit or inappropriate websites, whether they involve illegal content (child pornography, terrorism), fraudulent and malicious sites (phishing), or websites whose access is prohibited by the employer; and
- Preventing cyberattacks, particularly phishing or ransomware attacks, that could compromise the information systems security of data controllers.

To secure the web filtering solution and the access logging solution, the CNIL recommends:

- Regarding filtering: To limit the provider's ability to identify users of the filtering solution; and
- Regarding logging: To (i) ensure the administrators sign a strict confidentiality clause, (ii) store logs in an environment that ensures their security and confidentiality, (iii) restrict access to logs to duly authorized administrators, and (iv) implement multi-factor authentication for administrators accessing the solution.

Recommendation on multi-factor authentication

The CNIL has published a recommendation intended to support users and providers of multi-factor authentication solutions.

The purpose of this recommendation is to provide legal security for users of such solutions and to encourage providers to integrate privacy protection from the design stage of their products or services. This recommendation is specifically intended to guide data controllers on:

- The conditions under which the use of MFA (multi-factor authentication) is appropriate, considering security needs;
- Compliance with GDPR principles when using MFA, particularly the determination of a legal basis, minimization of collected data, retention periods, and respect for the exercise of rights by data subjects;
- Determining the qualification of the actors involved in an MFA solution;
- Choosing the appropriate methods (authentication factors: knowledge, possession, inherence) and their compliance with the GDPR; and
- Key considerations regarding the use of inherence factors, solutions based on sending a one-time code by SMS, or the use of employees' personal devices as a possession factor.

Organizations wishing to implement MFA, as well as providers of multi-factor authentication solutions themselves, must comply with certain rules, in particular those arising from the GDPR and any sector-specific regulations that may apply to them.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Development of AI systems: The CNIL publishes its recommendations on legitimate interest

Following a public consultation, the CNIL has published new recommendations on the development of artificial intelligence systems.

These recommendations clarify the conditions for relying on legitimate interest, particularly in cases of data harvesting (web scraping).

In line with the opinion adopted by the EDPB (European Data Protection Board) in December 2024, the CNIL considers that the development of AI systems does not systematically require individuals' consent. Legitimate interest can be a valid legal basis for developing AI systems, provided that strong safeguards are implemented.

In these recommendations, the CNIL helps stakeholders assess in which cases they can rely on this legal basis by providing criteria for analysis, including for the specific case of online data harvesting (web scraping).

The CNIL proposes concrete and tailored safeguards for different types of AI systems, such as excluding certain data from collection, increasing transparency, and facilitating the exercise of data subject rights.

The recommendations also give practical examples of data processing that may or may not be based on legitimate interest.

For example, reusing future user conversations from a chatbot to improve the AI model can be based on legitimate interest, provided that robust safeguards are in place: informing individuals, offering a discretionary right to object, limiting processing to certain pseudonymized or anonymized data, and so on.

AI systems in educational institutions

The CNIL has published two FAQs on the use of AI systems in educational institutions.

To support teachers and school administrators in integrating AI into schools, the CNIL provides two dedicated FAQs:

- One FAQ for teachers, focused on concrete pedagogical uses, best practices, and precautions to take in the classroom; and
- Another FAQ for data controllers (such as school principals, the ministry, and academic authorities), focused on legal obligations and compliance requirements.

AI and privacy: Objecting to the reuse of your personal data for training conversational agents

Without taking a position on the GDPR compliance of the methods offered, the CNIL explains how you can object to the reuse of your personal data by the main platforms of conversational agents.

More and more companies are using their users' personal data to train AI models. The CNIL identifies the technical methods for objecting to such processing on major platforms such as Gemini (Google), Meta AI (Meta), ChatGPT (Open AI), Copilot (Microsoft), Grok (X), DeepSeek, Le Chat (Mistral), Claude (Anthropic) and LinkedIn.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

"Augmented" cameras at self-checkout terminals

Some retailers wish to deploy augmented cameras to detect errors or attempted theft at self-checkout terminals. The CNIL has published two sets of recommendations: one to remind data controllers of the rules that must be followed to protect individuals' rights and one detailing the individual's rights in this regard.

Generally positioned above the self-checkout, these cameras film exclusively the checkout area, including the customer, their shopping basket and the items to be scanned, the scanning zone, and the area where products are placed after being scanned. The algorithm used can detect various "events" (for example, recognizing or tracking products, people's hands, or the position of a person relative to the checkout) in order to verify, in particular, that each product is actually scanned (as shown in the illustration below). Some systems can detect other anomalies or attempted fraud, which must be taken into account when analyzing the legality of the system. In the event of an anomaly, an alert can be displayed to allow the customer to correct themselves independently or to trigger intervention by an employee.

This type of system is generally not anonymous. It can be legally implemented, but it must comply with GDPR principles: establishing a legal basis, data minimization, informing individuals, limited retention periods, effective right to object, etc.

As a good practice, the CNIL recommends conducting a real-world pilot of the proposed system to ensure its effectiveness, legality, and minimal impact on individuals before any full-scale deployment.

"Augmented" cameras to estimate age: The CNIL clarifies its position

The CNIL considers that the use of "augmented" cameras to estimate the age of customers in tobacco shops, in order to control the sale of products prohibited to minors, is neither necessary nor proportionate.

Some shops use "augmented" camera systems to estimate the age of their customers before selling products prohibited to minors (such as tobacco, alcohol, gambling, etc.). These cameras rely on an artificial intelligence algorithm that scans a person's face to estimate whether they are a minor or an adult. These "augmented" cameras are currently used by tobacconists as a decision-support tool: they are not intended to allow customers to prove their age.

Facial analysis performed by so-called "augmented" cameras constitutes the processing of personal data, which must therefore comply with the principles established by the GDPR to be lawfully implemented. The CNIL conducted its analysis based on the following criteria:

- Processing must be necessary to achieve the intended objective: Indeed, since the "augmented" camera can only provide an estimate, fulfilling their obligations still requires tobacconists to systematically ask customers for proof of age. These tools are then not necessary and should be replaced by the checking of an ID or mini-wallet applications.
- Data processing must not unduly infringe on the rights and interests of individuals: The use of "augmented" cameras for age estimation poses significant risks to individuals' rights and freedoms since these systems operate continuously by default, filming and analyzing everyone in their view – including clearly adult customers – and prevent people from exercising their right to object.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Cookie pay walls and paying to access services without targeted advertising

The CNIL commissioned a survey to understand how French people perceive the use of their personal data and their consent to online advertising. This first part of a three-part series focuses on their willingness to pay to access services without targeted advertising.

Several types of services are affected by these questions: audio and video streaming, video games, social networks, press services, health and fitness tracking, as well as Generative AI.

To better understand the evolution of these business models, an online survey was conducted from 18-23 December 2024, with a representative sample of 2,082 French people aged 15 and over. The survey confirmed the growing popularity of paid subscriptions. However, it also shows that this option is not the preferred choice for those surveyed – even though the results vary significantly depending on the specific service. For example, the study reveals that more than half of French people (56%) pay for a video-on-demand subscription, with an average monthly cost of €20. This proportion drops when it comes to audio services (27%) or video games (18%).

The results also highlight the strong interest of the French citizens in protecting their personal data and confirm the relevance of the CNIL's approach: offering more options to enable users to better protect their privacy and ensuring that their preferences are respected. Further guidance is expected from the CNIL on this subject.

Upcoming recommendations on the responsibilities of actors in the AI value chain

In the second half of 2025, the CNIL will publish new recommendations to clarify the responsibilities of stakeholders involved in the creation of AI systems (such as model designers, hosting providers, re-users, integrators, etc.) with regard to the GDPR.

The main objectives of these recommendations will be (i) to clarify the consequences of applying the GDPR to models that are not anonymous, and (ii) to examine the case of open source, which is essential for the development of AI technologies. These recommendations will be subject to a public consultation in order to involve the entire community in the discussions.

AI and sectorial recommendations

AI and the health sector

A summary document outlining the rules applicable to the development of AI systems in the field of health, including concrete examples from authorization requests, the sandbox, or enhanced support, will be published soon.

AI and the work sector

The CNIL has initiated discussions with sector stakeholders (solution developers, employers using AI, unions, professional federations, public and scientific institutions, etc.) to clarify the regulatory framework for the use of AI in a professional context.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Germany

Contacts

Nikola Werry

Partner, Deloitte Legal Germany

nwerry@deloitte.de

Jan Rudolph

Counsel, Deloitte Legal Germany

jarudolph@deloitte.de

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Federal Data Protection Authority publishes questionnaire for AI tools

On 20 May 2025, the Federal Data Protection Authority has published a comprehensive questionnaire for ensuring the compliance of AI tools with applicable data protection law. Although meant primarily for entities under the supervision of the Federal Data Protection Authority, such as, e.g., federal administrative bodies and providers of telecommunications, this questionnaire may also serve as useful guidance for all entities considering the introduction and implementation of AI tools.

On 17 pages, the questionnaire contains detailed questions covering matters such as a general description of the tool, training and testing, the legal basis for data processing activities, contract management, confidentiality and data security. The questionnaire thus provides a useful tool for entities and serves as a general starting point for the assessment of tools and systems by the data protection officer and other relevant stakeholders.

Federal Data Protection Authority recognizes first web consent management tool

On 17 October 2025, the Federal Data Protection Authority has recognized the first web consent management tool to be in compliance with applicable data protection law, in particular, the ePrivacy Directive (Directive 2022/58/EC).

The management tool offers users a free plugin to be installed on their devices. By using the plugin, users can manage their consent over multiple devices and websites. Consequently, users installing and using the plug in no longer need to give individual consent when visiting a new website and/or service. This decision may give way to further facilitate web browsing and managing consent in a user-friendly manner.

Federal Data Protection Authority imposes fines on Vodafone GmbH

As announced in their press release on 3 June 2025, the Federal Data Protection Authority has imposed two fines on Vodafone GmbH, totaling €45 million, as well as issued a warning to Vodafone GmbH.

The first fine of €15 million was imposed due to a deficit in assessing and monitoring data processors as required by Article 28 paragraph 1 sentence 1 GDPR. The second fine of €30 million was imposed for gaps in the security of the user authentication process for “MeinVodafone” when used in combination with the Vodafone hotline. The exploitation of these gaps could potentially enable unauthorized third parties to, e.g., access eSIM profiles.

A warning was issued for security gaps in some distribution systems.

In response to the investigation, Vodafone GmbH has undertaken comprehensive measures to correct the identified matters. A subsequent assessment of the Federal Data Protection Authority is currently outstanding.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Data Protection Conference publishes guidelines on AI tools using retrieval augmented generation (RAG) and on TOMs for AI tools

As AI is becoming more and more important with regards to data protection, the German Data Protection Conference has recently published two guidelines on certain AI related aspects.

In June 2025, they published a guideline on technical and organizational measures to be considered in all lifecycles of an AI system, including the development and training phase. As such, the guideline complements the AI questionnaire published by the Federal Data Protection Officer by further detailing security considerations and requirements.

The second guideline was published in October 2025 and concerns the use of AI tools that implement retrieval augmented generation mechanisms. RAG systems as described by the guideline are AI systems that, after completion of their training, are used in a way that allows them to obtain access to information only available to the system user or operator, e.g., databases. This may influence the quality of output generated by the AI system in comparison to non-RAG systems. However, there are other data protection matters to consider when implementing RAG systems, e.g., concerning the correctness of outputs and the transparency of the system. In addition, compliance with the guideline on RAG systems does not guarantee a compliant system, in particular, where an LLM has been trained in a noncompliant manner.

Although there are additional RAG systems available, the guideline has put an initial focus on RAG systems working with embedding and vector databases. Additional guidelines may follow at a later point.

Federal Civil Court to present questions on the interpretation of Art. 82 GDPR to the ECJ

In its decision dated 28 August 2025, the Federal Civil Court has decided to present three questions on the interpretation of Article 82 GDPR to the ECJ.

In the underlying matter, the defendant had previously claimed damages from the claimant, alleging noncompliance with applicable data protection law due to the implementation of Google Fonts on the claimant's website. Prior to the claim, the defendant had used a web crawler to specifically search the web for websites using Google Fonts. When a website was identified accordingly, another program used by the defendant then automatically generated a visit to the website, triggering the alleged data processing activity. The defendant had then sent a reprimand to the claimant requesting €170 in turn for refraining from further measures. The defendant had sent out more than 100,000 letters with similar content and damage claims.

The claimant had originally paid the damages claimed by the defendant, however, later reclaimed the payment stating fraudulent conduct. In the first instance, the court ordered the defendant to repay €70 to the claimant, which was raised to the full €170 plus interest upon appeal of the claimant. The defendant has requested revision of the judgment by the Federal Civil Court, which has now requested a decision of the ECJ on the following questions:

- Is a dynamic IP address personal data in the sense Article 4(1) GDPR if only a third party has the required information to identify a data subject? Or is it necessary that either the controller sending the dynamic IP address or the recipient of the dynamic IP address hold the required information for reidentification and, if yes, what is the required quality of this information?
- Can damages arise if the event constituting an alleged breach of applicable data protection law has been caused by the claimant solely to raise a damage claim?
- If the answer to the second question is yes, can a damage claim be denied if the data subject is not acting in good faith? Is the intent of the data subject to be considered when adjudicating a damage claim under Article 82 GDPR?

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Federal Agency for Cybersecurity named as market surveillance authority under the Cyber Resilience Act

The federal government has officially named the Federal Agency for Cybersecurity (BSI) as the market surveillance authority under Article 36 paragraph 1 and Article 52 paragraph 2 Cyber Resilience Act.

As such, the Federal Agency for Cybersecurity is now authorized to notify conformity assessment bodies, which may then assess the compliance of products covered by the Cyber Resilience Act for conformity with the applicable requirements.

In addition, the Federal Agency for Cybersecurity may conduct assessments and investigations concerning covered products both proactively and upon information or notification of a third party and impose fines for noncompliance.

However, the Federal Agency for Cybersecurity has stressed that the exact form and extent of administrative powers as well as the necessary administrative procedural steps are still to be determined by a national law.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Federal government discusses centralization of data protection authorities

With a total of 18 data protection authorities covering both the public and the private sector, navigating data protection in Germany has often been found to be challenging. The new federal government, elected in February 2025, has therefore stated their intention to revise the current federal setup of data protection authority in the coalition contract and introduced the possibility of a centralized data protection authority.

According to available information, the centralized data protection authority would cover the whole private sector as well as federal administrative agencies. State data protection authorities would still remain; however, their supervision would be limited to administrative agencies of the respective state.

Discussions on this matter have been initiated, with a potential candidate for the centralized authority being the Federal Data Protection Authority, currently covering the federal administrative agencies as well as telecommunications providers. However, there has been significant political pushback. Alternative proposals include, for example, the creation of a centralized contact point for the private sector, simplifying notification requirements.

Under this second approach, requests and inquiries made to the centralized contact point would initiate one proceeding and the result would be binding for all state data protection authorities. This would put a stop to diverging assessments for the same data protection related matter depending on the state, in which the inquiry was raised, further improving the handling of data protection compliance matters.

NIS2 implementation law draft introduced into parliamentary discussions

Although the implementation deadline for the NIS2 Directive has already expired on 17 October 2024, Germany is yet to implement the directive into national law. After the initial government draft could not be passed before the federal elections in February 2025, the new timeline for the transposition law had been uncertain.

However, in July 2025, the new federal government published its draft for the transposition law, which has since been introduced into the federal parliament as well as the Bundesrat for further discussion. A first parliamentary reading took place on 11 September 2025. The draft proposal has since been delegated to the responsible working groups (internal affairs, digitalization and state modernization, and internal budget). A second reading has not yet been definitely scheduled.

The Bundesrat has considered the government draft and voted on a corresponding statement with various proposals for changes on 26 September 2025. The federal government has rejected the majority of these proposals in their answering statement.

Federal Ministry for Digitalization and State Modernization publishes ministerial draft for a law to execute Regulation (EU) 2024/1689 (AI Act)

On 12 September 2025, the Federal Ministry for Digitalization and State Modernization has published its ministerial draft for a law to execute the AI Act in Germany. Under this law, the Federal Network Agency would be named as a market surveillance agency.

Relevant stakeholder now have the opportunity to take position in relation to the law proposal. It currently remains unclear when a governmental draft as well as the introduction into the parliament and Bundesrat can be expected.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Greece

Contacts

Arianna Sekeri

Partner, KBVL Law Firm (member of the Deloitte Legal network)

asekeri@kbvl.gr

Maria-Alexandra Papoutsi

Senior Manager, KBVL Law Firm (member of the Deloitte Legal network)

mapapoutsi@kbvl.gr

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Hellenic Data Protection Authority: Enforcement updates

HDPA decisions

In 2025, the Hellenic Data Protection Authority (HDPA) has shown increased vigilance in enforcing GDPR compliance, issuing fines and sanctions to noncompliant organizations. We highlight some recent decisions reflecting HDPA's latest enforcement actions, including the imposition of substantial fines in key sectors.

Decision No. 23/23 June 2025

The HDPA examined a complaint against a large Greek bank regarding the erroneous processing of an individual's personal data. Due to a human error, the complainant was incorrectly recorded as a guarantor for a relative's business loan, leading the bank to send him multiple informational letters, although his data were never actually transferred to third parties. The HDPA found violations of the GDPR principles of lawfulness and accuracy (Articles 5(1)(a), 5(1)(d), and 6(1)) and imposed a €50,000 administrative fine on the bank, while noting the breach concerned a single incident without financial gain or material damage.

Decision No. 27/25 June 2025

The Greek affiliate of a large multinational telecommunications company was fined a total of €700,000 after a franchise store registered 15 prepaid mobile lines using a subscriber's personal details without the subscriber's knowledge. The fines were imposed for breaches of GDPR Articles 5(1)(d), 28(1), 28(3), 29, and 32, as well as Articles 12(1), 12(3), and 13(4) of Law 3471/2006 and Article 21(1) of Law 2472/1997. The company was also ordered to implement technical measures within three months to enhance the security of activating new mobile numbers under existing subscriber details, including notifying subscribers by SMS or equivalent and informing the HDPA.

Decision No. 32/11 July 2025

The Greek affiliate of a large multinational insurance company received a €20,000 fine for violating the complainant's right of access to recorded telephone calls, as it was found to be the data controller responsible for determining the purpose and means of recording calls at the dental care program's service center. The insurance company failed to provide the requested call recordings or transcripts, breaching Articles 15(1) and 15(3) of the GDPR. Additionally, the company was ordered to provide the complainant with the requested audio files or transcripts within 10 days and to notify the HDPA of its compliance.

HDPA ex officio investigations – June 2025

In June 2025, the HDPA carried out ex officio investigations in different entities in Greece operating across multiple business sectors, including retail, telecoms and financial institutions, to assess GDPR compliance of their online data processing activities (e.g., services provided online via websites and mobile applications).

As part of the relevant investigations, the HDPA, invoking the principle of accountability, requested the provision of extracts of the relevant entries of the entities' records of processing activities (RoPAs), relating to the above types of activities, as well as copies of the relevant data processing agreements (DPAs) executed with any third parties acting as data processors. They also requested the provision of documentation relating to the data processing activities carried out via social media networks for promotional and marketing purposes.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

HDPA Opinion, No. 3/8 July 2025

Review of the provisions of the draft law of the Ministry of Economy and Finance entitled "National Registry of Benefits and Aid"

The HDPA, in relation to the planned provisions of Articles 63-69 on the establishment of the National Registry of Benefits and Aid, calls on the Ministry of Economy and Finance to reassess the necessity and justify the independent existence of the proposed registry, which will contain nominative data of beneficiaries/natural persons. It also requests clarification of the roles and responsibilities of data controllers and processors among the involved entities, in connection with their assigned duties and powers.

Furthermore, the HDPA urges the ministry to include in the proposed regulations explicit provisions regarding the retention period of personal data, the obligation to conduct a data protection impact assessment (DPIA), and the requirements for data security within the registry. These recommendations are intended to ensure compliance with data protection principles and safeguard the rights of data subjects.

Transposition of the Data Governance Act in Greece

Law 5188/2025

Law 5188/2025 aims to make public sector data more accessible, especially for small businesses and research, while ensuring data protection. Key measures include appointing the Ministry of Digital Governance as the main authority for guidance, establishing data intermediation service providers, creating data altruism organizations for public interest purposes, and setting up a network of data officers in public entities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Transposition of the NIS2 Directive in Greece

Law 5160/2024

Law 5160/2024 implements the EU NIS2 Directive (Directive (EU) 2022/2555) into Greek law. The law defines the scope of cybersecurity obligations to cover sectors, including energy, transport, health, and digital services. It introduces stricter requirements for risk management and incident reporting. Law 5160/2024 aims to strengthen the overall cybersecurity framework and resilience of essential and important entities in Greece.

Joint Ministerial Decision No. 1689/6 May 2025

Joint Ministerial Decision 1689/2025 supplements this framework by introducing detailed national cybersecurity requirements aligned with Article 15(2) of Law 5160/2024. This framework operates as *lex generalis* and applies insofar as no sector-specific regulation exists. In the financial sector, DORA (Regulation (EU) 2022/2554) serves as *lex specialis*, imposing more detailed and stricter rules on ICT risk management and digital operational resilience.

Guidelines 28211/10 September 2025

Obligation for public sector entities to register on the digital platform for basic and important entities under Law 5160/2024

All central government entities, such as ministries, independent authorities, decentralized administrations, and legal entities of public and private law included in the Registry of General Government Entities, as well as second-level local government organizations (regions), are required to register on the platform within the deadline set in paragraph 1 of Article 9 of the relevant provision, with a final registration date of 30 September 2025.

Joint Ministerial Decision No. 2267/2 October 2025

According to Joint Ministerial Decision No. 2267/2025, first-level local government organizations in Greece (municipalities) must comply with the requirements of Law 5160/2024 (NIS2 Directive) from November 2026 onwards. This decision sets the official compliance deadline for these entities, allowing them a transition period to prepare for full implementation of the new cybersecurity obligations.

Ministerial Decision No. 1899/5 August 2025

On 5 August 2025, Ministerial Decision No. 1899/2025 was issued, defining the qualifications, duties, incompatibilities, and obligations of Information and Communications Systems Security Officers. The decision establishes the framework for their responsibilities in ensuring the security and proper operation of ICT systems within public sector entities.

Joint Ministerial Decision No. 1990/4 August 2025

On 4 August 2025, Joint Ministerial Decision No. 1990/2025 was issued, establishing a digital platform for the registration of essential and important entities as defined in Article 4 of Law 5160/2024. The decision sets out the procedures and technical specifications for the operation of this digital registry.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Transposition of Digital Operations Resilience Act (DORA) in Greece

Law 5193/2025

Law 5193/2025 (published on 11 April 2025) supplements Regulation (EU) 2022/2554 (DORA) by introducing national supervisory mechanisms and enforcement measures to enhance digital operational resilience across the financial sector. It designates the Bank of Greece and the Hellenic Capital Market Commission as the competent supervisory authorities, depending on the type of financial entity. Supervisory powers include access to documents, onsite inspections, and administrative fines of up to 10% of annual turnover in case of noncompliance.

Annual Report on Prudential Supervision and Resolution Activities of the Bank of Greece – DORA-related actions

In view of the requirements DORA and to support DORA compliance, the Bank of Greece has undertaken the following actions. In early 2024, the Bank of Greece developed a self-assessment questionnaire on the maturity level and distributed it to all supervised institutions falling under the scope of DORA. The aim was to document the current state and future compliance plans of these institutions regarding key regulatory requirements, as well as to inform them about areas of attention. Upon DORA's entry into force, the Bank of Greece created a dedicated section on its website to inform supervised institutions about the overall regulatory framework and its requirements. The Bank of Greece has also issued standardized templates for the notification of ICT-related incidents by supervised entities.

Furthermore, the Bank of Greece has implemented a mechanism for the prompt collection and forwarding of major incident reports to relevant stakeholders, in line with DORA's new requirements. To address the obligation of selected institutions to undergo threat-led penetration testing (TLPT), the Bank of Greece is establishing a dedicated TLPT team to fulfil this supervisory responsibility.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Greek bodies responsible for the protection of fundamental rights

On 12 November 2024, the Greek Ministry of Digital Governance, in compliance with the Article 77(2) of the EU AI Act, published the official catalogue of the Greek bodies responsible for the protection of fundamental rights. The catalogue includes the following bodies:

- The Hellenic Data Protection Authority;
- The Greek Ombudsman;
- The Hellenic Authority for Communication Security and Privacy; and
- The National Commission for Human Rights.

These bodies have the following powers:

- Seeking access to any documentation generated or maintained by AI system operators to illustrate adherence to the AI Act, as necessary to adequately perform their duties within their scope of authority.
- They may also submit a well-founded request to the market surveillance authority to facilitate the testing of a high-risk AI system through technical methods in situations where the documentation supplied by AI system operators is inadequate for assessing potential violations of fundamental rights.

These powers will take effect on 2 August 2026.

HDPA Decision Ordering EU Representative for Hangzhou DeepSeek Artificial Intelligence (Case No. 18/21 May 2025)

On 21 May 2025, the HDPA ordered Hangzhou DeepSeek Artificial Intelligence Co., Ltd. to appoint a representative in the EU for its DeepSeek AI services, as required by Article 27 GDPR. The company was found to be in violation of this obligation, since it offers services to individuals in Europe without an EU establishment or representative.

Special Secretariat for Artificial Intelligence and Data Governance

On 17 July 2025, the Greek government introduced the Special Secretariat for Artificial Intelligence and Data Governance at the Ministry of Digital Governance with the following competences:

- The effective coordination of the involved bodies and authorities regarding the implementation of the national and EU framework for AI and data;
- The promotion of the responsible adoption and the lawful and secure use of AI by public sector entities;
- The development of digital skills related to AI and data governance;
- The design and implementation of information and communication technology projects, with an emphasis on AI and data governance, funded by national and European resources;
- The promotion of cooperation between the private and public sectors in the fields of AI and data;
- The representation of the country and its participation in the shaping of policy on matters concerning AI and data at the European and international level;
- The drafting of legislative and regulatory acts and the harmonization of the national framework with EU and international law; and
- The promotion of actions to strengthen scientific research, as well as research-oriented activities related to AI and data governance applications.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Developments regarding the implementation of the EU AI Act in Greece

In light of the EU AI Act's entry into force, the following key developments are expected in Greece in Q1 2026, with the publication of the below legislation anticipated by 1 December 2025.:

- Determination of the Greek national authority responsible for overseeing and supervising the implementation of the EU AI Act;
- Amendment of the existing Greek Law No. 4961/2022 (which regulates the use of emerging technologies such as AI in Greece, establishing an early legal framework for their development and governance) to take into account the provisions of the EU AI Act; and
- Promotion and enhancement of AI literacy, as a priority for the Greek government, to support the responsible use of AI.

Developments regarding cybersecurity in Greece

The National Cybersecurity Authority of Greece has announced that its full supervisory and enforcement framework for "essential and important entities" under Law 5160/2024 will start with audits and controls as of 2026, after issuing necessary regulations and decisions by end of 2025.

National Cybersecurity Authority is also preparing two key decisions due by end of 2025, one defining what constitutes a "significant cybersecurity incident" that triggers mandatory obligations, and another establishing a "standardized cybersecurity policy framework" for entities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Guatemala

Contacts

Estuardo Paganini

Partner, Deloitte Legal Guatemala

egpaganini@deloitte.com

Johana García Perdomo

Manager, Deloitte Legal Guatemala

johagarcia@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Law on Access to Public Information (Decree 57-2008 of the Congress of the Republic)

Guatemala does not have a specific legislation addressing the protection of personal data, but this law, even though it pertains to public records, does address the matter in certain provisions that can be applicable to private parties.

This normative defines what constitutes personal data, sensitive personal data, and the National Data Protection Authority.

Article 64 establishes a prohibition for private parties to commercialize personal data without consent. Violation of this provision results in imprisonment ranging from five to eight years, a fine raging from GTQ 50,000 to GTQ 100,000, and the confiscation of any elements employed to commit 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; however, it is regarded as a form of communication and electronic communication, as it involves an exposition, statement, claim, advice, request, or offer, as well as the acceptance of an offer, in relation to the construction or execution of a contract.

This law helps expedite the registration of companies, trademarks, and company modifications.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Hong Kong

Contacts

Ven Tan

Managing Partner, Chan & Jamison LLP (member of the Deloitte Legal network)

venxtan@deloittelegal.com.hk

Kenneth Lee

Counsel, Chan & Jamison LLP (member of the Deloitte Legal network)

kennelee@deloittelegal.com.hk

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Updated Guidance on Cloud Computing by the Privacy Commissioner for Personal Data (PCPD)

- The updated guidance reinforces stringent obligations for businesses under Hong Kong's Personal Data (Privacy) Ordinance (PDPO). Organizations that utilise cloud services – whether private, public, SaaS, IaaS, or PaaS – retain legal responsibility for data protection, even if breaches stem from third-party providers.
- Key recommendations include encrypting data both while during storage and in transmission, implementing robust authentication methods, regularly evaluating the security practices of subcontractors, and negotiating enhanced contractual protections beyond standard vendor terms.
- In relation to cross-border data transfers, it highlights the importance of careful adherence to PDPO principles, including providing clear notifications to data subjects.
- Additionally, the guidance stresses the necessity of thorough access logging, continuous monitoring, and secure data erasure or return upon the termination of contracts.
- By considering the latest technologies and trends in cloud computing services, the guidance provides organizations recommended best practices to enhance the protection of personal data privacy, covering various aspects such as service and deployment models, standard services and contracts, as well as outsourcing arrangements.

The proposed Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance) put on hold

- Following a series of data breaches in the early 2020s, a comprehensive review of the PDPO was undertaken. Since its enactment, the PDPO has been fundamental to data protection in Hong Kong.
- The proposed Amendment Ordinance for 2024 was initially scheduled to roll out in stages starting in 2025, with full implementation expected by 2026.
- Key changes proposed include mandating that organizations notify the PCPD and affected individuals in the event of a significant data breach, enhanced consent protocols for sensitive personal data, such as biometric information and health records, and penalties for noncompliance with the PDPO increasing significantly, with organizations facing fines up to 10% of their annual turnover or HK$10 million, whichever is higher.
- However, plans to amend the PDPO have been postponed due to concerns about the financial burden on smaller businesses in complying with these new regulations.
- The government is considering a "piecemeal approach" to introduce the amendments gradually, aiming to alleviate the impact on local enterprises. As of now, no definitive timeline has been announced for these changes.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Protection of Critical Infrastructure (Computer System) Ordinance (2025) passed to strengthen cybersecurity for essential services

- On 19 March 2025, the Hong Kong Legislative Council passed the Protection of Critical Infrastructure (Computer System) Ordinance (2025), which is set to come into effect on 1 January 2026.
- This new legislation marks a significant enhancement of Hong Kong's cybersecurity regulatory framework, aimed at safeguarding critical infrastructures (CI) across vital sectors. It mandates that CI operators follow specific cybersecurity protocols and empowers regulatory authorities to manage and mitigate cyber risks.
- This move aligns Hong Kong with the global trend toward increased regulatory oversight and requirements for cybersecurity and operational resilience.
- The ordinance defines two categories of critical infrastructure:
  - The first category includes any infrastructure essential for the uninterrupted delivery of services in one of eight designated sectors: energy, information technology, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting services; and
  - The second category will be designated by the government at a later date and will encompass any other infrastructure whose damage, loss of functionality, or data leakage could significantly disrupt critical societal or economic activities in Hong Kong.
- Although the timeline for designating the second category of critical infrastructure is uncertain, it is expected to include major sports and performance venues, as well as research and development parks.
- The new legislation also includes computer systems accessed by CI operators in or from Hong Kong that are vital to the core operations of the relevant infrastructure.
- Designated CI operators are required to implement robust cybersecurity management systems, perform regular risk assessments, and maintain incident response capabilities and security standards that meet prescribed standards.
- Enforcement measures outlined in this ordinance encompass administrative penalties, criminal sanctions for serious breaches, and the possibility of government intervention when the security of critical infrastructure is at risk.
- Additionally, the legislation creates a framework for information sharing between government agencies and critical infrastructure operators, aimed at enhancing overall cybersecurity resilience.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Policy Statement on the Responsible Application of Artificial Intelligence in the Financial Market

- On 28 October 2024, the Financial Services and the Treasury Bureau released a policy statement outlining the government's stance and strategy regarding the responsible application of AI within the financial market.
- This policy statement aims to strike a balance between fostering AI development and addressing the associated risks related to cybersecurity, intellectual property rights, and data privacy. To ensure the responsible application of AI, it requires that financial institutions priorities the protection of data privacy, intellectual property rights, information security, accountability, operational resilience, and job security.
- The government recognizes the various benefits that AI applications can offer to the financial services sector. To this end, it will adopt a dual-track approach that encourages the adoption of AI while simultaneously tackling potential challenges, including cybersecurity threats, data privacy concerns, and the protection of intellectual property rights.
- Moreover, the policy statement encourages financial institutions to formulate a robust AI governance strategy that employs a risk-based approach throughout the entire AI lifecycle, including procurement, use and management of AI. It also advocates for the implementation of human oversight to effectively mitigate potential risks associated with AI deployment.

Introduction of voluntary Generative Artificial Intelligence Technical and Application Guidelines by the Digital Policy Office

- In April 2025, the Digital Policy Office introduced the voluntary Generative Artificial Intelligence Technical and Application Guidelines, designed to provide a best practice framework for the ethical and responsible development, deployment, and use of Generative AI technologies. It targets technology developers, platform providers, and AI users.
- The guidelines outline the scope and limitations of AI applications, addressing potential risks and governance principles associated with Generative AI technology. Key technical risks highlighted data leakage, model bias, and errors that must be addressed.
- The guidelines highlight five fundamental pillars of ethical AI governance:
  - Personal data privacy;
  - Intellectual property protection;
  - Crime prevention;
  - Reliability and trustworthiness; and
  - System security.
- While these guidelines do not carry legal force, they serve as an important reminder of the various legal and ethical risks associated with the deployment and use of AI tools.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Protection of Critical Infrastructure (Computer System) Ordinance (2025) to take effect on 1 January 2026

- The ordinance focuses on protecting critical infrastructure and aligns Hong Kong with the global movement towards heightened regulatory scrutiny around cybersecurity and operational resilience, similar to frameworks in Australia, the EU, and the UK.
- It will oversee designated critical infrastructure operators, and their systems classified as critical computer systems. Additionally, a Commissioner's Office will be established to manage and enforce this new regulatory framework, expected to launch in the first quarter of 2026.
- Penalties for violations of the ordinance will range from HK$500,000 to HK$5 million, along with daily fines for ongoing breaches, applying at the organizational level rather than targeting individuals.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Indonesia

Contacts

Stefanus Brian Audyanto

Partner, Deloitte Legal Indonesia

saudyanto@deloittelegal-id.com

Derryan Rahmat Putra

Director, Deloitte Legal Indonesia

dputra@DeloitteLegal-Id.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Implementation of personal data protection

The Indonesian government, through the Ministry of Communication and Informatics (MCI), published the draft Government Regulation on Personal Data Protection (PDP GR Draft) to the public as the implementing regulation of Law No. 27 of 2022 on Personal Data Protection (PDP Law), however the PDP GR Draft remains under preparation and is expected to be finalized and enacted in 2025. 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.

The implementing regulations of PDP Law is still in the process of harmonization with the Ministry of Law (MOL). It is shall be drafted and enacted remembering the high number of cases of personal data misuse by data controllers in Indonesia, by this it is expected to be a more comprehensive high-level provisions on personal data protection in Indonesia.

In June 2025, Ministry of Communication and Digital Affairs (MOCD), previously known as Ministry of Communication and Informatics (MCI), shared the updates regarding the progress of the implementing regulation of PDP Law, MOCD stated that the government regulation on the technical requirements of the PDP Law is being drafted and assessed by the MOCD and MOL. After the harmonization process between MOCD and MOL is complete, it will proceed to the next two stages, namely finalization and enactment.

The Director General of Digital Space Supervision at MOCD said that the draft government regulation of the PDP Law is still being discussed and is expected to be completed before the end of 2025.

It is hoped that the draft will include provisions regarding the imposition of sanctions on the government, as the current sanctions are only aimed at private operators, not the government.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Modification of Personal Data Protection Law

In September 2024, the PDP Law was submitted for review to the Constitutional Court. In this case, the applicant questioned the use of the word 'and' in relation to the provisions on the obligations of personal data controllers and personal data processors and the appointment of officials or officers to carry out personal data protection functions. The applicant objected to the word "and" in second point, arguing it limited which organizations must appoint a data protection officer (DPO). The court granted the petition, changing "and" to "and/or", thus expanding the obligation to appoint DPOs and strengthening citizens' personal data protection. In the Constitutional Court Decision Number 151/PUU-XXII/2024 granted the application and replaced the use of the word "and" in Article 53 paragraph 1 of the PDP Law with the words "and/or". This article carries three conditions which personal data controllers/processors must appoint a DPO, however, with this decision this article is amended as follows:

- They process personal data for public services (e.g., government agencies);
- They carry out a large-scale regular and systematic monitoring of data subjects as part of their core activities (e.g., online behavior tracking); and/or
- They process large volume of sensitive personal data or data related to criminal convictions and offenses.

Previously, the PDP Law uses the word "and" means that all three conditions must be met for the to apply. The changes of the conjunction from "and" to "and/or" means meeting any one of the conditions would trigger the DPO requirement.

Establishment of the Personal Data Protection Authority

The establishment of the Personal Data Protection Authority (PDP Authority) is still awaited. In the implementation of the PDP Law to date, PDP Authority has not been established, for the time being, the duties of the personal data protection agency are under the Directorate General of Digital Space Supervision of MOCD. The presidential regulation on the establishment of PDP Authority is still being drafted and is expected to be completed before 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Development of the Draft Law on Cybersecurity and Resilience in Indonesia

In strengthening national security against growing cybercrimes, the House of Representatives and the government has included the Draft of Law on Cybersecurity and Resilience as a priority in the 2025 National Legislation Program. The draft was first introduced in 2019 by the House of Representative. However, the progress on its development remained minimal. Indonesia currently has two presidential regulations concerning the matter of cybersecurity: Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crises Management and Presidential Regulation No. 82/2022 on the Protection of Vital Information Infrastructure.

In October 2025, the MOL announced that the government, namely MOL, MOCD and National Cyber and Crypto Agency (Badan Siber dan Sandi Negara (BSSN)) is currently drafting Draft of Law on Cyber Security and Resilience. The draft will shortly submit to the House of Representatives once it's finalized for joint deliberation. BSSN Deputy for Economic Cyber and Crypto stated that the draft is expected to be completed by the end of 2025 since this draft is a priority within the government's National Medium-Term Development Plan (Rencana Pembangunan Jangka Menengah Nasional (RPJMN)) 2025-2029.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Overview of Indonesia's Artificial Intelligence Regulatory Framework and forthcoming presidential regulation

There is a legal framework for the existence of AI in Indonesia that has been released, which is the MCI Regulation Number 9 of 2023 on Artificial Intelligence Ethics. There is no other specific law regulating the development of technology and the various risks that accompany it, such as disinformation, algorithmic errors, and potential threats to national security. This could raise a potential concern given the rapid development of AI technology, which necessitates protection for its users and guidelines for its development process.

Furthermore, to strengthen the enforcement of this regulation, MOCD is on the process of finalizing the draft of regulations on AI, namely the draft National AI Roadmap, which is expected to become a presidential regulation in the field of AI. The MOCD aiming to regulate the roadmap for AI development through presidential regulation, with hope that the regulation can help align existing policies related to AI use across ministries and other government institutions. One of the important points to be discussed in the draft is the security and safety of AI development and use. The MOCD explained that the draft is expected to be finalized soon.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

In June 2025, the Special Staff to the Minister for Inter-Institutional Relations and Strategic Programs at the MOCD, stated that the implementing regulations for the PDP Law are still in the process of being finalized, including both the establishment of the PDP supervisory body and the detailed technical implementation. The regulation for the formation of the supervisory body is currently being processed at the Ministry of State Apparatus Empowerment and Bureaucratic Reform, while the technical regulations are being handled by the MOL. The enactment process of these implementing regulations is still anticipated to be completed soon.

Plans to establish a PDP Authority are still under discussion. However, in the execution plan, the PDP Authority will not be under the MOCD, but directly under the president. It is therefore anticipated that the PDP Authority will be established in the near future to oversee data protection in Indonesia and help reduce the misuse of personal data. As mandated by the PDP Law, the PDP Authority should have been established following the end of the two-year transition period, which requires all parties to comply with its provisions, including the obligation to process personal data in accordance with the established principles.

Cybersecurity

With the ongoing process of finalizing draft of Law on Cybersecurity and Resilience, it is expected that the establishment of a much stronger and more coordinated national cyber defense framework in Indonesia

By having the draft of Law on Cybersecurity and Resilience as a priority in the 2025 National Legislation Program, it signals the government's urgency in addressing growing cybercrimes and it shows the commitment to strengthening digital security infrastructure.

AI

The Standard Industrial Classification (Klasifikasi Baku Lapangan Usaha Indonesia (KBLI)), is a national system that categorizes all types of business activities in Indonesia. The chosen KBLI code determines a company's licensing requirements, compliance obligations, and eligibility for investment incentives. As Indonesia's digital economy evolves, the government may introduce new KBLI classifications to better accommodate and regulate AI-focused enterprises.

However, in the context of the AI sector, there is no specific KBLI code exclusively for artificial intelligence, AI-related activities are generally classified under existing categories such as software development, data processing, or IT services. Therefore, in highlighting the creative economy growth in Indonesia, there's a plan of updating Indonesia's KBLI to include emerging sectors such as cybersecurity, artificial intelligence, blockchain, and the internet of things. From the process of drafting the National AI Roadmap by the MOCD, it is expected to be a comprehensive, high level regulatory framework for AI in Indonesia.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Italy

Contacts

Ida Palombella

Equity Partner, Deloitte Legal Italy

ipalombella@deloitte.it

Pietro Boccaccini

Director, Deloitte Legal Italy

pbocaccini@deloitte.it

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Annual report of the Italian DPA on personal data protection for 2024

In July 2025, the Italian Data Protection Authority (DPA) (the Garante per la protezione dei dati personali) published its annual report on personal data protection for the year 2024. The report summarizes the authority's key activities in 2024 across various sectors, such as public administration, healthcare, research activities, AI, web scraping, marketing, telemarketing, electronic communications, etc.

Some of the most relevant topics addressed by the Italian DPA have been digitalization and AI. Additional areas that have been examined by the DPA have been aggressive telemarketing, processing of biometric data and use of healthcare data.

The following numbers characterize the work done by the Italian DPA in 2024:

- 835 board decisions (compared to 634 in 2023);
- 4,090 complaints replied and 93,877 reports managed;
- 16 reports of facts to the criminal judicial authority (seven in 2023);
- 468 corrective measures and sanctions issued (394 in 2023);
- €24 million in fines collected (8 million in 2023);
- 2204 data breaches notified to the DPA (2037 in 2023); and
- 130 inspections carried out (144 in 2023).

In the report the Italian DPA has underlined the main obligations on organizations for the development and use of AI systems. Among such obligations, the DPA 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.

Consent for marketing purposes must be obtained through a double opt-in process

In June 2025, with the Decision No. 330 of 4 June 2025, the Italian Data Protection Authority (DPA) imposed a fine of €45,000 on an online car resale company for unlawful processing of personal data for direct marketing purposes.

Among other infringements, the DPA found that the company had not implemented adequate technical and organizational measures to ensure lawful processing and valid consent collection.

In particular, the complainant stated they had not given consent to receive marketing emails, while the company relied on subscription logs as proof of consent.

The Italian DPA, referring to Article 7 of the GDPR, deemed this evidence insufficient in light of the principle of accountability, emphasizing that the most reliable way to demonstrate valid consent is through a double opt-in process. As a result of the lack of evidence, for the infringement of the principle of accountability the marketing activities were considered to have been carried out without valid consent.

While there is no explicit legal obligation to use this mechanism, the DPA reinforces the role of double opt-in as best practice and appropriate measure for collecting and documenting consent for the processing of personal data for marketing purposes.

In other words, what matters is that the controller can verify and demonstrate the source of the data, ensuring that the consent was indeed provided by the data subject through procedures such as double opt-in or possibly with another equivalent measure.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Italian DPA: An “omnibus consent” is invalid

In a controversial decision – Decision No. 114 of 27 February 2025 – the Italian Data Protection Authority (DPA) challenged the lawfulness of a single consent given for the communication for marketing purposes to various third-party recipients, processing the data as autonomous data controllers, in relation to various channels.

In particular, following its investigations, the DPA had found that the data controller was relying on a single check box to collect consent to communicate the personal data to a large pool of recipient belonging to very heterogeneous business categories and in relation to a diversity of means of communication.

Despite confirming the consolidated interpretation of the DPA that a single consent may apply to a variety of recipients, including those identified by business categories, the DPA emphasized that the use of overly broad consent forms – encompassing numerous recipients and various communication channels – does not allow the data subject to express a genuine and free choice and unreasonably undermines the data subject’s ability to retain control over the processing of their personal data.

The Italian DPA specified that any consent form must, at a minimum, allow the data subject to choose among the different categories (or macro-categories) of data recipients and limit the range of means of communication. Otherwise, the processing would result in an undue intrusion into the individual’s privacy and cause an irreparable loss of control over their personal data.

Sanctions to an Italian region for excessive retention of metadata in the workplace

The Italian DPA sanctioned an Italian region for not complying with Provision No. 243, of 29 April 2025, which represents an important reminder about the proper handling of personal data within the digital workplace, balancing security needs with workers' rights, and affirms that the prolonged retention of metadata constitutes a form of monitoring that requires specific authorization.

Here are the DPA’s key findings:

- Internet browsing logs were stored for 12 months, with the possibility of identifying users by cross-referencing separate data and although the region justified this practice on security grounds, it did not have the legally required authorization. The DPA determined that this retention and processing breached the GDPR and the regulations on remote monitoring, and imposed corrective measures including anonymization, reduction of the retention period to 90 days and access restrictions.
- Email metadata was stored for 90 days for technical support and security purposes. The region argued that no authorization was necessary for the use of such metadata, but the DPA clarified that prolonged retention of email metadata constitutes a form of remote monitoring and therefore requires procedural safeguards, such as an agreement or authorization. Furthermore, a data protection impact assessment (DPIA) was initially missing and was only conducted belatedly.
- Technical support request data (OTRS system) were retained even after the system was deactivated, without an adequate legal basis or contractual data processing agreements with suppliers, thereby violating the GDPR. Subsequently, the region deleted the data and reduced the retention periods in the new system.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

ACN detailed obligations under the NIS2 Legislative Decree for essential and important entities

The Italian National Cybersecurity Agency (ACN) with the Decision No. 164179/2025 has detailed the basic obligations under the NIS2 Legislative Decree (i.e. Legislative Decree No. 138/2024), including requirements for risk management, incident reporting, and security measures for essential and important entities, effective from January 2026.

The ACN decision outlines the fundamental security measures that essential and important entities must implement, including measures regarding security governance, training, risk analysis and vulnerability management, cryptography, incident management, and supply chain security, as well as ensuring proper involvement of management bodies.

The resolution contains four different annexes:

- Annex 1 concerns security measures and risk management measures applicable to important entities;
- Annex 2 concerns security measures and risk management measures applicable to essential entities;
- Annex 3 concerns requirements in relation to significant incidents applicable to important entities; and
- Annex 4 concerns requirements in relation to significant incidents applicable to essential entities.

Such obligations are gradually going to become applicable, with incident reporting obligations already applicable from January 2026 whilst security measures obligations and risk management measures applicable from October 2026.

The CAN further illustrated such obligations in a following guideline meant to explain how to interpret the various requirements for NIS2 entities.

In consideration of this legal framework, NIS2 entities must conduct a comprehensive gap analysis, adopt the required security measures as well as the risk management and security procedures, ensure management oversight and establish procedures to notify incidents.

ACN issued a determination detailing the functioning of the NIS2 platform

With a determination, the ACN has set the basic guidelines for the registration of the NIS2 entities onto the NIS2 platform of the authority.

The determination requires the designation of a point of contact and of a cybersecurity incident response team (CSIRT) representative as well as their possible substitutes.

The point of contact is responsible for the registration process under Article 7 of the NIS Decree and acts as the official intermediary between the ACN and the NIS entity whilst the CSIRT representative – designated by the point of contact through the platform – acts as the operational interface with CSIRT Italia. Thus, the CSIRT representative is responsible for reporting incidents that significantly impact the provision of the services of the NIS2 entity. The CSIRT representative and any substitutes must possess proven expertise in cybersecurity and incident management, along with a thorough understanding of the information systems and networks operated by the entity they represent.

In conclusion, such determination is another step towards consolidating the operational framework established under the NIS Decree in Italy, introducing the mechanisms to ensure ease of contact between the authority and the NIS2 entities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

DPCM No. 221 of 9 December 2024: Regulation establishing criteria for the application of the safeguard clause

On 10 February 2025, Prime Ministerial Decree (DPCM) No. 221/2024 was published in the Italian Official Journal, setting out the criteria for applying the safeguard clause under the NIS2 Italian Legislative Decree.

Article 3 sets out the conditions for invoking the safeguard clause, stating that it may be applied if the requesting entity declares:

- The complete independence of its NIS-related information and network systems from those of linked entities, meaning that the information and network systems of such linked entities do not in any way contribute to the functioning of the requesting entity's systems; or
- The complete independence of its NIS-related activities and services from those of linked entities, meaning that the activities of the linked entities and services do not in any way contribute to the performance or delivery of the requesting entity's NIS-related operations.

In order for the clause to apply, both conditions must be met. An entity that believes it satisfies these requirements must submit a request for the application of the safeguard clause during the registration process on the NIS2 digital platform.

Publication of Legislative Decree No. 23/2025 for the adaptation of the national legislation

In March 2025, the Legislative Decree No.23 entered into force, containing provisions for the adaptation of the national legislation to Regulation (EU) 2022/2554, known as the Digital Operational Resilience Act (DORA), and to Directive (EU) 2022/2556.

The decree applies to the entities referred to in Article 2 of the DORA which include, among others, credit institutions, payment institution, investment firms, insurance and reinsurance undertakings and intermediaries, pension entities, and third-party ICT service providers for the financial sector.

Some of the new measures introduced by the decree include:

- The identification of the competent DORA authorities, such as the Bank of Italy, Consob, IVASS and COVIP;
- The entities responsible for receiving reports of major ICT incidents, based on the entity that suffered them (i.e., the DORA competent authorities mentioned above), including the CSIRT Italy established at the ACN; and
- The identification of forms of operational and informational coordination among the competent DORA authorities through memoranda of understanding, ensuring the timely and complete sharing of data and information useful for the exercise of their functions.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

National AI law: Safeguarding fundamental rights and defining governance

On 17 September 2025, Italy became the first country in Europe to adopt a national AI law by approving Law No. 132/2025, which contains provisions and delegations to the government regarding artificial intelligence (AI).

The purpose of the law is to promote the correct and responsible use of AI, prioritizing the protection of citizens and ensuring oversight of social and economic risks, as well as the impact that these new technologies may have on fundamental rights.

Below are some of the key points covered by the law.

- Protection of minors: Minors under the age of 14 won't be able to access AI tools without prior consent of those holding parental responsibility.
- AI in various key sectors: The use of AI tools in different sectors – including healthcare, scientific research, labour, public administration, and judicial activities – must respect fundamental principles, such as transparency, proportionality, security, protection and confidentiality of personal data, as well as accuracy, fairness, quality, and data accessibility. Moreover, it is mandatory to provide clear and simple information when using AI tools no matter the sector.
- Protection of copyright: It is established that works created with the aid of AI tools, may be protected by copyright if proven that human contribution is creative, significant and demonstrable.
- Provisions regarding intellectual professions: The use of AI must be instrumental and supportive of professional activity only, and clients must be informed about the AI systems used by the professionals.
- The government's role: The Italian government must adopt a national strategy on AI, which will be updated every two years by the Interministerial Committee for Digital Transition, supported by the Department for Digital Transformation of the Presidency of the Council.
- Amendments to the criminal code: A new offense concerning the illegal dissemination of content generated or manipulated through artificial intelligence systems was introduced, establishing that the use of AI in the commission of a crime may constitute an aggravating circumstance.

Furthermore, the law recognizes the following authorities as responsible for overseeing compliance with the above principles:

- The Agency for Digital Italy (AGID), tasked with promoting innovation and the development of artificial intelligence, as well as conducting monitoring activities;
- The National Cybersecurity Agency (ACN), responsible for cybersecurity protection, with supervisory duties including inspections and sanctions; and
- The Data Protection Authority (the Garante per la protezione dei dati personali), which retains its powers regarding personal data.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Developer of an AI chatbot fined by the Italian DPA

The Italian Data Protection Authority (DPA) (the Garante per la protezione dei dati personali) fined a US-based company, developer of an AI-chatbot accessible online, for €5 million and initiated an investigation into the training of the Generative AI model underlying the service. With such decision, the DPA confirmed the regulatory violations previously alleged in February 2023 when it ordered the block of the processing. The main infringements the DPA found in its decision included:

- Lack of a valid legal basis for the processing of personal data: The company did not clearly identify the applicable legal basis for the various processing activities carried out. The information provided was generic and insufficiently detailed, violating the principle of granularity, which requires the data controller to clearly specify which legal basis is used for each purpose and processing operation, avoiding vague, cumulative, or indistinct formulations;
- Failure to conduct a legitimate interest assessment (LIA): The absence of this analysis undermines the validity of the legal basis invoked for the model's development, constituting a breach of the accountability principle;
- The privacy notice provided by the company was not compliant with the transparency and intelligibility requirements under the GDPR. Specifically, it was available only in English and contained generic and unclear information regarding the categories of personal data actually processed, data retention periods, and any transfer of personal data to non-EU third countries; and
- Lack of effective age verification systems for users: The company had not implemented adequate technical mechanisms to reliably verify users' ages.

Italian DPA fined a municipality for the use of AI cameras

The Italian Data Protection Authority (DPA) became aware, through news reports, that an Italian municipality had deployed AI cameras in public areas to collect data via such surveillance system, aiming to gather information on traffic and the number and types of vehicles on public roads.

Following an extensive investigation, the DPA found that the measures implemented by the controller, such as the claimed anonymization of the personal data collected, were inadequate.

The DPA emphasized that the processing could not genuinely be considered anonymization.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Italian DPA published inspection plan for the second semester of 2025

The Italian Data Protection Authority published its inspection plan for the second semester of 2025 (July 2025 to December 2025).

The DPA announced that its activities will be focusing on the following areas:

- Data breaches that have affected, in recent months, public databases of particular significance and sensitivity with specific reference to security systems and the accessibility profiles of the databases themselves;
- Data processing operations carried out in the insurance sector to provide fee estimates;
- Widely used applications for the acquisition and management of whistleblowing reports;
- On data processing operations carried out by local public transport services entities;
- Processing operations through biometric recognition systems, used for customer identification processes in banking services;
- In the context of data processing for statistical purposes for scientific research purposes with specific reference to the maintenance of pathology registers;
- The processing of personal data contained in the so-called health dossier; and
- The unlawful processing of data for telemarketing purposes in the energy sector.

It is expected that the DPA will issue decisions relating to these areas and sectors.

Italy's new rules on the exposure of minors on digital platforms:

Italy is currently discussing the introduction of new rules with regards to the presence of minors in video, audio and images on digital platforms, media and on the internet in general (Bill No. 1166).

The bill introduces new limitations and obligations aiming to better protect the children's rights, particularly below the age of 14, while using digital platforms:

- The earnings made by using the minors' image in social media content must be deposited into a blocked account in their name, which they will be able to access only when turning 18 years old.
- Upon turning 14, the minor whose image has been used on digital platforms has the right to request for all of this content to be removed from the internet and all search engines.
- Companies that wish to employ children under 14 in their commercial content must obtain express authorization from the person exercising parental responsibility or the legal representative of the child, while simultaneously informing the Italian Communications Regulatory Authority (AGCOM) of such employment.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Ivory Coast

Contacts

Ursula Dutauziet

Partner, Deloitte Legal Côte d'Ivoire

udutauziet@deloitte.fr

Audrey Allo-Ello

Senior Manager, Deloitte Legal Côte d'Ivoire

nallo-ello@deloitte.fr

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Authorizations for the processing of personal data

The Regulatory Authority for Telecommunications/ICT of Côte d'Ivoire (ARTCI) authorized the following decisions allowing companies to process personal data, particularly for video surveillance, security, human resources management, or cross-border data transfers as part of digital or value-added services.

- ARTCI Decision No. 2025-1249 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 19 June 2025 authorizing the processing of personal data by QATAR AIRWAYS CI 'Video surveillance';
- ARTCI Decision No. 2025-1236 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 2 May 2025 authorizing the processing of personal data by INVESTECH SARL (video surveillance);
- ARTCI Décision No. 2025-1235 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 2 May 2025 authorizing the processing of personal data by Danaya INC Côte d'Ivoire;
- ARTCI Decision No. 2025-1234 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 2 May 2025 authorizing the processing of personal data by Bureau Veritas Côte d'Ivoire;
- ARTCI Decision No. 2025-1224 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 authorizing the transfer of personal data to BOOZ TECHNOLOGIES (provision of value-added services);
- ARTCI Decision No. 2025-1215 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 authorizing the processing of personal data by FALCON SECURITY HUB;
- ARTCI Decision No. 2025-1221 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 authorizing the transfer of personal data to Germany LONACI (Digital Ocean);
- ARTCI Decision No. 2025-1218 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 authorizing the transfer of personal data to South Africa LONACI (AMAZON); and
- ARTCI Decision No. 2025-1216 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 authorizing the processing of personal data by Mota Engil Côte d'Ivoire.

Warnings and formal notices for noncompliance with data protection law

ARTCI has taken the following decisions:

- ARTCI Decision No. 2025-1233 of the Protection Authority of the Republic of Côte d'Ivoire dated 2 May 2025 issuing a warning and formal notice to the social welfare institution Caisse Générale des Agents de l'État (IPS-CGRAE) regarding the protection of personal data (San Pedro Agency); and
- ARTCI Decision No. 2025-1232 of the Protection Authority of the Republic of Côte d'Ivoire dated 2 May 2025 issuing a warning and formal notice to the Directorate General of the Treasury and Public Accounting regarding the protection of personal data (Abengourou Agency).

Warnings against unlawful use of biometric data (without prior authorization)

Refusal of authorization for biometric time-tracking system using facial recognition.

ARTCI has taken the following decision:

- ARTCI Decision No. 2025-1213 of the Data Protection Authority of the Republic of Côte d'Ivoire dated 18 February 2025 refusing the processing of personal data by G4S SECURE SOLUTIONS.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Creation of the National Agency for Information System Security

The Ministry of Digital Transition and Digitalization announced the creation of the National Agency for Information Systems Security (ANSSI), a new national body dedicated to cybersecurity in Côte d'Ivoire.

Adopted by the Council of Ministers on 30 October 2024, this decree aims to strengthen the security of information systems in the country. From now on, a single structure will be responsible for the coordination, protection and crisis management of cybersecurity, covering both critical infrastructure and public and private information systems.

The missions of ANSSI are:

- Implementation of cybersecurity action plans;
- Coordination of critical infrastructure protection efforts;
- Monitoring, detection, and response to incidents; and
- Management of prevention and protection processes for information systems.

This initiative marks a turning point in Côte d'Ivoire's digital security, with an agency fully dedicated to the protection and resilience of national information systems.

The ANSSI officially launched its digital operations on 11 February 2025.

ANSSI has taken over functions that were previously the responsibility of ARTCI, including security audits, incident management and the issuing of electronic certificates.

2024 Report on Cybercrime (published by ANSSI)

On 22 May 2025, during the first edition of the Digital Law Days (Journées du Droit Numérique (JDN)), the National Agency for Information Systems Security of Côte d'Ivoire (ANSSI-CI) presented two key documents:

- The 2024 Report on the state of Cybercrime in Côte d'Ivoire; and
- The Practical Guide to Securing Information Systems – Legal Aspects.

Organized by the Ministry of Digital Transition and Digitalization, the event was held under the theme: "Law and Digital for All: Building Trust in the Digital Space."

The report highlights a significant increase in cybercrime cases, rising from 8,132 incidents in 2023 to 12,100 in 2024.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

National AI Strategy: An ambitious roadmap

The Ivorian government unveiled its National Artificial Intelligence Strategy 2024-2027 during the Artificial Intelligence Days (JIA 2025) held in Abidjan from 20-22 February 2025.

This event, organized by the International Council of Artificial Intelligence (CONIIA) and Human AI, in partnership with the Ministry of Digital Transition, aims to position AI as a catalyst for transformation in Côte d'Ivoire.

Discussions focused on the integration of AI into various sectors such as:

- Health;
- Education;
- Agriculture; and
- Media.

AI in the service of education: A balance to preserve

During the International Day of Education celebrated by UNESCO in New York on 24 January 2025, the Minister of National Education and Literacy, Mariatou Koné, reaffirmed the Ivorian government's commitment to leveraging AI while preserving human autonomy in the education system. She emphasized that AI should never dictate educational choices nor standardize thinking, in accordance with the recommendations of the General Assembly on National Education and Literacy (EGENA).

Demystification and training: Concrete actions

The 2025 AI Days (JIA 2025) provided a platform for exchange, training, and collaboration among the public and private sectors, academia, and civil society.

The main objective was to "demystify AI," promote its adoption, and develop solutions tailored to Ivorian realities. Training workshops, conferences, and mentoring sessions were organized for various audiences, thereby strengthening the human skills needed for AI to become a true driver of development.

AI and public services: A revolution underway

The panels at JIA 2025 addressed the impact of artificial intelligence on improving public services in Côte d'Ivoire, particularly in the health and education sectors. The goal is to explore how AI can be used to optimize resource management, enhance the quality of services, and ensure equitable access for all citizens.

The National Artificial Intelligence Strategy for 2030

Developed by the Ministry of Digital Transition and Digitalization in collaboration with the World Bank, it aims to make inclusive, ethical, and responsible artificial intelligence a major lever for digital transformation, serving a united and prosperous Côte d'Ivoire by 2030. https://telecom.gouv.ci/new/uploads/publications/174196670372.pdf.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

To date, ARTCI has not yet formally expressed its position regarding the development prospects related to the strengthening of the legal and institutional framework for the protection of personal data.

Cybersecurity

The fifth edition of the Cyber Africa Forum 2025 will be held between 24-25 June 2025, in Cotonou, Benin.

This event brings together decision-makers and senior leaders from the digital sector in Africa.

The general commissioner announced that the two-day program will feature panels, keynote speeches, masterclasses, and competitions, including the Hacker Lab.

AI

Côte d'Ivoire has adopted a 2024-2027 roadmap for the development of artificial intelligence, based on the principles of digital sovereignty, ethics, and inclusion.

This strategic framework is built around three pillars: investment, inclusion, and governance, and aims to regulate the use of AI in key economic sectors while safeguarding fundamental rights.

The formulation of this public policy involved a multisectoral consultative process, engaging government bodies, the private sector, civil society, and academic institutions.

This strategic framework is reinforced by the national artificial intelligence strategy for 2030, whose mission is to promote inclusive technological, economic, and social transformation, while preserving and promoting Ivorian cultural identity.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Japan

Contacts

Hiroshi Suga

Partner, Deloitte Legal Japan

hiroshi.suga@tohmatsu.co.jp

Yosuke Araki

Manager, Deloitte Legal Japan

yosuke.araki@tohmatsu.co.jp

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Amendment to the Management Guidelines for Trade Secrets

The Unfair Competition Prevention Act provides civil remedies including injunctions and damages against acts of the wrongful acquisition, use and disclosure of trade secrets.

The Management Guidelines for Trade Secret (the Guidelines) address the definitions and other details of trade secrets including requirements for protection under the Unfair Competition Prevention Act.

The Guidelines were revised in March 2025 to further clarify the criteria for management of trade secrets based on the innovation, the changes in work styles and the accumulation of relevant court precedents in Japan and overseas.

The main points of the revision are;

- To clarify the concept regarding the subjects of confidentiality management measures;
- To reasonably classify regarding “the degree of confidentiality management measures”;
- To include specific examples of confidentiality management measures when using external cloud services and the utilization of Generative AI;
- To add that the requirement of usefulness is satisfied as long as the information is utilized in the business activities of the companies, regardless of the awareness of the third person who obtained the information;
- To clarify that even if trade secrets are published on the dark web as a result of hacking or other actions by third parties, the requirement “not publicly known” is not necessarily lost immediately; and
- To explain that if trade secrets can be extracted from product itself by reverse engineering, whether or not the trade secrets are publicly known depends on the difficulty of extraction.

A governmental alert to prevent from leak of personal data

Personal Information Protection Commission Issued an alert to prevent from leak of personal data caused by unauthorized computer access (the Alert) on 11 December 2024, suggesting that businesses handling personal information address to establish necessary security measures.

Under the Article 23 of the Act on the Protection of Personal Information, businesses handling personal information shall take the necessary and appropriate measures for managing the security of personal data including preventing the leaking, loss or damage of the personal data they handle.

The Alert provides eight categories of incidents that personal data was leaked from businesses handling personal information and reminded businesses handling personal information to take the necessary and appropriate measures for managing the security of personal data with referring to these incidents.

The eight categories which the Alert provides are:

- Cases where vulnerabilities were left unaddressed;
- Cases of delayed response to vulnerabilities;
- Cases of unauthorized logins;
- Cases targeting group companies or overseas offices;
- Cases of inadequate access control among group companies;
- Cases of data leaks involving information stored in personal areas;
- Cases of inadequate oversight of group companies; and
- Cases of data leaks from cloud services in use.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

A governmental alert regarding use of Generative AI service

The Personal Information Protection Commission issued an alert on 2 June 2024 (the Alert) concerning the use of Generative AI services. The Alert provides guidance on the handling of personal information when using Generative AI services by personal information handling businesses and administrative agencies.

The alert notes following two points:

- A business handling personal information must adequately ensure that the use is within the scope necessary to achieve the specified purposes of use for that personal information when it inputs prompts containing personal information into Generative AI services.
- A business handling personal information must thoroughly ensure that the provider of the Generative AI service does not use the personal data for machine learning or any other such purposes when it inputs prompts containing personal data into Generative AI services without obtaining the prior consent of the individual, and such personal data may be used for purposes other than generating responses to those prompts.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Enactment of the Act for Preventing Damage from Unauthorized Activities Directed at Critical Computers (the Cyber Response Capacity Enhancement Act)

The Cyber Response Capacity Enhancement Act (the Act) was enacted on 16 May 2025, the purpose of which is to prevent damage caused by unauthorized acts directed at critical computers of national entities, in light of the growing importance of ensuring cybersecurity for such computers – whose compromise could threaten national and public safety or have a significant impact on the lives of citizens and economic activities.

The Act mainly stipulates the following three points:

- Strengthening government-private collaboration: Improve information sharing with the government in the event that essential infrastructure service providers are cyberattacked, information sharing from the government to private businesses, and assistance in countermeasures.
- Use of communications information: Use and analysis of communications information to understand the actual situation of cyberattacks against Japan. These shall be checked by an independent agency. The secrecy of communications shall be carefully considered in designing these procedures.
- Provision of analysis and vulnerability information, etc.: To ensure cybersecurity, the Prime Minister shall organize and analyze the acquired information, including information related to incident reports, etc. by essential infrastructure service providers, and provide the information to administrative agencies that should conduct access and detoxification and other relevant administrative agencies. In addition, the Prime Minister may, when necessary, provide analyzed information to foreign governments, etc., and the competent minister for the business may, when necessary, provide the analyzed information to essential infrastructure service providers.

The main part of the Act will come into effect within a period not exceeding one year and six months from the date of promulgation (23 May 2025).

Guidelines for Cybersecurity in the Financial Sector

On 4 October 2024, the Financial Service Agency published the "Guidelines for Cybersecurity in the Financial Sector" (the Guidelines).

The Guidelines target financial institutions etc. and suggest that they adopt the substantial and effective cybersecurity systems from the viewpoint of the soundness and appropriateness of their business operations.

Under the Guidelines, financial institutions and related entities are required to take the following actions to establish substantial and effective cybersecurity systems:

- To establish the cybersecurity systems;
- To identify cybersecurity risks;
- To defend from cyberattacks;
- To detect cyberattacks;
- To address and recover from cyber incidents; and
- To manage third-party risks.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Guidelines for ensuring information security in critical infrastructure

The Ministry of Land, Infrastructure, Transport and Tourism published or revised the following cybersecurity guidelines for various critical infrastructure. These guidelines target businesses that operate critical infrastructure designated under the Basic Act on Cybersecurity and provide recommended measures for such businesses to refer to when implementing security measures.

- Safety Guidelines for Ensuring Information Security in the Aviation Sector (Revised on 25 April 2024);
- Safety Guidelines for Ensuring Information Security in the Airport Sector (Revised on 25 April 2024);
- Safety Guidelines for Ensuring Information Security in the Railway Sector (Revised on 18 April 2024);
- Safety Guidelines for Ensuring Information Security in the Water Supply Sector (Released on 5 March 2025);
- Safety Guidelines for Ensuring Information Security in the Logistics Sector (Truck Transportation) (Released on 18 April 2024);
- Safety Guidelines for Ensuring Information Security in the Logistics Sector (Warehousing) (Released on 18 April 2024);
- Safety Guidelines for Ensuring Information Security in the Logistics Sector (Vessel Operations) (Released on 26 April 2024);
- Safety Guidelines for Ensuring Information Security in the Port Sector (Revised on 28 March 2025).

Amendment to the Basic Act on Cybersecurity

The amendment to the Basic Act on Cybersecurity has come into effect since July 2025.

This amendment imposes information system providers to endeavor to support information system users so that the information system users can secure cybersecurity.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The Act on Promotion of Research and Development, and Utilization of AI-related Technology

The Act on Promotion of Research and Development, and Utilization of AI-related Technology (the AI Act) was enacted on 28 May 2025, and fully came into effect on 1 September 2025. The AI Act was the first statute in Japan that regulates the AI systems. The purpose of the AI Act is to promote innovation while mitigating risks so as to improve people's lives and develop the national economy.

The AI Act imposes on the Japanese government;

- To promote research and development, and the expansion and share of facilities and data;
- To ensure human resources, and to promote education;
- To participate in formulating international norms;
- To establish guidelines in accordance with the international norms;
- To collect information, investigating cases where human rights and interests are infringed; and
- To give guidance, advice and announcement to business operators and citizens.

In addition, under the AI Act, business operators have responsibility (not a duty to endeavor) to cooperate with measures implemented by the government and related authorities. The reason for imposing the business operators a "responsibility," not a "duty to endeavor," is that the business operators are in a closer position to AI users and engage in actions that have greater impacts on AI users.

AI Guidelines for Business Ver1.1

In November 2024, the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) published "AI Guidelines for Business Ver1.01," and then, in March 2025, they published "AI Guidelines for Business Ver1.1" (the Ver1.1 updates).

These guidelines are the guidelines updated from "AI Guidelines for Business Ver. 1.0," which 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.

The most part of these updates are merely minor revision, such as adding references or footnotes. However, the Ver1.1 updates also contains important revision regarding bias. For instance, the Ver1.1 updates provide an example of "biases not reflected in the training data" that sensitive attributes such as race or gender are inferred from related information even when they are removed from the data, or where biases arise from the combination of multiple attributes.

In addition, AI Guidelines for Business Appendix, which is an appendix for the AI Guidelines for Business, was also updated (AI Guidelines for Business Appendix Ver1.1). This update added some examples of efforts for the AI governance, which business operators can refer when they address the AI governance.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Checklist and Guidance regarding AI and Copyright

Agency for Cultural Affair provided "Checklist and Guidance regarding AI and Copyright" (the Checklist and Guidance) on 31 July 2024.

The Checklist and Guidance introduces recommended measures for reducing risks arising from the relationship between copyright and Generative AI, as well as for protecting and exercising one's own rights. It provides an easy-to-understand introduction to these measures from the perspectives of each of various stakeholders involved with Generative AI.

The Checklist and Guidance consist of two parts:

- Measures useful for reducing risks associated with the development, provision, and use of AI, primarily intended for those who develop and provide systems or services incorporating Generative AI, as well as for those who use AI systems or services in business or nonbusiness settings; and
- Explanations for copyright holders and other rights holders under copyright law, addressing topics such as how their works may be used in relation to Generative AI, what countermeasures can be taken against infringements, and what actions can be taken as rights holders to ensure the protection of their rights and the appropriate return of compensation.

The Checklist and Guidance provide measures useful for mitigating risks arising from the relationship between copyright and Generative AI, organized according to four stakeholder categories, AI developer, AI provider, AI business user, and common users.

It also notes that the risk mitigation measures for each stakeholder do not mean that stakeholders will immediately incur legal liability if they do not implement all of these measures as described, nor do they guarantee exemption from legal liability simply by implementing all of them.

Guidebook for the Utilization of Generative AI in Content Creation

Ministry of Economy, Trade and Industry published the Guidebook for the Utilization of Generative AI in Content Creation (the Guidebook) in July 2024, which introduces, to members of the industries involved in content creation, cases of Generative AI utilization in the game, animation, and advertising sectors, as well as points of caution and countermeasures for each usage scenario. It presents directions for the appropriate use of Generative AI in content creation, with careful consideration for the protection of intellectual property rights and other relevant interests. The Guidebook can be used for planning and considering content creation utilizing Generative AI, selecting Generative AI services to use, conducting legal checks, and drafting internal guidelines regarding the use of Generative AI.

The Guidebook mainly consists of three parts:

- Introduction;
- Use Cases of Generative AI; and
- Key Considerations and Countermeasures for Each Application Scenario of Generative AI.

The "Key Considerations and Countermeasures for Each Application Scenario of Generative AI" part contains (i) anticipated use cases and key considerations, (ii) overview of application scenarios and key considerations in each industry, and (iii) key considerations and countermeasures, which explains key considerations and countermeasures from the view of copyright, trademark and design, publicity right, human voice, and others.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Guidelines for the Utilization of Medical Digital Data in AI Research and Development

Ministry of Health, Labor and Welfare provided the Guidelines for the Utilization of Medical Digital Data in AI Research and Development (the Guidelines) in September 2024. The Guidelines consider a case where medical institutions, academic research organizations, and private companies engage in product development utilizing medical information held by medical institutions through joint research. They clarify the appropriate legal basis for the use of medical information according to the stage of research and development, and provide procedures for the creation and management of pseudonymized data, taking into account the characteristics of medical information. The Guidelines consists of the following contents:

- The utilization of medical data and its legal basis;
- Pseudonymized data and its joint use;
- Procedures for creating pseudonymized data taking into account the characteristics of medical information;
- Specific procedures for creating pseudonymized data according to the type of medical information; and
- The research and development cycle of medical devices and the positioning of various legal bases.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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 (PPC) began considering the three-year review, and in June 2024, it published an "Interim Report." After that, in December 2024, PPC released "Report of the Study Group on the Triennial Review of the Act on the Protection of Personal Information" (the Report).

The Report consists of following two discussion points;

- Administrative Monetary Penalty: The Report proposes to limit the scope of orders for administrative monetary penalty based on following requirements:
  - Limiting to acts in violation of important regulations;
  - Limiting to the case where a personal information handling business operator fails to exercise reasonable care to prevent violations;
  - Limiting to the case where an individual's rights and interests have been, or likely to be infringed; and
  - Limiting to large-scale violation.
- System for Injunctions and Damage Recovery by Organizations: The Report proposes to authorize qualified consumer organizations (defined in the Article 2, Section 4 of the Act on the Protection of Personal Information) to seek injunctions under the Act on the Protection of Personal Information as their own legal right.

The bill reflected above two points is expected to be submitted to the National Diet in this Fall.

Guidelines on Ensuring Compliance under the AI Act

Guidelines on Ensuring Compliance (the Guidelines) under the AI Act will be expected to be formulated around the beginning of 2026. A draft of the Guidelines will be discussed by the AI Strategic Headquarter and will be reported at a meeting of the AI Strategic Headquarter withing this year.

The AI Strategic Headquarter was established on 1 September 2025, based on Article 19 of the AI Act, and held the first meeting on 12 September 2025. The AI Strategy Headquarters, of which the Prime Minister is a chairman according to the Article 22, Section 1 of the AI Act, is responsible for drafting and promoting the implementation of the AI basic plan, as well as planning and formulating policies critical for the promotion of R&D, and utilization of AI-related technologies according to the Article 20 of the AI Act. It will discuss the Guidelines, an AI basic plan, and others from now on.

The following policies to draft the guidelines on ensuring compliance under the AI Act have been discussed in the AI Strategic Headquarter:

- To establish an environment in which businesses and citizens can trust and effectively utilize AI;
- With reference to international norms on AI, such as the outcome documents of the Hiroshima AI Process and the OECD AI Principles, to formulate guidelines to set forth approaches for the proper research, development, and utilization of AI; and
- To flexibly revise the guidelines in response to advancements in AI technology and changes in associated risks.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Luxembourg

Contacts

Thomas Held

Partner, Deloitte Legal Luxembourg

theld@deloittelegal.lu

Sophie Brisson

Managing Director, Deloitte Legal Luxembourg

sbrisson@deloittelegal.lu

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Continuous effort within the Luxembourg government's strategy related to the following matters:

Data Protection Authority (CNPD) guidance:

- Data subject rights: Detailed guides are published on how companies should handle requests from individuals regarding access, rectification, erasure and data portability.
- Sensitive data: Guidelines are developed on handling sensitive personal data, including practical examples.
- Security measures: The CNPD issues recommendations on implementing appropriate technical and organizational measures to protect personal data, including the use of encryption, pseudonymization, and access management.
- Trainings and conferences: The CNPD regularly offers trainings and conferences on data protection.

High-profile fines:

- Financial sanctions: The CNPD keeps imposing 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: Publication of decisions and fines to encourage all companies to strengthen their compliance efforts and highlight the importance of adhering to data protection regulations.

Sector-specific guidelines:

- Finance: Specific directives are 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 are provided on managing electronic medical records, patient confidentiality, and security protocols.
- Telecommunications: Guidelines exist to manage subscriber data, including data retention, protection against breaches, and user consent for marketing purposes.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The European Union Artificial Intelligence Act:

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (the AI Act) entered into force on 2 August 2024, and the first provisions became applicable in February 2025.

The AI Act is the first-ever comprehensive legal framework on AI worldwide. The AI Act sets out a clear set of risk-based rules for AI developers and deployers regarding specific uses of AI. The AI Act defines four levels of risk for AI systems: (i) minimal risk, (ii) limited risk, (iii) high risk, and (iv) unacceptable risk.

The implementation of the provisions of the AI Act is gradual in all EU member states, but certain provisions have already been applicable:

Since 2 February 2025:

- Banning certain AI practices deemed unacceptable (e.g., social scoring or subliminal cognitive manipulation); and
- The requirement for AI systems to be mastered by the operator concerned on 23 December 2024, Draft Law No. 8476 was issued to implement key provisions of the AI Act into Luxembourg law.

Since 2 August 2025:

- Transparency obligation for generative or interactive AI systems (which implies, for example, an explicit mention when a user interacts with an AI);
- Requirements for conformity assessment bodies;
- Criteria for the assessment of general-purpose AI models and their qualification according to the level of risk; and
- Possibility for providers of AI models to adopt a voluntary code of conduct (Chapter V of the Regulation.

At the national level, Draft Law No. 8476 was issued on 23 December 2024, to implement key provisions of the AI Act in Luxembourg law. The draft law provides, inter alia:

- The designation of the competent authorities;
- Measures to support AI innovation;
- Facilitating cooperation between stakeholders; and
- The definition of sanctions and redress mechanisms.

In order to ensure an effective and consistent implementation of the AI Act, the draft law foresees a significant expansion of the tasks of the Luxembourg National Commission for Data Protection (CNPD). Notably, the CNPD would have the following roles: (i) notified body, (ii) default market surveillance authority, (iii) establishment of a regulatory sandbox, (iv) single point of contact, and (v) fundamental rights authority.

Luxembourg's AI strategy:

- Published in May 2025, Luxembourg's AI strategy constitutes the national ambition aimed at accelerating the digital sovereignty of the Grand Duch by 2030.
- Luxembourg seeks to demonstrate how AI can benefit its citizens and businesses, achieve its ecological ambitions and share its experiences in the spirit of international cooperation.
- To achieve this, Luxembourg is committed to creating a trusted AI ecosystem that is coherent, inclusive and collaborative, involving the private, public and research sectors.
- A thriving and constructive AI ecosystem incorporates the following: (i) human-centered AI, (ii) effective and proactive public administration, (iii) strengthened competitiveness of businesses, and (iv) world-class research that draws and develops talents.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

By judgment dated 18 March 2025, the administrative court of Luxembourg dismissed the appeal filed by Amazon Europe Core S.à r.l. against the decision of 15 July 2021 of the CNPD, which had imposed an administrative fine of €746 million, ordered corrective measures under a daily penalty of €746,000, and required publication of the decision.

The court upheld the CNPD's findings that Amazon Europe Core S.à r.l., in processing personal data for interest-based advertising purposes, had infringed Articles 6, 12-17 and 21 of the GDPR. The violations related to the absence of a lawful basis for processing, failure to meet transparency and information obligations, breaches of data subjects' rights of access, rectification, erasure, and objection.

The court further noted that Amazon had failed to implement the required corrective measures to comply with the GDPR. It nevertheless granted suspensive effect to the appeal for the duration of the appeal proceedings.

The judgment of 18 March 2025, may be appealed before the administrative court.

Cybersecurity

Launch of the Luxembourg Cybersecurity Factory

A four-engine powered factory (Data Space, AI Hub, Open Source Communities, Quantum Lab) aiming at building an open cybersecurity data economy by fostering open and trusted cyber commons. This flagship project is part of Luxembourg's data/AI/quantum strategies, and relies on the following three pillars:

- Develop AI models to increase effectiveness in gathering and contextualizing of threat intelligence;
- Strengthening governance, risk management and compliance by and related to the adoption of AI technologies (also for SMEs); and
- Managing and testing inherent vulnerabilities of AI systems and helping the private sector to mitigate the quantum threat.

Luxembourg's data strategy – democratizing cybersecurity

Luxembourg is taking major steps to strengthen its cybersecurity ecosystem, particularly for SMEs, which make up over 95% of the EU economy but often lack access to affordable protection tools. The country's flagship initiative under the IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS) is the CLAUSEN project (CLoud and dAta SecUrity reSource cENter), designed to create Europe's first Open Cybersecurity Data Space (OCDS).

The initiative focuses on three priorities:

- AI-powered threat intelligence – turning raw data into actionable insights and "cyber weather reports" to strengthen national resilience.
- Support for SMEs – providing affordable, AI-based governance, risk, and compliance tools to help smaller firms manage cyber risks.
- Emerging tech risks – preparing for AI vulnerabilities and the quantum threat by promoting post-quantum cryptography and testing frameworks.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Malaysia

Contacts

Ho Wei Lih

Managing Partner, Wei Lih Ho & Co. (member of the Deloitte Legal network)

wlho@weilihho.com

Rebecca Chong

Associate, Wei Lih Ho & Co. (member of the Deloitte Legal network)

rchong@weilihho.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Amendments to the Malaysian Personal Data Protection Law

In July 2024, the Personal Data Protection (Amendment) Act 2024 (Amendment Act) was passed by both Malaysia's House of Representatives and Senate and received Royal Assent on 9 October 2024. The Amendment Act introduces significant changes to the Personal Data Protection Act 2010 (PDPA) with the aim of strengthening Malaysia's personal data protection framework and aligning it more closely with international standards.

The changes introduced by the Amendment Act came into force in three phrases, effective from 1 January 2025, 1 April 2025 and 1 June 2025, respectively.

Salient changes effective from 1 January 2025

The revisions that came into operation on 1 January 2025 relate to ancillary provisions of the PDPA, namely certain references to the commissioner in the Malay language version of the PDPA, the powers of the commissioner to open and maintain bank accounts, and the service of notices or other documents under the PDPA by electronic means.

The following transitional provisions also took effect on the same date:

- Any order, directions, circular or notice or code of practice issued by the commissioner before the commencement of the Amendment Act remains valid; and
- Any investigation, trial, proceedings or action pending before the coming into operation of the Amendment Act will be continued in accordance with the provisions of the PDPA as if it had not been amended by the Amendment Act.

Salient changes effective from 1 April 2025

Alignment of terminology

- A notable change under the Amendment Act is the substitution of the term "data user" with "data controller" in the PDPA, reflecting Malaysia's effort to align its data protection framework with internationally recognized terminology.

Key amendments to the definitions

- The definition of "sensitive personal data" is expanded to include "biometric data," which refers to any personal data resulting from technical processing relating to the physical, physiological or behavioral characteristics of a person. Thus, the processing of biometric data is subject to the same conditions applicable to the processing of sensitive personal data (e.g., with the explicit consent of the data subject);
- The definition of "data subject" is narrowed to exclude deceased individuals. In other words, the PDPA does not apply to any personal data of deceased individuals.

Increased penalties for noncompliance

- The maximum criminal penalties for breach of the seven personal data protection principles have been increased, with fines not exceeding MYR 1 million (previously MYR 300,000) and imprisonment for a term not exceeding three years (previously two years), or both.

Enhanced accountability for data processors

- Data processors now have a direct obligation to comply with the Security Principle under the PDPA when processing personal data on behalf of a data controller. Failure to do so may, upon conviction, result in criminal penalties of a fine not exceeding MYR 1 million, imprisonment for a term not exceeding three years, or both.

Data controller forum

- The Commissioner has enhanced powers to designate not only a body but also a data controller as a data controller forum in respect of a specific class of data controllers for the purposes of the PDPA.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Amendments to the Malaysian Personal Data Protection Law (cont.)

Cross-border personal data transfers

- Previously, a data controller could not transfer any personal data outside Malaysia unless to a place notified by the minister by publication in the Gazette, or where any of the conditions specified under Section 129(3) of the PDPA is met. Ultimately, no whitelisted countries were gazetted.
- The Amendment Act removes the previous whitelist regime, and now permits a data controller to transfer personal data to any place outside Malaysia if:
  - There is in that place in force any law which is substantially similar to the PDPA; or
  - That place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.
- The Amendment Act also removes the previously permitted condition under Section 129(3) of the PDPA that allowed the transfer of personal data outside Malaysia where such transfer was necessary to protect the vital interests of the data subject.
- On 29 April 2025, the commissioner issued the Personal Data Protection Guideline on Cross-Border Personal Data Transfer (CBPDT Guideline), which sets out the requirements to be met for compliance with the conditions for cross-border personal data transfers as specified under Section 129 of the PDPA.
- Notably, the CBPDT Guideline provides that in determining whether the receiving jurisdiction has laws substantially similar to the PDPA or affords an adequate level or at least equivalent level of protection as the PDPA, data controllers may conduct a transfer impact assessment (TIA). The minimum factors to be considered will differ depending on whether the assessment aims to determine the similarity of laws or the adequacy of protection in the receiving jurisdiction.
- The results of the TIA remain valid for a maximum of three years, after which the data controller would need to conduct a follow-up TIA. The data controller would need to conduct a review of any changes to the relevant personal data protection laws during the validity of the TIA to determine whether such laws are still substantially similar or afford adequate protection equivalent to the PDPA.

Salient changes effective from 1 June 2025

Appointment of Data Protection Officer

- Based on the Personal Data Protection Guideline on the Appointment of Data Protection Officer (DPO Guideline) and the Circular of Personal Data Protection Commissioner No. 2/2025 (Appointment of Data Protection Officer), data controllers and data processors are required to appoint a DPO if their processing of personal data involves:
  - Personal data exceeding 20,000 data subjects;
  - Sensitive personal data including financial information data exceeding 10,000 data subjects; or
  - Involves activities that require regular and systematic monitoring of personal data.
- Data controllers are required to notify the commissioner of the appointment of a DPO within 21 days thereof via the personal data protection system, and similarly, to notify any change to the appointment within 14 days thereof.
- The DPO may be an employee of the data controller or data processor or may be engaged through outsourcing services for a recommended minimum term of two years.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Amendments to the Malaysian Personal Data Protection Law (cont.)

- The DPO should possess sound knowledge of the PDPA, information technology, data security, business operations and personal data processing activities of the data controller or data processor. Further, the DPO should:
  - Be a resident in Malaysia (i.e. be physically present in Malaysia for at least 180 days in a calendar year) or otherwise easily contactable by any means; and
  - Be proficient in both the Malay and English languages.

Mandatory data breach notification

- According to the Personal Data Protection Guideline on Data Breach Notification (DBN Guideline) and the Circular of Personal Data Protection Commissioner 1/2025 (Data Breach Notification), a data controller is required to notify the commissioner, as soon as possible and no later than 72 hours thereafter, of any breach, loss, misuse or unauthorized access of personal data (personal data breach) if it causes or is likely to cause significant harm.
- A personal data breach is considered to cause or is likely to cause significant harm if there is a risk that the compromised personal data:
  - May result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
  - May be misused for illegal purposes;
  - Consists of sensitive personal data;
  - Consists of personal data or other personal information which when combined could potentially enable identity fraud; or
  - Is of significant scale (i.e., the number of affected data subjects exceeds 1,000).
- The data breach notification can be made by completing and submitting the notification form at www.pdp.gov.my or completing the notification form in Annex B of the DBN Guideline and submitting it to dbnpdp@pdp.gov.my or in hardcopy to the commissioner.
- The data controller is also required to notify the affected data subjects, without unnecessary delay and in any event no later than seven days after the initial data breach notification to the commissioner, of a personal data breach that results in or is likely to result in significant harm to the data subjects.
- Other than the "significant scale" criterion, the definition of significant harm applicable to notification to the commissioner shall apply equally for the purpose of notification to data subjects.
- The notification to the affected data subjects must be provided directly and individually to the data subjects in a practicable manner using intelligible language appropriate to the circumstances in order to allow them to take necessary precautions or measures to protect themselves against possible adverse effects of the breach.
- The DBN Guideline prescribes certain minimum information relating to a personal data breach that must be included in the notification submitted by the data controller to the commissioner and the affected data subjects.

Rights to data portability

- The Amendment Act introduces a new right of data portability pursuant to which a data subject may request the data controller to transmit his personal data to another data controller of his choice directly by giving written notice via electronics means to the data controller.
- Upon receipt of such request, the data controller must complete the transmission of personal data within the prescribed period, subject to technical feasibility and compatibility of the data format.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cyber Security Act 2024

On 26 June 2024, the Cyber Security Act 2024 (CSA) of Malaysia was published in the Official Gazette and, together with the following four regulations (collectively, Regulations), came into force on 26 August 2024:

- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024;
- Cyber Security (Notification of Cyber Security Incident) Regulations 2024;
- Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024; and
- Cyber Security (Compounding of Offences) Regulations 2024.

The highly anticipated CSA signifies a key milestone in Malaysia's efforts to combat cyberthreats by introducing a comprehensive national cybersecurity framework.

Extra-territorial application

The CSA has extra-territorial application – it applies to any person, irrespective of nationality or citizenship, and to offences committed within or outside Malaysia, where the national critical information infrastructure is located wholly or partly in Malaysia.

The National Cyber Security Committee and the Chief Executive

The CSA establishes the National Cyber Security Committee (Committee) which is chaired by Malaysia's premier. The Committee's functions include advising on and formulating policies, strategies and strategic measures relating to national cybersecurity, and giving directors to the Chief Executive of the National Cyber Security Agency (NACSA) and NCII Sector Leads on national cybersecurity matters.

On the other hand, the chief executive is tasked with, among others, implementing the policies, strategies and strategic measures made and directions given by the committee or the federal government on national cybersecurity matters.

National critical information infrastructure

The CSA centers around the concept of a national critical information infrastructure (NCII), which is a computer or computer system which the disruption to or destruction of would have a detrimental impact on the delivery of any service essential to the security, defense, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the federal or any state government to carry out its functions effectively.

NCII sectors

The CSA identifies the following as NCII sectors (each an NCII Sector): government; banking and finance; transportation; defense and national security; information, communication and digital; healthcare services; water, sewerage and waste management; energy; agriculture and plantation; trade, industry and economy; and science, technology and innovation.

NCII sector leads

The Prime Minister had on 11 September 2024 appointed sector leads for each NCII sector (NCII Sector Lead).
The NCII Sector Lead is responsible for, among others, designating any government entity or person that owns or operates a NCII as an NCII entity (NCII Entity) within its appointed NCII Sector, and preparing a code of practice that sets out the measures, standards and processes for ensuring the cybersecurity of a NCII within its NCII Sector.
In relation to the former, the chief executive has, pursuant to his powers conferred by the CSA, issued the Chief Executive Directive No. 3: Determination of National Critical Information Infrastructure Entity (effective 18 September 2024). This directive sets out, among others, the criteria and procedures for an NCII Sector Lead to designate an NCII Entity.
As for the latter, the chief executive has issued the Chief Executive Directive No. 7: Preparation of Codes of Practice by the National Critical information Infrastructure Lead (effective 25 March 2025), which prescribes the requirements and guidelines for the preparation of a code of practice by an NCII Sector Lead.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cyber Security Act 2024 (cont.)

NCII entities

An NCII Entity has the following duties under the CSA:

- **Provision of information:** The NCII Entity is required to provide its NCII Sector Lead with information on the NCII it owns or operates, upon request. Additionally, the NCII Entity must notify its NCII Sector Lead of any new NCII that it procured or comes within the possession or control of the NCII Entity, and of any material change (i.e. any change that affects or may affect the cybersecurity of the NCII or the NCII Entity's ability to respond to a cybersecurity threat or incident) to the design, configuration, security, or operation of the NCII it owns or operates.
- **Implementation of code of practice:** The NCII Entity is required to implement the measures, standards, and processes in the code of practice issued by its NCII Sector Lead, or alternatively any other measures, standards and processes of equal or a higher level of protection. The NCII Entity may also in addition to the foregoing, establish and implement cybersecurity measures, standards and processes based on internationally recognized standards or frameworks.
- **Cybersecurity risk assessment:** The NCII Entity is required to conduct a cybersecurity risk assessment in respect of the NCII it owns or operates in accordance with the code of practice at least once a year, and cause to be carried out an audit by an auditor approved by the chief executive at least once in every two years. Such risk assessment or audit report must be provided to the chief executive within 30 days after its completion. The chief executive has issued the Chief Executive Directive No. 5: Cyber Security Risk Assessment (effective 10 October 2024) and the Chief Executive Directive No. 8: Cyber Security Audit for National Critical Infrastructure Entities (effective 17 July 2025), which outlines the scope, process and criteria of the cybersecurity risk assessment report and the cybersecurity audit respectively. An example of a cybersecurity risk assessment report can be found on NACSA's website.
- **Incident reporting:** If an NCII Entity becomes aware of a cybersecurity incident that has occurred or might have occurred in respect of the NCII it owns or operates, it must notify the chief executive and its NCII Sector Lead. The initial notification must be made within six hours of the NCII Entity becoming aware of such incident, followed by a comprehensive incident report within 14 days of the initial notification. The Cyber Security (Notification of Cyber Security Incident) Regulations 2024 specify the information required to be included in both the initial notification and the comprehensive incident report, while the Chief Executive Directive No. 1: Cyber Security Incident Reporting (effective 26 August 2024) prescribes the procedures for incident reporting and sets out additional obligations to ensure compliance with the reporting obligation.
- **Cybersecurity exercise:** The chief executive may conduct a cybersecurity exercise to assess the readiness of any NCII Entity in responding to a cybersecurity threat or incident. To this end, the chief executive may give directions to the NCII Entity as they deem necessary for the purpose of publishing the cybersecurity exercise in the Gazette, and the NCII Entity is obliged to comply with such directions.

Licensing of Cyber Security Service Provider

The CSA, read together with the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024, requires any person who provides, advertises or otherwise holds himself out as providing any cybersecurity service relating to managed security operation center monitoring service and penetration testing service to obtain a license from the chief executive.

Managed security operation center monitoring service refers to a service for:

- Monitoring the level of cybersecurity of a computer or computer system of another person by acquiring, identifying or scanning information that is stored in, processed by or transmitted through, the computer or computer system for the purpose of identifying or detecting cybersecurity threats to the computer or computer system; or
- Determining the measures necessary to respond to or recover from any cybersecurity incident and to prevent such cybersecurity incident from occurring in the future.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Whereas penetration service testing refers to a service for assessing, testing or evaluating the level of cybersecurity of a computer or computer system, by searching for vulnerabilities on, and compromising, the cybersecurity defenses of the computer or computer system, and includes any of the following activities:

- Determining the cybersecurity vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of;
- Determining or testing the organization's ability to identify and respond to cybersecurity incident through simulation of attempts to penetrate the cybersecurity defenses of the computer or computer system;
- Identifying and measuring the cybersecurity vulnerabilities of a computer or computer system, indicating vulnerabilities and preparing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk; or
- Utilizing social engineering to assess the level of vulnerability of an organization to cybersecurity threats.

This licensing requirement does not apply where the cybersecurity service is provided by a government entity, by a person (other than a company) to its related company, or in respect of a cybersecurity service for a computer or computer system located outside Malaysia. The license is valid for one year, with a license fee of MYR 400 for individual applicants and MYR 1,000 for nonindividual applicants for each type of service. The chief executive has since issued the Chief Executive Directive No. 2: Licensing of Cyber Security Service Provider (effective 26 August 2024) which outlines the procedures to apply for this license.

National Cyber Security Baseline

On 1 October 2024, NACSA introduced the National Cyber Security Baseline (NCSB), which is a set of minimum security controls and best practices that organizations need to implement and ensure a basic level of cybersecurity protection.

The NCSB is structured around six core domains: govern, identify, protect, detect, respond, and recover. These six core domains are divided into 15 cybersecurity categories and further broken down into 33 cybersecurity elements. These domains cover the full range of cybersecurity management, including governance and policy oversight, asset identification and protection, threat detection, incident response, and rapid recovery.

In this regard, the chief executive has issued the Chief Executive Directive No. 4: National Cyber Security Self Assessment (effective 1 October 2024), requiring all NCII Entities to complete the NCSB Self-Assessment within two weeks from the date they are designated as an NCII Entity. Once completed, the NCII Entity is required to submit the self-assessment to the chief executive of NACSA via email, as well as to their respective NCII Sector Lead. The format of the NCSB Self Assessment is available on NACSA's website.

Implementation of Post-Quantum Cryptography Migration by NCII Entities

The chief executive has recently issued the Chief Executive Directive No. 9: Preparation of Data and Information on the Implementation of Post-Quantum Cryptography Migration by National Critical Information Infrastructure Entities (effective 22 September 2025). Under this directive, NCII Entities are required to prepare and furnish to the chief executive data and information on their implementation of post-quantum cryptography (PQC) migration, as specified in Appendix A to this directive, in such form and manner as may be specified in a written notice issued by the chief executive, within three months from the date of such notice.

Exempted entities

On 28 January 2025, the Cyber Security (Exemption) Order 2025 was published in the Official Gazette and came into force on 1 February 2025. Under this order, the following persons are exempted from all provisions of the CSA: Amazon Data Services Malaysia Sdn. Bhd.; Amazon Web Services Malaysia Sdn. Bhd.; Google Asia Pacific Pte. Ltd.; Google Cloud Malaysia Sdn. Bhd.; Google Malaysia Sdn. Bhd.; Microsoft Knowledge Capital Sdn. Bhd.; Microsoft (Malaysia) Sdn. Bhd.; Microsoft Payments (Malaysia) Sdn. Bhd.; and Pearl Computing Malaysia Sdn. Bhd.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

National Guidelines on AI Governance and Ethics

At present, there is no specific legislation in Malaysia on AI governance. However, in September 2024, the Ministry of Science, Technology and Innovation (MOSTI) issued the National Guidelines on AI Governance and Ethics (AIGE Guidelines). The AIGE Guidelines serve as a nonbinding reference framework for the following three categories of AI stakeholders: (i) AI end-users, (ii) policymakers of government, agencies, organizations and institutions, and (iii) developers, designers, technology providers and suppliers (collectively, the AI Stakeholders), pending the formulation of comprehensive AI legislation. The AIGE Guidelines form part of the government's initiatives to support the implementation of the National Artificial Intelligence Roadmap 2021-2025 (AI-Rmap).

The AIGE Guidelines prescribe seven AI principles (AI Principles) summarized as follows:

- Fairness: AI systems must be designed in a manner that does not contain bias or discrimination against target users.
- Reliability, safety, and control: AI systems should be designed to be safe, secure, and resilient against unauthorized access. Developers must ensure lawful and nondiscriminatory use of data, obtain consent where necessary, and adopt security-by-design and privacy-by-design principles and international standards relating to information security and privacy.
- Privacy and security: AI systems must be robustly tested to be reliable, safe and fail-safe so that users can trust and depend on them. They should operate reliably and consistently under both normal and unexpected conditions.
- Inclusiveness: AI must be inclusive of all stakeholders and ensure equal access across all segments of society.
- Transparency: AI algorithms should be transparent for stakeholders to evaluate the risks involved and address issues that may arise.
- Accountability: AI developers, owners and actors should be responsible and held accountable for the proper functioning of AI systems.
- The pursuit of human benefit and happiness: AI systems should be designed in a manner that is aligned with human-centered values, promote societal well-being, enhance quality of life, and contribute to human happiness. They should not be used for malicious purposes.

The AIGE Guidelines describe in detail the application of the AI Principles apply to each category of AI Stakeholders and provide guidance on responsible AI practices for adoption by each category.

The establishment of a National AI Office

On 12 December 2024, the National AI Office (NAIO), a key initiative under the Ministry of Digital, was launched. This office is designed to position Malaysia as a regional leader in AI and a global driver of digital transformation. NAIO has been tasked with fostering innovation, promoting cross-sector collaborations, and integrating AI into government, industry and societal frameworks. NAIO will operate under the guidance of MyDIGITAL Corporation within its first year, and will spearhead efforts in AI research, adoption, and commercialization to improve the digital economy and public services.

On 14 February 2025, NAIO announced the establishment of seven specialized working groups to drive Malaysia's AI agenda. NAIO has engaged a diverse pool of experts and community representatives with expertise in technology, policy, ethics, security, education and societal impact to contribute to these working groups.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The working groups officially commenced work in February 2025, and their key focus areas of the working groups are as follows:

- AI Sovereignty: Enhancing Malaysia's control over AI technologies, data and infrastructure;
- AI Regulation and Policy: Developing a regulatory framework and national strategic roadmap for AI development;
- AI Security: Addressing risks and threats related to AI to safeguard national and digital security;
- AI Governance and Ethics: Implementing governance models and ethical guidelines;
- AI Safety: Ensuring AI systems are trustworthy, reliable and aligned with public interest;
- AI Talent: Developing a robust AI talent pipeline in Malaysia; and
- AI Advisory: Offering insights on the latest AI trends and challenges faced in AI implementation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

New guidelines to supplement the PDPA

In January 2024, Malaysia's Digital Minister had announced plans for the issuance of seven new guidelines under the PDPA. Since then, the commissioner has issued the following guidelines:

- The Data Breach Notification Guideline (issued on 25 February 2025);
- The Data Protection Officer Guideline (issued on 25 February 2025); and
- The Cross-Border Personal Data Transfer Guideline (issued on 29 April 2025).

With the following four highly anticipated guidelines still pending issuance:

- The Data Portability Guideline;
- The data protection impact assessment;
- The Privacy by Design Guideline; and
- The Profiling and Automated Decision-Making Guideline.

While public consultation papers have been issued in respect of all seven guidelines, the focus will on those relating to the four pending guidelines with the aim of providing insight into what may be expected in these upcoming guidelines. The commissioner has also issued the Public Consultation Paper No. 4/2024: Personal Data Protection Standards and the Public Consultation Paper No. 4/2025: Proposed Amendments to the Personal Data Protection Regulations 2013 which outlines proposals to revise the existing Data Protection Standards 2015 and Personal Data Protection Regulations 2013, respectively.

Public Consultation Paper No. 3/2024: The Right to Data Portability

According to the Public Consultation Paper No. 3/2024: The Right to Data Portability, a proposed Personal Data Protection (Right to Data Portability) Regulations (Data Portability Regulations) and Data Portability Guideline are being developed. It is also proposed that:

- Data controllers be required to transmit only personal data belonging to categories listed in a whitelist to be issued by the commissioner, data controller forum or relevant regulator.
- The right to data portability be limited to personal data that is:
  - Directly provided by the data subject;
  - Processed based on consent or a contract to which the data subject is a party;
  - Processed by automated means; and
  - Not classified as inferred data or derived data.

Public Consultation Paper No. 1/2025: DPIA Guideline

In the Public Consultation Paper No. 1/2025: Data Protection Impact Assessment Guideline, the following two-tier approach is proposed:

- Quantitative threshold: Data controller to determine if the following quantitative thresholds are met, and if so, a data protection impact assessment (DPIA) will need to be conducted:
  - Processing of sensitive personal data involving more than 10,000 data subjects;
  - Processing of personal data for automated decision-making purposes involving more than 10,000 data subjects; or
  - Processing of personal data is expected to involve more than 20,000 data subjects,
- Qualitative threshold: If the quantitative threshold is not met, the DPO to consider the following qualitative factors to determine whether a DPIA is required:
  - Potential legal or significant effects on data subjects;
  - Systematic monitoring of publicly accessible area;
  - Use of innovative technology;
  - Denial or restriction of right of data subjects;
  - Tracking of data subjects' location or behavior; and
  - Targeting of children or other vulnerable individuals.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Public Consultation Paper No. 2/2025: Data Protection by Design Guideline

The Public Consultation Paper No. 2/2025: Data Protection by Design Guideline offers insight into the implementation of data protection by design (DPbD), and proposes the following seven foundational principles for adoption of DPbD by data controllers:

- Proactive not reactive, preventive not remedial;
- Privacy as the default setting;
- Privacy embedded into design;
- Full functionality – positive sum, not zero sum;
- End-to-end security – full lifecycle protection;
- Visibility and transparency – keep it open; and
- Respect of user privacy – keep it user-centric.

Public Consultation Paper No. 3/2025: Automated Decision Making and Profiling Guideline

The Public Consultation Paper No. 3/2025: Automated Decision Making and Profiling Guideline proposes that automated decision-making (ADM) (and by extension profiling) be regulated if it results in legal effects concerning the data subject or significantly affects the data subject. To this end, it is proposed that a data subject be accorded with the following rights:

- Right to refuse to be subjected to a decision based solely on ADM (including profiling) which produces legal effects concerning the data subjects or significantly affects the data subject;
- Right to information on the ADM being undertaken; and
- Right to request a human review of the ADM.

Subject to specific exceptions, it is also proposed that ADM involving sensitive personal data be only allowed with the data subject's explicit consent or where it is necessary for public interest reasons and suitable measures have been put in place to safeguard the data subject's rights.

New Cybercrime Bill

A new Cybercrime Bill is currently being drafted and is expected to be tabled in Parliament before the end of year 2025. The proposed bill is intended to replace the Computer Crimes Act 1997, which is generally considered to be outdated and less relevant in addressing current day cyberthreats.

New National AI Action Plan 2026-2030

NAIO is currently developing the National AI Action Plan 2026-2030 (Action Plan) which serves as a continuation of the AI Roadmap 2021-2025 and is expected to expand on the existing AIGE Guidelines. The Action Plan aims to promote collaboration among the government, industries, academia and the wider community, facilitate knowledge sharing, boost AI adoption across key sectors, and develop sustainable human capital within the national AI ecosystem.

NAIO has convened four strategic roundtable sessions in respect of the Action Plan, focusing respectively on AI safety and security, policy regulation, talent, and advisory and industry engagement.

At the AI safety and security roundtable, NAIO presented proposed safety components of the Action Plan, which include a regulatory baseline supported by voluntary guidelines, a tiered risk classification model aligned with international standards, a dedicated risk function and incident response function to monitor AI-related harms.

During the policy and regulation roundtable, stakeholders discussed the proposed hybrid-tiered regulatory model, which combines principles-based oversight by NAIO with sector-specific mechanisms led by relevant regulators and incorporates a blend of hard-law and soft-law instruments (e.g., standards and circulars).

The discussions at the AI talent roundtable focused on strengthening Malaysia's AI talent pipeline, encompassing initiatives from early education to workforce reskilling. The advisory and industry roundtable brought together leaders from Konsortium AI Negara and the AI Advisory Working Group to discuss the alignment of national AI strategies with actual industry needs.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Malta

Contacts

Gianluca Busuttil

Senior Manager, Deloitte Legal Malta

gbusuttil@deloitte.com.mt

Michael Agius

Senior Manager, Deloitte Legal Malta

magius@deloitte.com.mt

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The Information and Data Protection Commissioner's (IDPC) Guidelines on the processing of personal data relating to the employment sector

Processing of employees' biometric data

Employers may only implement biometric systems in the workplace under stringent conditions. The processing must be both proportionate and necessary to achieve the intended purpose.

- Employers must consider less intrusive alternatives and obtain explicit employee consent before processing biometric data, except in specific cases requiring strict security measures.
- A DPIA is required prior to processing biometric data, carefully evaluating and documenting the potential impact on employees, ensuring full compliance with GDPR requirements.

Managing employee email accounts

Employers must balance business continuity with employee data privacy by limiting work email use to work purposes.

- Policy must be in place to ensure that employees distinguish personal from work emails.
- Upon an employee's departure, employers should allow them to delete any personal emails, restrict mailbox access, and use automatic replies to inform contacts of an employee's departure.
- Automatic email forwarding rules should be avoided.

Employee monitoring

Employers may require employees to use webcams at specific times for legitimate purposes.

- However, continuous monitoring is invasive and must be necessary, proportionate, and justified under data protection laws.
- Employers must inform employees transparently about monitoring software or webcam use and ensure monitoring respects employees' privacy rights and is legally compliant.

Processing employees' police conduct certificates

As a general rule, employers cannot retain police conduct certificates of employees, including prospective employees.

- Employers can have a legitimate interest to request police conduct to verify whether a current or prospective employee, has a clean conduct and no prior criminal convictions.
- Once the individual has presented the certificate to the employer, the employer may document it, however, any physical/digital copies of the certificate itself should be deleted.

Preemployment medical checks

The guidelines lay down the following with regards medical screening of prospective and current employees.

Prospective employees:

- Employers cannot require medical tests during recruitment but may do so for selected candidates to confirm fitness, provided candidates are informed of this possibility at recruitment stage. Refusal to undergo tests cannot be grounds for rejection.

Current employees:

- Medical data is considered 'special category personal data' under Article 9(2) GDPR and, so, requires enhanced protection. A proportionality assessment should be carried out to evaluate whether the medical examinations/tests are justified and necessary.

Data retention

- Personal data must not be retained longer than necessary for its processing purpose.
- Controllers are responsible for justifying and setting reasonable retention periods through risk-based assessments considering legal, operational, and purpose-related factors.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

IDPC Decision: CDP/COMP/151/2025, 26 May 2025

Complaint regarding unauthorized disclosure of reasons for resignation

Employer emailed entire team (30 staff) disclosing complainant's resignation and personal family-related reasons without complainant's consent.

The employer claimed that sending such an email was standard practice for business continuity and relied on legitimate interest under Article 6(1)(f) GDPR, arguing that no sensitive data was disclosed.

Commissioner confirmed the email contained personal data under GDPR and no prior authorization from the employee was obtained.

Applying the CJEU three-part test for legitimate interest, the commissioner found:

- The legitimate interest of the employer was valid;
- The disclosure of personal reasons was not necessary to achieve business continuity; and
- Therefore, necessity test failed (balancing test was not assessed).

The employer's disclosure of personal reasons was unlawful and could not be justified under Article 6(1)(f) GDPR.

LN 227 of 2025, the Artificial Intelligence (Designation of the Information and Data Protection Commissioner for the purposes of Regulation (EU) 2024/1689) Regulations

IDPC designated as a Market Surveillance Authority for certain high-risk AI systems under Annex III of the AI Act

The IDPC, as the designated market surveillance authority of certain high-risk AI systems, may institute enforcement action applicable to infringements of the AI Act committed by operators,

The high-risk AI systems under the IDPC's surveillance are:

- High-risk biometric systems insofar as the systems are used for law enforcement purposes, border management, and justice and democracy, where permitted by law;
- High-risk systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services;
- High-risk systems used for law enforcement, insofar as their use is permitted by law;
- High-risk systems used for migration, asylum and border control management, in so far as their use is permitted by law; and
- High-risk systems used for administration of justice and democratic processes.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Transposition of the EU Cybersecurity Framework in Malta

With the Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, Malta has transposed the NIS2 Directive (EU 2022/2555) into national law, significantly strengthening the country's cybersecurity regime and aligning it with the latest EU standards. The directive and its implementing measures aim to enhance the security and resilience of essential and important entities across a wide range of critical sectors, and to standardize incident response and regulatory oversight across the EU. The new Maltese framework provides for:

- The establishment of the Critical Infrastructure Protection Department (CIPD) as the main national cybersecurity regulator, responsible for compliance oversight, audits, and enforcement of penalties.
- The designation of CSIRT-Malta as the national Computer Security Incident Response Team, coordinating incident responses, managing Coordinated Vulnerability Disclosures (CVD), and supporting affected entities.
- The introduction of a formal national CVD framework, allowing individuals and organizations to safely report ICT vulnerabilities, with legal protections for authorized reporters.
- Strict incident reporting obligations requiring entities to notify CSIRT-Malta of significant cyber incidents within 24 hours (initial alert), 72 hours (detailed report), and one month (final report).
- The imposition of substantial fines for noncompliance (up to €10 million or 2% of global turnover for essential entities, and €7 million or 1.4% for important entities), as well as potential operational suspensions and personal liability for senior management.
- Mandatory cybersecurity training for management and the requirement for senior leadership to approve and oversee cybersecurity measures.

Implementation of the Digital Operational Resilience Act (DORA) in Malta

With the full application of Regulation (EU) 2022/2554 (DORA) on 17 January 2025, Malta has established a harmonized framework for digital operational resilience in the financial sector, aligning national requirements with EU standards. DORA aims to ensure that financial entities can effectively manage ICT-related risks, respond to cyberthreats, and maintain business continuity. The Maltese DORA framework provides for:

- The issuance of targeted guidance and circulars by the Malta Financial Services Authority (MFSA), strengthening local cybersecurity oversight and compliance;
- Mandatory submission of the Register of Information (RoI) by financial entities, supporting enhanced ICT risk management and regulatory visibility;
- The establishment of national Threat-Led Penetration Testing through the TIBER-MT framework, enabling advanced resilience testing and sector-wide threat intelligence sharing;
- Updates to the Financial Institutions Rulebook, aligning requirements for ICT risk management, incident reporting, and third-party oversight with DORA standards;
- Comprehensive incident reporting obligations, ensuring timely notifications and management of ICT-related disruptions and cyber incidents;
- Rigorous oversight of third-party ICT service providers, including contractual and governance requirements to mitigate outsourcing risks; and
- The embedding of DORA's operational resilience at the national level, promoting robust cybersecurity practices and effective governance across Maltese financial institutions.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

MFSA Cybersecurity Supervisory Priorities for 2025 and Cyber Finance Summit 2025

Strengthening sector-wide cyber risk management

In 2025, the MFSA is advancing its cybersecurity supervisory approach through enhanced sectoral engagement, data-driven oversight, and alignment with European Supervisory Authorities. The MFSA has released its 2025 supervisory priorities, which, among other areas, set out the following cybersecurity-related priorities:

- Cross-sectoral engagement and data-driven analysis to identify and address emerging ICT risks across financial entities;
- Emphasis on board-level oversight of ICT risk, reinforced through regular 'Dear CEO' letters outlining supervisory expectations and best practices;
- Outcomes-based supervisory assessments, with findings used to guide remedial actions and inform future supervisory cycles;
- Promotion of collaboration among financial institutions, ICT third-party providers, law enforcement, and digital forensics experts, as highlighted during the Cyber Finance Summit 2025;
- Continuous improvement in cybersecurity practices, informed by lessons learned from incident reporting and supervisory feedback; and
- Proactive preparation for future regulatory developments, ensuring the financial sector maintains a resilient and secure digital development.

Cyber Finance Summit 2025 – Advancing Malta's digital resilience

On 15-16 October 2025, the Mediterranean Conference in Valletta hosted the MFSA's Cyber Finance Summit 2025. The event brought together financial regulators, industry leaders, ICT service providers, and cybersecurity experts from Malta and abroad, fostering a collaborative environment to address the evolving cybersecurity landscape. The key elements of the summit included:

- The summit featured keynote speeches, expert panels and thematic sessions covering:
  - The generic threat landscape and organized crime;
  - Achieving cyber resilience from a macro-prudential perspective; and
  - Regulatory updates on Malta's supervisory advancements.
- Insights from distinguished speakers, including cyber-policy authorities, law enforcement, central bank officials, and MFSA leads; and
- Identification of three strategic priorities for Malta's financial sector:
  - Cross-sector collaboration to address complex cyber risks;
  - Enhanced governance and accountability at board and senior management levels; and
  - Regulatory foresight to anticipate future threats and supervisory developments.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

EU AI Act institutional designations and national legal instruments

Malta has finalized its core institutional designations and issued key legal instruments to implement the new AI regulatory framework:

- The Government Gazette published Legal Notice 226 of 2025, the Artificial Intelligence Regulations, 2025 (under the Malta Digital Innovation Authority Act). This legal notice establishes the Malta Digital Innovation Authority's (MDIA) regulatory responsibilities, detailing its duties for market surveillance, procedural arrangements for supervised testing, and the operation of recognition and sandbox regimes for AI systems.
- Separately, Legal Notice 227 of 2025, the Artificial Intelligence (Designation of the Information and Data Protection Commissioner for the purposes of Regulation (EU) 2024/1689) Regulations, 2025 designates the Information and Data Protection Commissioner (IDPC) for specific market surveillance and fundamental rights monitoring functions. This applies particularly to AI systems that significantly impact personal data and related rights.
- The IDPC has issued explanatory materials outlining its role as the national Fundamental Rights Authority for AI-related personal data matters. These materials clarify the scope of the IDPC's oversight, especially regarding certain high-impact AI systems that raise fundamental rights or data protection concerns;
- Together, L.N. 226 and L.N. 227 provide the formal legal basis for Malta's AI regulatory architecture:
  - L.N. 226 operationalizes the MDIA's supervisory tools and sandbox regime; and
  - L.N. 227 clarifies the IDPC's mandate for data protection and fundamental rights oversight in the context of AI.
- These instruments ensure clear allocation of responsibilities, supporting effective supervision, innovation, and the protection of fundamental rights as Malta enacts the AI Act.

Prohibitions, phased national effect, and implications for Maltese deployment

Malta has clearly articulated the national legal effect of AI prohibitions and the phased compliance obligations for operators through its legal instruments and regulatory guidance:

- Maltese guidance documents, including MDIA web pages and IDPC communications, specify categories of AI systems that are strictly prohibited from being placed on the domestic market. These include:
  - Social scoring by public authorities;
  - Subliminal manipulative systems;
  - Untargeted scraping of facial image databases;
  - Emotion-recognition technologies in sensitive settings; and
  - Real-time biometric identification in public spaces (except where narrowly authorized by law).
- Both public sector bodies and private operators in Malta have been instructed to review all live AI deployments and to cease or withdraw any systems that fall within these banned categories, ensuring immediate compliance with national and EU-level prohibitions.
- For general-purpose and high-impact AI models, MDIA guidance requires providers to prepare comprehensive technical documentation, conduct system-level risk assessments, and complete Fundamental Rights Impact Assessments (FRIA) using MDIA templates and the AI Self-Assessment Toolbox. These steps must be completed prior to seeking system recognition or participation in the regulatory sandbox.
- The combined effect of Malta's guidance and legal notices is immediate and unambiguous: AI systems deemed unacceptable are not permitted for use in Malta, while high-impact models must follow a structured, documented pathway to lawful deployment.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

MDIA operational tooling, Technology Assurance Sandbox, and TARF deployment

With Legal Notices No. 226 and 227 of 2025, Malta transposed the EU AI Act into national law. Regulated firms should prioritize the following:

- Malta has introduced a suite of practical compliance tools through the MDIA to support AI regulation and innovation.
- The MDIA now offers several operational instruments, including the AI Classification Guide, AI Compliance Role Finder (v1), and the AI Self-Assessment Toolbox. These resources enable Maltese AI providers and deployers to:
  - Determine whether a system falls within Malta's regulatory scope;
  - Identify their stakeholder role (provider, deployer, importer, distributor); and
  - Conduct an initial conformity triage to assess regulatory obligations.
- The Technology Assurance Sandbox (TARF) and the broader Technology Sandbox framework have been expanded to facilitate phased, low-cost participation for start-ups and innovators. Within this environment, participants can validate their compliance controls, maintain audit logs through a forensic node, and designate a technical officer responsible for failure reporting and incident management.
- The TARF Guidelines and dedicated sandbox web pages outline the staged assessment process, documentation requirements, and the availability of government grants to subsidize system auditor costs. These guidelines clarify expectations for each stage of the sandbox, from initial entry to full recognition.
- Collectively, these instruments establish a Malta-centric pathway from prototype development through supervised testing to recognized assurance. This approach reduces time-to-market for innovative AI solutions while ensuring that essential documentation such as FRIA and technical files is integrated throughout the product lifecycle.
- By operationalizing these tools, the MDIA supports both regulatory compliance and responsible innovation, positioning Malta as a leader in AI governance and technology assurance.

National AI Strategy: "Malta - The Ultimate AI Launchpad (Strategy and Vision 2030)"

Malta's national AI strategy, "Malta: The Ultimate AI Launchpad - Strategy and Vision for Artificial Intelligence in Malta 2030," remains the government's key operational framework:

- Over the past year, the MDIA has actively updated and promoted the strategy to align industrial incentives, skills programs, and regulatory tools with new legal requirements.
- The updated plan now directly connects MDIA sandboxing, funding opportunities, university-industry partnerships, and sector-specific pilots (finance, gaming, healthcare, transport) to practical compliance pathways, including FRIA training, technical documentation templates, and government grants for conformity costs.
- The strategy balances investor-friendly incentives and a rapid start-up environment with robust legal and fundamental rights protections for AI systems developed or deployed in Malta.
- As a policy instrument, the plan coordinates industrial policy, capacity building, and the MDIA's regulatory support to ensure Malta's AI ecosystem remains both innovative and compliant.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Guidelines on NIS2 implementation

Following the transposition of the NIS2 Directive, it is expected that the National Cybersecurity Coordination and the competent authorities may publish detailed guidelines and recommendations on compliance procedures, incident reporting, and registration requirements for essential and important entities during 2026.

Adoption of the CVD framework

Malta is expected to adopt a legal framework for CVD to guide how security researchers report vulnerabilities and how organizations should respond. Once implemented, it is assumed that this should support alignment with NIS2 obligations on vulnerably handling.

Implementation of the EU AI Act

In 2026, the MDIA and the IDPC are expected to fully operationalize their roles as the national authorities under the EU AI Act. They will supervise compliance, oversee high-risk AI systems, and coordinate market surveillance in Malta.

- MDIA will act as Notifying Authority and primary Market Surveillance Authority overseeing conformity assessment bodies and monitoring high-risk AI systems. It is also expected the MDIA will establish an AI regulatory sandbox to allow supervised testing of high-risk or innovative AI systems before full market development.
- IDPC will supervise certain high-risk AI systems, including those used in law enforcement, border control, and administration of justice.
- The expectation is that the Act will come into full effect on 2 August 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Mexico

Contacts

Mauricio Oropeza

Partner, Deloitte Legal Mexico

moropeza@deloittemx.com

Melissa Franco

Manager, Deloitte Legal Mexico

melfranco@deloittemx.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Enactment of the new Federal Law on the Protection of Personal Data Held by Private Parties

As of 21 March 2025, several data privacy laws were enacted, marking a substantial change in the data protection regulation in Mexico. All the major laws on the matter were derogated and enacted looking to homologate the data protection regulation in views of the extinction of the autonomous constitutional body that acted as guarantor in matters of data protection and transparency (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)) at a federal and local level.

General Law on Transparency and Access to Public Information

One of the laws enacted is the General Law on Transparency and Access to Public Information (LGTAIP), which is fundamentally focused on regulating the governmental entities and private entities that use or receives public resources or exercises any kind of act of authority.

As a major key point, he LGTAIP contains the body that will substitute the INAI at a federal level as guarantor of data protection and transparency, being the "People's Transparency" (Transparencia para el Pueblo), and decentralized administrative body of the Ministry for Anti-Corruption and Good Governance, stating, at a local level, that the guarantor will be the body of the local executive power incorporated according the local law of each state.

Another of the key points of this new law is that the LGTAIP all information generated, obtained, acquired, transformed, or held by obligated entities is deemed as public and must be accessible to any person, under the terms and conditions established in the law, in the international treaties to which the Mexican State is a party, the laws of the federal entities, and in the applicable legal provisions within their respective jurisdictions. Having the obligated entities the duty to habilitate the applicable means and take the actions required for such purposes.

This law also states that the public information can be deemed as reserved temporarily only by reasons of public interest or national security, but the information related to serious violations of human rights or crimes against humanity can not be classified as reserved.

For the public information marked as reserved or confidential, it can only hold this status for a maximum of five years from the date of classification, which can be extended for an additional five-year term if duly justified by a damage test.

In addition, public information can be deemed as reserved only if its publication:

- Compromises national security, public safety, national defense, or social peace;
- May undermine the conduct of international negotiations and relations;
- It's provided to the Mexican government under a confidential basis by an international body or subject; or
- Puts the life, integrity or health of an individual at risk, among other cases.

Under this, the LGTAIP also provides that no individual can be subject to judicial or administrative inquiry arising from the exercise of the right of access to information, nor may this right be restricted by any means, direct or indirect.

Federal Law on the Protection of Personal Data Held by Private Parties

Another of the data protection laws that was enacted as a result of this major amendment, is the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP).

Such law regulates all private party that holds any kind of personal data.

One of the major key points to this new law, is that, as the case of the LGTAIP, the new guarantor body is the People's Transparency or analogous body from each state.

In addition, now the law contains several updated definitions such as of "data processor," "database," or "consent," among others.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Regarding the consent, the LFPDPPP kept the possibility of tacit or express consent; stating that, by general rule, tacit consent will be valid unless the law or applicable regulation require express consent. However, for the processing of financial information express consent is mandatory, as well as in the case of sensitive data, which, must be, in addition, collected in writing, either by wet-ink or electronic signature.

Another relevant amendment is that the processing now also covers the automated processes as well as any manual processing of personal data, related to the obtaining, use, recording, organization, preservation, processing, utilization, communication, dissemination, storage, possession, access, handling, exploitation, disclosure, transfer, or disposal of personal data.

From the procedural standpoint, the LFPDPPP, states the following key points into its transitory section:

- That, all procedures filed and pending to resolve before the INAI in matters of information access, due to its extinction will be resolved and discussed by the People's Transparency. The same apply to any new request or procedure.
- In any other matters pending to be resolved by the INAI, the procedure will be followed according to the regulation and disposition published by the Ministry for Anti-Corruption and Good Governance.
- The digital platforms, databases and records previously owned by the INAI, will be transferred to the Ministry for Anti-Corruption and Good Governance in a 15-day term after the entry into force of the decree.
- The organic regulation on the People's Transparency must be issued within a 90-day calendar days after the entry into force of the decree (published on 21 March 2025).
- The federal courts must establish district courts and circuit courts specializing in matters of access to public information and protection of personal data in a 120-calendar day term after the entry in force of the decree to resolve amparo proceedings in such matters that are pending to resolve (habilitated on 20 June 2025).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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, a 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.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Project of a Law on Ethical Regulation of Artificial Intelligence and Robotics

As in cybersecurity 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 AI 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 (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).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

AI and cybersecurity regulation

Project of a Law on Ethical Regulation of Artificial Intelligence and Robotics

It is expected that the review process of this project will resume in 2026 for discussion and approval in mid-2026.

Project of a Federal Cybersecurity Law

It is expected that the review process of this project is resumed in this period of legislative bodies.

Amendment to the data protection guarantor bodies

Due to the comprehensive amendment to the data protection and information access laws and regulations, there are still several secondary regulations pending to be issued. This is expected to happen in the rest of 2025 and mid 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Morocco

Contacts

Grégoire Chaste

Partner, Deloitte Conseil Morocco

gchaste@deloitte.com

Amal Barhon

Manager, Deloitte Conseil Morocco

abarhon@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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.

The authority responsible for personal data protection has highlighted a number of concepts relating to privacy, notably through press releases.

- **CCTV and data privacy:** The National Commission for the Protection of Personal Data Protection (CNDP) emphasizes the issue that the use of video surveillance, particularly with sensitive technologies such as facial recognition, must be governed by robust legal and technical safeguards in order to protect privacy and personal data, while reconciling the public interest and respect for constitutional values. This is why the CNDP is holding hearings to draw up a deliberation clarifying these provisions and ensuring a common interpretation of Law No. 09-08 by all stakeholders.
- **Artificial intelligence and data privacy**: Artificial intelligence processing that uses personal data must comply with Law No. 09-08, ensuring transparency, fairness, and protection of citizens' rights. To this end, the CNDP is launching a deliberation process based on hearings with experts, institutions, and civil society.

Although no major developments have been established, it is important to highlight certain actions undertaken by the CNDP:

- **January 2025: National Data Protection Week:** From 27-31 January 2025, the CNDP organized a week dedicated to the protection of personal data, in commemoration of Data Privacy Day. This event included conferences and workshops on topics such as the protection of digital identity, genomic and neurological data, as well as discussions on the risks associated with deepfakes and the internet of things.
- **May 2025: Acceleration of compliance controls:** The CNDP has intensified its control efforts to ensure compliance with laws related to the protection of personal data. This approach is part of a desire to strengthen data governance and respond to the challenges posed by the rapid digitalization of the country. For example, nearly 3,000 pharmacists have already begun the steps to ensure compliance. It is worth noting that the CNDP allows employees and citizens in general to file complaints in case of violations of their personal data, via its website, by fax, or by phone. The commission then sends a warning to the data controller to regularize their legal situation.
- **July 2025: Strengthening of legislation:** Moroccan legislation on the protection of personal data, particularly Law No. 09-08, has been strengthened to better meet the challenges of the digital age. This strengthening is part of a dynamic aimed at harmonizing the Moroccan legal framework with international standards, such as the European General Data Protection Regulation (GDPR).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Publication in the Official Bulletin of the Order of the Head of Government No. 3-17-25 of 7 Safar 1447 (1 August 2025) Setting the Reference Framework for the Qualification Requirements of Cloud Service Providers

- This framework establishes the organizational, technical, legal, and governance criteria that providers must meet in order to obtain the qualification granted by the national authority. It serves as the normative basis used by the General Directorate of Information Systems Security (DGSSI) or any designated evaluation body to conduct the required assessments.
- The framework, aligned with international standards, regulates the security of cloud services by covering security governance, access and data management, physical and operational protection, business continuity, incident management, legal compliance, and third-party relationships.
- The framework requires the conclusion of service agreements to define the responsibilities between the provider, the client, and third parties (legal compliance, termination, reversibility, data deletion). It also describes the qualification process: submission of the file, evaluation of capabilities and guarantees, followed by the final decision.

Publication of joint order No. 1148.25 approving the agreement establishing the Cybersecurity Innovation Center

- The Cybersecurity Innovation Center (CIC) serves as a strategic lever designed to unite the efforts of public, academic, and private stakeholders around a common goal – the development of advanced national expertise in cybersecurity, both academically and technically.
- The CIC will carry out, for the benefit of its members, a multidimensional mission, including notably: advanced training in cybersecurity professions, fundamental and applied research on emerging threats, technological development and innovation, and shared management of specialized equipment.

The development of the National Cybersecurity Strategy for the horizon 2030 by the DGSSI

The new national cybersecurity strategy, developed in consultation with the stakeholders involved, is built around four main pillars as follows:

- **National cybersecurity governance - institutional and legal framework:** Maintain and strengthen the legal and nominative framework, and improve national coordination mechanisms;
- **Security and resilience of the national cyberspace:** Support decision-making and support data-driven policies, strengthen national capabilities for prevention, management, and response to cyber incidents and crises, promote the protection of information systems of vital infrastructures, and promote the implementation of cybersecurity standards and norms;
- **Development of capacities and awareness:** Develop a culture of cybersecurity within the company, strengthen the capacities of human resources in cybersecurity, support the development of the national cybersecurity ecosystem and encourage innovation; and
- **Regional and international cooperation:** Strengthening and promoting active participation at the regional and international level on cybersecurity issues, and the development of bilateral cooperation.

The ultimate goal of the national strategy is to create the conditions for a trustworthy digital environment, capable of supporting and accompanying the digital transformation of the kingdom, one of the levers for economic and social development in Morocco.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Absence of AI legal framework in Morocco

Currently, Morocco has no specific legal framework governing 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.

The AI updates introduced in 2025

Signing of an agreement for a national responsible AI platform in Morocco

On 11 September 2025, in Rabat, the Ministry of Digital Transition and the CNDP signed an agreement to develop a national platform for responsible artificial intelligence, tailored to Moroccan specificities (language, culture, digital identity). Based on a large language model (LLM), it will aim to provide citizens, businesses, and administrations with secure, efficient, and fundamental rights-respecting generative and conversational AI tools.

- **Creation of the Morocco Digital for Sustainable Development Hub: An Arab-African Hub for AI and digital innovation:** On 8 April 2025, in Rabat, Morocco and the United Nations Development Programme (UNDP) signed a declaration of intent to create the Morocco Digital for Sustainable Development Hub, a regional digital hub dedicated to AI, data science, and innovation
- **Framework bill on AI in Morocco: Towards ethical and responsible governance:** The draft framework law in preparation lays the foundations for robust governance: legal responsibility in case of slippage, transparency of algorithms, mandatory technical audits, and compliance with international standards (OECD, UNESCO, EU). A specialized direction in AI and emerging technologies has already been established within the Ministry of Digital Transition. It will guide public policies regarding data, AI, and innovation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

- **Strengthening of the application and interpretation of Law No. 09-08 (2009 framework)**: The CNDP is increasing the number of consultations and hearings (e.g., rules governing video surveillance, use of facial recognition) to clarify and update the application of the law in light of new digital uses.
- **Rising influence of the CNDP**: Stricter controls, sectoral frameworks, and compliance deadlines (reported for 2024-2025), with more active public communication.
- **Gradual alignment with international standards**: As part of the national digital strategy (Digital Morocco 2030) and to promote exchanges/cooperation, harmonization efforts are expected (individual rights, data protection impact assessments, transfer security).

Cybersecurity

- **Implementation and ramp-up of the National Cybersecurity Strategy (public documents and roadmaps via the DGSSI):** Strengthening incident detection/management capabilities, securing public information systems, and certifying sensitive systems.
- **Operational structuring (CERTs, labeling/certification, security by design):** Strengthening security requirements for critical service providers and standardization/certification initiatives.
- **Convergence of security and privacy:** Cybersecurity and data protection issues are addressed in a cross-cutting manner (e.g., incident reporting obligations, securing personal data).

AI

Morocco on the verge of a technological revolution: AI 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 AI 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.

Parliamentary work and draft texts under discussion aimed at defining responsibilities, transparency, risk governance, and sanctions for dangerous uses of artificial intelligence are underway.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Nigeria

Contacts

Asiata Agboluaje

Partner, Deloitte Legal Nigeria

aagboluaje@deloitte.com.ng

Inepaimi Ayah

Manager, Deloitte Legal Nigeria

iayah@deloitte.com.ng

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

General Application and Implementation Directive on data protection

The General Application and Implementation Directive (GAID) was issued by the Nigeria Data Protection Commission (NDPC) on 12 March 2025 and took effect on 19 September 2025. GAID, which replaces the Nigeria Data Protection Regulations 2019 (NDPR), was established to enhance clarity as it relates to legal obligations, especially in situations where the rights and freedoms of individuals could be jeopardized without such assurances. Additionally, the Directive aims to strengthen Nigeria's legal framework for data protection and privacy rights.

GAID provides guidance particularly as it concerns processing of personal information. It prescribes robust compliance measures to be undertaken by data controllers and data processors in line with the Nigeria Data Protection Act 2023 (NDPA). It covers matters such as the processing of data by individuals for household or personal purposes, designation of data controllers and data processors of major importance, filing of NDPA compliance audit returns with the NDPC, designation of a data protection officer, and principles of personal data protection etc.

It also provides for the lawful bases of data protection, data processing which requires consent, and data privacy impact assessment, etc.

Whilst GAID replaces the NDPR, Article 3 stipulates that this replacement does not affect anything done under the NDPR prior to the issuance of GAID. Also, in the event of a conflict between the provisions of GAID and the NDPA, the provisions of the NDPA shall prevail.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Nigerian Atlas for Languages and AI at Scale (N-ATLAS) 2025

On 20 September 2025, the Nigerian Atlas for Languages and AI at Scale (N-ATLAS) was officially launched on the sidelines of the 80th United Nations General Assembly (UNGA80) in New York. It was developed by the Federal Ministry of Communications, Innovation, and Digital Economy and powered by Awarri, in partnership with the National Information Technology Development Agency (NITDA) and the National for Artificial Intelligence and Robotics (NCAIR). It is also supported by the Bill and Melinda Gates Foundation.

As a pioneering open-source multilingual large language model, N-ATLAS is a transformative initiative aimed at preserving and promoting Nigeria's rich linguistic heritage. With over 500 languages spoken across Nigeria, N-ATLAS is designed to understand and generate content in Nigeria's diverse languages, including the three major languages (Yoruba, Hausa, and Igbo) and Nigerian-accented English.

N-ATLAS is a multilingual and multimodal AI system equipped with a comprehensive speech-technology suite, including language-specific automatic speech recognition (ASR) models. These capabilities enable a wide range of applications, from transcribing radio, television, and online content into text with captions, to powering chatbots that provide government services in local languages and supporting call centers and voice assistants with accurate transcription and response generation.

This initiative marks a significant step in ensuring that Nigeria's linguistic and cultural diversity is not only preserved but also integrated into the global AI ecosystem. By creating open-source datasets and tools, N-ATLAS paves the way for innovation in education, healthcare, commerce, and governance, ensuring that no voice is left behind in the digital age.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

Increased enforcement activity

A significant increase in enforcement activities by the Nigeria Data Protection Commission is anticipated, with stricter regulatory scrutiny and the enforcement of sanctions and penalties for noncompliance with the Nigeria Data Protection Act (NDPA). This trend was evident over the past year, as the Nigeria Data Protection Commission (NDPC) intensified efforts to ensure data protection awareness and regulatory compliance across sectors.

Cybersecurity

Cyber risk guidelines

The National Insurance Commission (NAICOM) is developing cyber risk guidelines aimed at strengthening the insurance industry's resilience against emerging digital threats. This initiative was highlighted during the Insurers' Committee Meeting held in Lagos, where NAICOM reiterated its call for insurance companies to develop and roll out cyber insurance products in response to the growing risks of digital transformation.

Recognizing the insurance industry's unique role in mitigating cyber risks, NAICOM is working closely with key stakeholders, including the National Information Technology Development Agency (NITDA) and the Nigeria Data Protection Commission, to advance this effort. The forthcoming guidelines are expected to support innovation, enhance claims transparency, and unlock new growth opportunities in cyber insurance.

AI

Ongoing legislative efforts

There are several bills under consideration by the National Assembly that reflect Nigeria's commitment to responsible AI development and digital transformation. Some of these bills are:

- **National Digital Economy and E-Governance Bill:** This bill seeks to revolutionize Nigeria's digital landscape by creating a comprehensive framework for digital governance. It provides legal recognition for electronic transactions, mandates ethical AI deployment, and promotes digital literacy and skills development; and
- **National AI and Robotics Sciences Bill:** This bill proposes the establishment of a dedicated regulatory commission to oversee AI and robotics development in Nigeria.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Norway

Contacts

Bjørn Ofstad

Partner, Deloitte Legal Norway

bofstad@deloitte.no

Hanne Pernille Gulbrandsen

Partner, Deloitte Legal Norway

hgulbrandsen@deloitte.no

Eirin Helen Hauvik

Partner, Deloitte Legal Norway

ehauvik@deloitte.no

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Fine issued to Telenor ASA

On 10 March 2025, the Norwegian Data Protection Authority (Datatilsynet) issued a fine of NOK 4 million to the Norwegian company Telenor ASA for data protection breaches

Telenor ASA **had not carried out all necessary assessments and documentation of the role of the data protection officer**, including the data protection officer's independence and possible conflict of interest. Nor had a direct reporting line for the data protection officer to the highest management level been established and documented. The company also had inadequate internal controls.

The Norwegian Data Protection Authority imposed the fine for the lack of appropriate organizational measures and guidelines for the data protection officer scheme. It was considered a mitigating factor that no specific damage to the data subjects' privacy was identified. The long processing time when assessing the size of the fee was also considered.

Fine issued to Grue Municipality

The Norwegian Data Protection Authority imposed an administrative fine of NOK 250,000 to Grue Municipality for **violation of the municipality's obligation to ensure adequate security in accordance with the GDPR and of the requirements for a legal basis under the GDPR.**

New rules on cookies and similar technologies

Consent requirements for the use of cookies and similar technologies were tightened on 1 January 2025

Consent requirements for the use of cookies and similar technologies were tightened on January 1, 2025. The Norwegian Parliament passed a new e-communications act that came into force on 1 January 2025. The act states that the use of cookies and similar technologies requires consent that is valid under the General Data Protection Regulation (GDPR) in order to be legal. The Norwegian Data Protection Authority and the Norwegian Communications Authority (Nkom) will have joint supervisory authority with the provision. The amendment means that Norwegian law is in line with EU law when it comes to cookies and similar technologies, and that Norwegian internet users in Norway will receive stronger protection against online tracking.

Guideline from the Norwegian Data Protection Authority on cookies and similar technologies

In connection with the new rules, a new guideline was presented in April 2025

The guidance provides businesses with concrete advice and examples on how to design their consent solutions to be compliant with the GDPR. The aim is to make it easier to comply with the new rules in the Electronic Communications Act that came into force on 1 January 2025.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The appeal from the Norwegian Labor and Welfare Administration (Nav) was processed by the Privacy Appeal Board December 2024

The Norwegian Data Protection Board has processed the complaint from Nav regarding the Norwegian Data Protection Authority's decision regarding an order for violation of the GDPR and the imposition of a violation fine

On 18 March 2024, the Norwegian Data Protection Authority issued a fine of NOK 20 million to Nav. The decision followed a supervisory inspection where we reviewed Nav's safeguards for confidentiality through access control and log monitoring. Nav appealed the fine to the Privacy Appeal Board.

The Privacy Appeal Board stated that the ambiguity in the data protection authority's application of the law, the authority's explanation of the facts, and the authority's inadequate assessment of the claim of fault represent such shortcomings in the decision that the board concluded that the decision on the violation fee must be overturned.

On 10 January 2025, the Norwegian Data Protection Authority stated that if, after a thorough assessment, conclude that the case should be reexamined. In the further consideration of the case, the assessments and justifications from the data protection board shall be taken into account. On this background, this case is not closed.

Ruling by Sogn og Fjordane District Court – 25-017890TVI-TSOF/TSOG

On 18 July 2025, Sogn og Fjordane District Court ruled in case regarding the legality of the termination of a termination agreement in employment, as well as claims for reinstatement of the employment relationship, redress and compensation due to breach of the GDPR

The plaintiff claimed compensatory damages for breach of data protection regulations. The plaintiff alleged that the defendant (the municipality) processed personal data in violation of the GDPR, including by sharing sensitive personal data without a legal basis (GDPR Article 6) and without fulfilling the information obligation. (GDPR Articles 12-14). The background was eight different scenarios where the plaintiff claimed that the GDPR was violated. The scenarios concerned both verbal and written sharing of personal data, including sensitive information, with external and internal parties.

The court assessed the question of whether these eight scenarios was a violation of the GDPR and concluded that the processing of the personal data represented a serious breach of data protection regulations; there was no valid basis for processing (GDPR Article 6), and the conditions for processing special categories of personal data were not met.

In terms of damage, the court assumes that the data subject (the plaintiff) has suffered nonmaterial damage as a result of the plaintiff's processing. It was documented that the data subject had experienced significant loss of reputation in the local community and the public sector, that he has lost control over his own personal data, and that he had been expose to extensive psychological stress. Overall, the court concluded that compensatory damages equivalent to NOK 175,000 were appropriate.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Digitalsikkerhetsloven – The Digital Security Act (Directive (EU) 2022/2555 (NIS) implementation)

Norway adopted the Digital Security Act (Digitalsikkerhetsloven) on 20 December 2023 – the act will enter into force on 1 October 2025, along with the Digital Security Regulation. These implement the EU's NIS Directive and apply to providers of essential services and major digital-service providers.

When the Digital Security Act comes into force, it will apply to a wide range of organizations. Covered entities include operators of essential services in sectors such as energy, transport, health, water supply, banking and financial market infrastructure and digital infrastructure, as well as certain digital service providers. It will also impact companies that form part of their supply chains, such as data-center operators and other vendors, even if they are not directly subject to the act.

Norway has not yet incorporated the successor NIS2 Directive. The Norwegian government has however repeatedly emphasized its plan to **implement both NIS2 and the Critical Entities Resilience Directive** (CER) as quickly as possible, which is stressed in the white paper "Total Preparedness" (Meld. St. 9 (2024-2025)). This will bring Norwegian legislation in line with European standards.

DORA-loven - Digital Operational Resilience Act for the financial sector (Regulation (EU) 2022/2554 implementation)

Norway's DORA-loven (Digital Operational Resilience Act for the financial sector) is the national implementation of EU Regulation (EU) 2022/2554. It was presented to the Stortinget on 7 March 2025 and approved in May; the law and its implementing regulation entered into force on 1 July 2025

DORA will be enforced in Norway by the Financial Supervisory Authority (Finanstilsynet), It covers most financial entities their key IT providers. Covered entities need to update ICT risk frameworks, continuity and recovery plans, and vendor contracts, making sure they include audit and exit rights. They must also map third-party providers, appoint someone responsible for DORA compliance, and be ready to report serious ICT incidents to Finanstilsynet. Incident reporting must follow Finanstilsynet's template, with serious incidents notified within four hours of classification.

The Cryptoassets ACT – Norway's EU MiCA implementation (Regulation (EU) 2023/1114)

Norway incorporated the EU MiCA regulation through a new Cryptoassets Act, entering into force on 1 July 2025

Operating crypto-asset services in Norway will require a license from the Financial Supervisory Authority, and breaches of the rules can lead to fines of up to NOK 60 million. The MiCA license application must include documentation such as organizational descriptions, procedures, and formal governance documents.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Proposal for a Norwegian AI Act (implementation of the EU AI Act)

The Norwegian Ministry of Digitalization and Public Governance has launched a public consultation on a draft law to implement the EU AI Act into Norwegian law

The proposal largely mirrors the EU regulation, with entry into force planned for summer 2026. It introduces legally binding requirements for developers, importers, distributors, and users of AI systems, based on risk categories. The deadline for comments in the public consultation was 30 September 2025.

NKOM (the Norwegian Communications Authority) was designated by the Norwegian government to act as the supervisory authority for the forthcoming AI Act in Norway.

Establishment of "KI Norge" (AI Norway)

"KI Norge" has been launched as part of the national governance structure for AI, tasked with fostering safe and responsible AI use while supporting innovation

KI Norge will be set up as a new and expanded center of expertise within the Norwegian Digitalization Agency (Digdir) and will serve as a driving force and advisor, as well as act as a link and partner between key AI stakeholders in the public sector, industry, the research community and academia.

AI research centers

The government has decided to establish six national research centers for AI

The centers will conduct research on how AI affects society, develop the technology, and strengthen innovation and value creation in both the business sector and the public sector.

Development of a Norwegian LLM

The National Library of Norway is actively involved in developing a Norwegian large language model based on the library's extensive datasets

This initiative is part of a broader effort to create LLMs tailored to Norwegian society, ensuring control over data and alignment with local values.

The government is heavily involved in the project, providing funding, legal guidance and strategic oversight. Key collaborations involve NTNU, the University of Oslo and different private partners like NorwAI, creating a framework for research and development.

Supreme Court updates lawyer's guidelines for use of AI

The Supreme Court of Norway received a pleading containing so-called hallucinations, leading to updates in lawyer's guide with a new section on the use of AI tools

The new section states, among other things, that "it is known that AI can hallucinate and invent, among other things, legal sources. Sources and other information provided by AI must be quality assured. AI should only be used in areas where the lawyer has sufficient expertise to check the content" (translated from Norwegian).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Draft of a new act on Digital Services

The Ministry of Digitalization and Public Administration has recently sent a draft of a new Norwegian act on Digital Services for consultation

The Ministry of Digitalization and Public Administration has recently sent a draft of a new Norwegian act on Digital Services for consultation. The act will implement the EU regulation Digital Services Act (DSA) into Norwegian law. The purpose of the Norwegian act is, among other things, to protect fundamental rights on the internet, including strengthening privacy. The Norwegian Data Protection Authority has been designated as one of the several authorities that will supervise the act.

The government has announced that the Norwegian Communications Authority (Nkom) will be the main supervisory authority for the DSA in Norway. The Norwegian Media Authority (Medietilsynet), the Norwegian Consumer Authority (Forbrukertilsynet), and the Norwegian Data Protection Authority (Datatilsynet) will also have responsibilities within their respective areas.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Peru

Contacts

José Francisco Iturrizaga

Partner, Deloitte Legal Peru

jiturrizaga@deloitte.com

Mariana Cordero

Senior Associate, Deloitte Legal Peru

marcordero@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Regulation of the Law No. 29733 on the Personal Data Protection Law was published

Supreme Decree No. 016-2024-JUS

On 30 November 2024, the new regulation for Law No. 29733, the Personal Data Protection Law, was published. This regulation replaces the previous framework and introduces significant updates designed to align Peru's data protection regime with international standards and address emerging technological challenges. The regulation will enter into force 120 days after publication (29 March 2025), with certain obligations subject to progressive implementation depending on the size, complexity, and nature of the organization.

This update represents a major step forward in modernizing Peru's approach to data privacy in the digital era. It not only establishes new obligations for data controllers and processors but also incorporates best practices from global frameworks and ISO standards related to information security. The regulation emphasizes accountability, transparency, and proactive compliance, ensuring that organizations adopt robust measures to protect personal data.

Key highlights of the regulation

- **Mandatory data protection officer (DPO):** Organizations that process large volumes of personal or sensitive data must appoint a DPO by 2028. This role will be responsible for overseeing compliance, advising on data protection obligations, and serving as a point of contact with the supervisory authority.
- **Expanded territorial scope:** The regulation now applies to foreign companies that offer goods or services to individuals in Peru or monitor their behavior online. This extraterritorial reach ensures that Peruvian citizens' data is protected regardless of where the processing occurs.
- **Enhanced security measures:** Organizations are required to implement security controls aligned with ISO/IEC 27001 standards, reinforcing the importance of risk management and continuous monitoring to prevent data breaches.
- **New data subject rights:** Individuals gain stronger rights, including data portability and greater transparency in automated decision-making processes. These rights empower citizens to have more control over their personal information and how it is used.
- **Breach notification requirements:** In the event of a data breach, organizations must notify the National Authority for Personal Data Protection and affected individuals within 48 hours of detection. This rapid reporting obligation aims to minimize harm and ensure timely corrective actions.
- **Penalties for noncompliance:** The regulation introduces stricter sanctions, with fines of up to 100 UIT (approximately S/535,000) and potential criminal liability for severe violations. These measures underscore the government's commitment to enforcing compliance and deterring negligent practices.

The regulation aims to strengthen privacy protection, ensure responsible data processing, and provide greater transparency and accountability, while enhancing Peru's capacity to respond to digital risks and align with global best practices.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Unified Virtual Form for reporting information security incidents was presented to simplify compliance with the legal obligation to report such incidents to the National Center of Digital Security

This initiative ensures compliance with reporting obligations established in Emergency Decree No. 007-2020, which approves the Digital Trust Framework, and the Regulation of Law No. 29733, Personal Data Protection Law, approved by Supreme Decree No. 016-2024-JUS.

The form allows for the registration of relevant and detailed information about incidents: affected systems, types of compromised personal data, number of impacted individuals, date and time of occurrence and detection, description of events, measures adopted, among other aspects. This enables case tracking, corrective actions, and the generation of statistics to identify patterns in information security incidents, contributing to prevention.

In this context, all public entities and digital service providers are required to report incidents that compromise the confidentiality, integrity, or availability of their systems or data.

The form serves as the official and unified channel to fulfill this obligation, ensuring efficiency, transparency, and strengthening the state's response capacity against growing digital risks.

The tool is available at: https://reporte.cnsd.gob.pe/home/minjus.

MINJUSDH invites citizens to participate in the review of the new methodology for calculating fines related to personal data protection

The Ministry of Justice and Human Rights (MINJUSDH) has published the draft "Methodology for Calculating Fines in Personal Data Protection Matters" on its website. This document will define how fines will be imposed on companies or entities that misuse personal data in their possession, in violation of the Personal Data Protection Law and its regulations.

The new proposal considers recent changes in personal data protection regulations, such as the inclusion of new infractions and liability factors. Therefore, it is necessary to update the methodology that will serve as a guide to apply sanctions more fairly and clearly.

Through this initiative, MINJUSDH, via the National Authority for Personal Data Protection, reaffirms its commitment to ensuring that sanctioning procedures are carried out in accordance with the principles established in the regulations, promoting greater transparency for those subject to the law and adequately protecting the rights involved.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Proposal for Peru's National Cybersecurity Strategy 2026-2028 – August 2025

This strategic instrument defines the framework for action by the Peruvian State to ensure a secure, resilient, and reliable cyberspace. It seeks to protect critical infrastructures and digital information assets, as well as safeguard citizens' rights against cyberthreats and cyberattacks.

Main objectives

- Protect critical infrastructures and digital information assets;
- Safeguard citizens' rights against cyberthreats and cyberattacks;
- Strengthen Peru's digital resilience and response capacity; and
- Align with international standards such as the ITU Global Cybersecurity Index, OECD Digital Security Framework, and UN Sustainable Development Goals.

This strategy applies to public sector entities at all levels (national, regional, and local) and encourages participation from the private sector, academia, and civil society. It is designed to be holistic, covering governance, risk management, education, and international cooperation.

Key challenges

- Need for normative alignment with existing Peruvian laws, such as Emergency Decree No. 007-2020 on cybersecurity and Law No. 30999 on cyber defense;
- Coordination between civil cybersecurity and military cyber defense; and
- Addressing emerging risks from AI and quantum computing.

Core pillars

- Governance and leadership;
- Protection of critical infrastructures and digital assets;
- Regulation and compliance;
- Risk management, resilience, and incident response;
- Combating cybercrime;
- Strengthening cyber defense;
- Research, innovation, and cybersecurity culture; and
- International cooperation.

Together, these measures form a comprehensive approach to strengthening Peru's cybersecurity posture. By implementing this strategy, the country aims to protect critical infrastructures, secure digital assets, and uphold citizens' rights, ensuring a resilient and trustworthy digital environment for sustainable development.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cyberattacks in Peru exceed 748 million in six months – 3 September 2025

According to the latest report from FortiGuard Labs, Peru experienced more than 748 million cyberattacks in the first half of 2025, marking an unprecedented surge in malicious activity. The report highlights that scanning techniques and intrusion attempts have grown at an alarming rate, driven by increasingly sophisticated cybercriminal strategies.

This sharp increase underscores the urgent need for:

- Enhanced cybersecurity measures across public and private sectors;
- Investment in advanced technologies to detect and prevent attacks; and
- Training and awareness programs to strengthen digital resilience.

Experts warn that the rise in attacks is linked to global trends, where cybercriminals exploit vulnerabilities in critical systems and leverage automation to accelerate intrusion attempts. Peru's position as a growing digital economy makes it a prime target, emphasizing the importance of a national cybersecurity strategy to protect data, infrastructure, and citizens.

International Cyberattack Simulation 2025

The Presidency of the Council of Ministers (PCM), through the Secretariat of Government and Digital Transformation (SGTD) and the National Center for Digital Security (CNSD), organized the International Cyberattack Simulation (SIMAC) 2025 as part of Peru's commitment to strengthening digital security and resilience.

The event aimed to measure and enhance the response capacity of public and private institutions against potential cyberattacks. It provided a controlled environment where participating organizations faced simulated attack scenarios and tested their Incident Response Teams (CSIRT).

Key objectives:

- Evaluate institutional readiness for cyberthreats;
- Test protocols for prevention, detection, and recovery;
- Identify vulnerabilities and improve security strategies; and
- Promote collaboration between government, private sector, and international experts.

This initiative supports the National Digital Transformation Policy, specifically its fifth priority: ensuring digital security and trust. The lessons learned will feed into a technical report with tailored recommendations for each entity, reinforcing Peru's digital sovereignty and resilience.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Regulation of the Law that promotes the use of AI in Peru was published

Supreme Decree No. 115-2025-PCM, on 9 September 2025 (the Regulation)

The publication of this regulation marks a historic milestone, making Peru the first country in Latin America to adopt a comprehensive regulatory framework for AI. This legal instrument seeks to balance two critical objectives: fostering innovation and technological development while ensuring robust safeguards for fundamental rights and ethical principles in the use of AI systems.

The Regulation establishes clear guidelines for the responsible development, deployment, and use of AI technologies across both public and private sectors. It aims to create an environment that encourages innovation while minimizing risks associated with algorithmic bias, privacy violations, and misuse of AI in sensitive contexts. By doing so, Peru positions itself as a regional leader in digital governance and aligns with global best practices.

The Regulation reinforces principles consistent with international standards, including:

- Nondiscrimination and prevention of algorithmic bias to ensure fairness in automated decision-making;
- Privacy and personal data protection, in line with Peru's data protection laws;
- Mandatory human oversight in critical decision-making processes, preventing fully autonomous decisions in high-impact areas; and
- Accountability and responsibility, requiring organizations to demonstrate compliance and maintain transparency in AI operations.

Inspired by the European Union's AI Act, the Regulation introduces a risk-based approach to AI governance, categorizing systems into three levels:

- Misuse (prohibited): Activities such as deceptive manipulation of decisions, real-time biometric surveillance in public spaces, predictive policing, autonomous lethal capabilities, and mass surveillance without a legal basis are strictly banned;
- High risk: AI applications in sensitive sectors, including health, education, recruitment and workforce management, credit scoring, social programs, and critical infrastructure (energy, telecommunications, banking, water, and transport), are subject to stringent compliance requirements; and
- Acceptable risk: All other uses fall under this category and must adhere to general principles and best practices for ethical and secure AI deployment.

The Regulation will enter into force 90 working days after publication, in January 2026, and establishes a phased implementation schedule for both public and private entities. This gradual approach allows organizations to adapt their processes, train personnel, and implement necessary technical and organizational measures to comply with the new standards.

By adopting this framework, Peru demonstrates its commitment to responsible AI governance and positions itself as a pioneer in Latin America. The Regulation not only addresses current challenges but also anticipates emerging risks associated with advanced technologies such as Generative AI and quantum computing. It provides legal certainty for businesses, promotes trust among users, and ensures that innovation occurs within a framework that respects human rights and democratic values.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Artificial intelligence in Peru

The Peruvian government is actively promoting the responsible, ethical, and sustainable use of AI as a strategic tool to foster economic growth, social inclusion, and technological innovation. This effort seeks to position Peru as a competitive player in the global digital economy while ensuring that AI adoption aligns with fundamental rights and democratic values.

Key initiatives include:

- Legal framework:
  - Law No. 31814: Establishes the foundation for promoting AI as a driver of national development, encouraging its integration across public and private sectors; and
  - Regulation of Law No. 31814: Defines guiding principles, obligations, and safeguards to ensure safe, transparent, and accountable AI implementation, minimizing risks and protecting citizens' rights.
- International cooperation: Strategic partnerships with leading countries and global organizations to develop joint AI projects, exchange technical expertise, and share best practices for ethical and innovative AI deployment; and
- Global positioning: Peru ranks fifth in Latin America in AI readiness according to Oxford Insights 2024, with a score of 57.11, surpassing the global average. This reflects progress in governance, infrastructure, and talent development.

Focus areas for AI development:

- Ethical principles: Emphasis on nondiscrimination, transparency, and accountability to ensure fairness and trust in AI systems;
- Risk-based approach: Inspired by the EU AI Act, prioritizing proportional regulation based on the level of risk associated with different AI applications; and
- Promotion of research and STEM talent: Investment in education, research programs, and innovation hubs to strengthen local capabilities and attract global collaboration.

Strategic goal

Build an inclusive, sustainable, and innovative digital ecosystem through AI, enabling Peru to harness technology for public welfare, economic competitiveness, and long-term development.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

National Data Governance Strategy for 2026-2030 – August 2025

The Peruvian government has launched the National Data Governance Strategy (ENGD) 2026-2030 to transform data into a strategic asset for public value creation. This initiative seeks to ensure that government data is secure, reliable, and accessible, enabling better decision-making and fostering trust among citizens.

The vision for 2030, Peru aims to become a regional leader in ethical and innovative data use, promoting transparency, collaboration, and digital transformation to support inclusive development.

Why it matters:

- Improves quality and protection of government data;
- Facilitates interoperability and open data for efficient services;
- Encourages innovation and economic growth through data-driven solutions; and
- Strengthens public confidence in government processes.

Strategic pillars:

- Regulatory framework: Updated rules for governance and compliance;
- Data quality and privacy: Reliable, secure, and ethically managed information;
- Open data and interoperability: Accessible data to empower citizens and institutions;
- Infrastructure and platforms: Modern digital tools and secure systems;
- Human talent and data culture: Skilled professionals and awareness programs; and
- Collaborative ecosystem: Partnerships among government, private sector, academia, and civil society.

The goal is to build an inclusive, transparent, and innovative data ecosystem that generates social and economic value, supports public trust, and drives Peru's digital transformation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Poland

Contacts

Monika Skocz

Director, Deloitte Legal Poland

mskocz@deloittece.com

Kamila Mróz

Partner, Deloitte Legal Poland

kmroz@deloittece.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

New guide on personal data protection

In February 2025, the Personal Data Protection Office (UODO) published an updated version of its guide on personal data breaches, the first edition of which was published in 2018. The new version takes into account the latest interpretations of regulations, case law, and practical guidelines. It includes, among other things:

- Updated procedures for responding to breaches (reporting to the President of the UODO);
- Guidelines for cooperation with the President of the UODO and other supervisory authorities;
- Key recommendations for risk assessment and breach prevention.

Key changes in the new UODO guide

- Distinction between a data breach and a GDPR violation:
  - A personal data breach is any incident that leads or may lead to accidental or unauthorized destruction, loss, modification, or access to data. A GDPR breach, on the other hand, refers to a failure to comply with legal obligations under the regulations. Importantly, the mere occurrence of a data breach does not necessarily constitute a breach of personal data protection regulations if the controller has implemented appropriate security measures – unlike a GDPR breach.
- Clarification of the role of the data protection officer (DPO):
  - Indication that the DPO should not perform tasks that fall within the competence of the controller or processor, and that his function is more advisory and guidance-oriented.
- Expanded definition of a breach and risk classification:
  - A data breach now also includes situations that “may lead” to unauthorized access to data, not just those that have already led to it. The guide introduces a three-level risk classification (no risk, risk, high risk).
- The concept of a “trusted recipient”:
  - The concept of a “trusted recipient” has been introduced. A trusted recipient is understood to be an entity that has accidentally received personal data but can be considered trustworthy thanks to its previous cooperation (e.g., business) with the controller.

Supreme Administrative Court ruling confirming that land register numbers are personal data

In its judgment of 28 January 2025, the Supreme Administrative Court (NSA) agreed with the President of the UODO that land register numbers are personal data. This judgment therefore ends the dispute between the UODO and the former General Surveyor of Poland.

The NSA ruling also means that the administrative fine of PLN 100,000 imposed by the President of the UODO on General Surveyor of Poland in 2020 for disclosing land register numbers on the Geoportal2 website is justified.

Disclosure of the land and mortgage register number allows for the identification of the person whose data is contained in the land and mortgage register. By publishing land and mortgage register numbers on websites, any interested internet user can access the information contained therein. The scope of data disclosed in the land and mortgage register of natural persons includes, among others, first names, surnames, parents' names, PESEL number, property address, and mortgage information. Easy access to this data exposes a very large number of people (whose data is concerned) to the risk of identity theft.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Most notable Data Protection Authority decisions in Poland

The President of the UODO imposed fines of PLN 27 million (approx. €6.4 million) on a Polish postal operator and PLN 100,000 (approx. €23.4k) on the Minister of Digital Affairs for organizing the so-called envelope elections

The penalties imposed concerned the processing of data of 30 million citizens without legal basis. So far, this is the highest penalty imposed in Poland.

The case concerns an attempt to organize the Polish presidential election exclusively by mail in the spring of 2020. At that time, Poland was during the COVID-19 pandemic. The authorities began organizing the election process in this form, even though the law amending the election rules had not yet entered into force. This law, which was not in force in April 2020, provided that the Polish postal operator would deliver election packages to voters' mailboxes and that voters would cast their votes by mail so as not to gather in person at polling stations.

On 16 April 2020, the Prime Minister issued an administrative decision requiring preparations to be made for the postal election of the President of Poland. Citing this order, the postal operator requested data from the PESEL database on 30 million Polish citizens who were expected to be of legal age and residing in Poland on the planned election date.

The Minister of Digital Affairs gave his consent, and the data copied onto a DVD was delivered (made available) to the postal operator on 22 April 2020, where it was processed.

The personal data of approximately 30 million Polish citizens was only destroyed between 15-22 May 2020, after it became clear that the elections would not take place.

The President of the UODO emphasized that the unjustified disclosure of personal data from the PESEL register and its processing by the postal operator threatened the proper exercise of citizens' rights under the Constitution and that the violations committed within the entire data protection system were fundamental in nature.

Bank fined PLN 18.4 million (approx. €4.3 million) for violating the GDPR by unlawfully copying customers' identity documents

The penalty applies to scanning ID cards not only of customers, but even of potential customers.

The bank began doing this in 2018 after the Anti-Money Laundering and Terrorist Financing Act came into force. According to Article 34(4) of the GDPR, it allows “the processing of information contained in the identity documents of the customer and the person authorized to act on their behalf, and the making of copies thereof.”

However, according to the President of the UODO, this does not mean that the bank had the right to copy the identity documents of all existing and potential customers. Such action was considered to be excessive and in violation of the principles set out in Article 5 of the GDPR (primarily the lawfulness of processing).

The President of the UODO imposed fines totaling PLN 16,932,657 (approx. €3.9 million) on a fast-food restaurant chain

In the same case, the President of the UODO also imposed penalties on the controller’s PR agency (the processor) in the total amount of PLN 183,858 (approx. €45k).

A fast-food restaurant chain entrusted the processing of its employees' personal data to an external company for the purpose of managing work schedules. The lack of risk analysis of this process, the failure to implement appropriate security measures, and the failure to comply with the provisions of the personal data processing agreement led to the disclosure of personal data in a publicly accessible directory.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Act adapting Polish law to DORA

On 6 August 2025, the Act of 25 June 2025, was announced in the Polish Journal of Laws, introducing changes to certain laws related to ensuring the operational digital resilience of the financial sector (the Act). One of the main objectives of the Act is to ensure the full application of Regulation (EU) 2022/2554 (DORA).

It is important to remember that EU regulations – such as DORA – are directly applicable in EU member states and, as a rule, do not require implementation into national law. However, for DORA to be fully effective, it was necessary to designate a national supervisory authority and implement other essential changes to align national law with the new EU regulation.

According to the Act, the authority responsible for overseeing DORA compliance by financial entities in Poland is the Polish Financial Supervision Authority (KNF). Its tasks include:

- Conducting control proceedings regarding financial entities concerning compliance with the requirements arising from DORA;
- Providing financial entities with information about risks identified in recommendations issued to key external ICT service providers under DORA;
- Receiving reports of significant ICT incidents, and for entities classified as key or important entities, also forwarding such reports to appropriate Computer Security Incident Response Team (CSIRT); and
- Deciding to order specified financial entities to conduct threat-led penetration tests (TLPT).

The Polish legislator decided not to use the so-called national option provided in Article 2(4) of DORA, which allows certain institutions – in Poland credit unions (SKOKs) or Polish development bank (BGK) – to be exempt from DORA's application. The rationale stated that SKOKs' activities are largely similar to those of banks and thus exposed to similar cybersecurity risks.

NIS2 implementation status

Legislative work is underway concerning the implementation of the Directive (EU) 2022/2555 (NIS2) into Polish law. In August and September 2025, subsequent versions of the draft implementation act (Act amending the Act on the national cybersecurity system (the Act)) were published. In October 2025, the Council of Ministers adopted the final draft of the Act, which will be further processed by the Parliament.

The latest changes to the draft Act included:

- Introducing a criterion for verifying the main place of business to determine the scope of obligations under the Act for entities in the digital services sectors;
- Specifying entities responsible for maintaining the register of essential and important entities;
- Expanding the list of entities authorized to exchange information related to cybersecurity, including information on cyberthreats and vulnerabilities;
- The principles for filing complaints against decisions of the cybersecurity authority regarding, among other things, the suspension of granting a concession, limiting its scope, and suspending the activities of essential entity; and
- The principles for designating essential and important entities among units subordinate to the Minister of National Defense.

The catalog of entities in the national cybersecurity system will be expanded to include new sectors of the economy, such as wastewater management, postal services, space, or the production and distribution of chemicals and food. Entities qualified as essential and important entities will be required to implement an information security management system, conduct regular risk analysis, implement appropriate technical and organizational measures to counter threats, and report incidents.

Entities subject to the new regulations will have only 6 months to comply with the new obligations.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The draft law on AI systems

In 2025, the draft Act on AI Systems (the Draft), intended to implement the AI Act within the Polish legal framework, was subject to multiple revisions.

The February version of the Draft introduced a mechanism of regulatory sandboxes designed to foster innovation in the field of AI. These sandboxes enable entities to test AI systems in controlled conditions, with the possibility of temporary derogation from certain legal requirements. The purpose of this mechanism is to facilitate the development and deployment of new AI technologies while ensuring appropriate supervision by the Commission for the Development and Security of AI (Commission).

The August version of the Draft clarified that, when issuing individual opinions, the Commission may seek opinions from other public authorities and organizational units. Amendments were also introduced to procedures concerning serious incidents, extending the list of authorities entitled to receive related information to include, inter alia, the President of the Office of Electronic Communications (UKE), the President of Personal Data Protection Office (UODO), and the Polish Financial Supervision Authority (KNF), as well as specifying the scope of information to be transmitted.

The most recent version of the Draft, dated 2 September 2025 and published on 12 September 2025 on the website of the Government Legislation (Rządowe Centrum Legislacji), maintains the previously adopted framework without introducing substantive amendments. The revisions are predominantly editorial and technical in nature. Although in the area of individual opinions and explanatory statements, it clarifies the obligation to publish them – after anonymization – in the Public Information Bulletin on the Commission's website, together with an indication of their validity status.

It is expected that the Draft will be adopted by the Council of Ministers by the end of November 2025 and subsequently submitted to the Parliament for adoption.

Poland's AI Development Policy 2030

In July 2025, the Ministry of Digital Affairs concluded public consultations on the draft on Poland's AI Development Policy 2030 (AI Policy). The document defines the strategic directions for AI development in Poland and sets out the principles for its safe, responsible, and public interest-oriented implementation.

The new AI Policy envisions that Poland will become one of the leaders of the so-called "AI Continent" by creating a coherent and coordinated ecosystem of trustworthy AI, contributing to economic growth and social well-being.

The main objectives of the AI Policy include:

- Building a strong AI ecosystem;
- Developing a society with advanced competences in the practical use of AI, supported by professional research infrastructure;
- Creating an efficient state administration that makes use of AI-based solutions;
- Strengthening Poland's position as the "Heart of the AI Continent" through extensive implementation across key sectors of the economy; and
- Promoting human-centric, trustworthy AI that enhances quality of life.

Comments submitted during the public consultations primarily concerned the development of regional AI hubs (including in the Górnośląsko-Zagłębiowska Metropolis and Łódź), systemic digital education, and the identification of priority sectors that could strengthen Poland's position as an exporter of safe and trustworthy AI solutions.

The Ministry has announced that the draft will be updated to ensure the final document meets stakeholders' expectations and serves as a realistic roadmap for AI development in Poland through 2030.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Legislative work is underway to adopt an act on fair access to data in response to the entry into force of the Data Act

From 12 September 2025, the provisions of the Data Act (DA) apply directly in all EU member states.

Polish law does not currently provide for solutions that would correspond to all the mechanisms regulated by the DA, so it is necessary to adopt national regulations that will serve to implement the provisions of the regulation.

Key aspects of the new law

- The draft law provides for the appointment of the President of the Office of Electronic Communications as the competent authority responsible for the application and enforcement of the provisions of the DA in Poland.
- The new law is to define national procedures and rules for imposing administrative penalties for breaches of obligations under the DA.
- The regulation creates the organizational and institutional framework necessary for the application of the DA, including the function of data coordinator and certifying authority for dispute resolution bodies.

The project is currently at the government stage.

Work on the implementation of the Artificial Intelligence Systems Act

The draft law aims to introduce the provisions of the AI Act into the national legal system.

Due to the frequent processing of personal data by AI systems, the draft law provides for close cooperation between the Artificial Intelligence Development and Security Commission (to be established under the law) and the President of the UODO.

Emphasis has been placed on the need to consult on projects involving the implementation of high-risk systems. These may lead to the violation of individual rights and freedoms.

This approach is intended to ensure that the use of artificial intelligence complies with the provisions of the GDPR, in particular in the context of automated decision-making and profiling.

The project is currently at the government stage.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Portugal

Contacts

Jacinto Moniz de Bettencourt

Partner, Deloitte Legal Portugal

jbettencourt@deloitte.pt

Joana Diniz Figueiredo

Manager, Deloitte Legal Portugal

joanafigueiredo@deloitte.pt

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

CNPD Annual Activity Report 2024 – End-of-year insights

The latest annual activity report from the Portuguese Data Protection Authority (CNPD) confirms a growing regulatory and cultural maturity in data protection across Portugal. In 2024, the number of prior consultation requests under Article 36 of the GDPR increased by 216.7%, reflecting that Portuguese organizations are increasingly aware of the need to assess in advance the impact of high-risk data processing operations.

The CNPD also recorded 2,879 new cases (+10% compared to 2023), including 332 data breach incidents, mainly caused by human error and phishing attacks. On the enforcement front, the authority imposed 23 fines and issued several warnings, demonstrating a more assertive and preventive regulatory approach.

In parallel, 2025 has been marked by stronger international cooperation, notably through the launch of the Lusophone Data Protection Network (RLPD) and the CNPD's active participation in European and global working groups on Generative AI and privacy.

Celebrating 30 years of activity, the CNPD called for the modernization of its structure and resources, underlining the need for a regulatory model capable of responding to the pace of technological change and the complexity of the digital ecosystem.

In summary, 2024-2025 represent a turning point in Portugal, from a reactive approach to a proactive and preventive culture of compliance in data protection.

CNPD decisions – CCTV systems

The Portuguese Data Protection Authority (CNPD) issued several opinions on video surveillance in public spaces, including the amendment of the CCTV system in Faro (Opinion/2024/17), the installation of systems in Sintra (Opinion/2024/18) and Ponta Delgada (Opinion/2024/40), and the expansion of systems in Porto (Opinion/2024/19) and Coimbra (Opinion/2024/54).

The CNPD reiterated the obligation to apply privacy masking to areas such as windows, balconies, and doors of residential and hotel buildings, in order to safeguard individuals' privacy.

It also clarified that certain features lack legal basis under current law – namely, counting and classification tools, license plate recognition, data analytics systems, and thermal imaging technologies, whose necessity has not been demonstrated.

The CNPD stressed the need to ensure system security, auditability, and alert mechanisms against unauthorized access, tampering, or vandalism, as well as to clearly define the responsibilities of municipalities and subcontractors involved in data processing.

In Porto, the CNPD could not issue a full opinion due to insufficient documentation. It further noted that inspections of authorized systems revealed widespread non-compliance with legal and authorization requirements, particularly in cases where municipalities contracted installation and maintenance services without PSP oversight. The CNPD urged that these irregularities be addressed to ensure lawful and accountable operation of future systems.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Data protection as a democratic limit on state power

Reaffirming constitutional boundaries in the digital state

Opinion No. 63/2025, issued by the Portuguese Data Protection Authority (CNPD), offers an in-depth analysis of the Draft State Budget Law for 2026 (OE2026), highlighting provisions that raise serious concerns regarding personal data protection and fundamental rights.

The CNPD notes that several measures in the draft budget entail large-scale processing of personal data by public entities, including the tax authority, social security, the justice sector, and health services. The opinion focuses particularly on the publication of social security debtor lists, the interconnection of public databases, and the processing of health data, all of which, according to the CNPD, lack a clear and proportionate legal basis.

The CNPD concludes that the proposal fails to comply with the core principles of the GDPR, namely purpose limitation, data minimization, necessity, and proportionality. It further highlights:

- The absence of a mandatory data protection impact assessment (DPIA), required in high-risk processing situations;
- The use of vague and open-ended terminology, such as “relevant data” or “similar registries,” which could allow arbitrary interpretations; and
- The disproportionate nature of publishing debtor lists, considered potentially stigmatizing and incompatible with the right to privacy.

In addition, the CNPD warns that the interconnection of databases between the tax authority, social security, and judicial systems risks creating a state “super-file,” centralizing vast amounts of sensitive information about citizens without adequate safeguards for access, transparency, or accountability.

The opinion strongly reaffirms the institutional independence of the CNPD and the need to limit the state’s data-processing powers. It stresses that the protection of personal data is a fundamental right, enshrined in Article 35 of the Portuguese Constitution, and that no public policy, however legitimate, may erode or override this right. Administrative efficiency and digital transformation, the CNPD argues, must operate within the boundaries of constitutional and European data protection law.

Politically, this opinion stands out for placing the CNPD in direct opposition to the Portuguese government, exposing the tension between state digitalization and the protection of individual privacy. It reinforces the CNPD’s role as an independent supervisory authority, a crucial safeguard in a democratic state governed by the rule of law, ensuring that digital transformation does not turn into a tool for mass surveillance or uncontrolled data collection.

In conclusion, Opinion No. 63/2025 serves as a landmark in the debate on the constitutional and democratic limits of state digitalization. The CNPD underscores that data protection is not an obstacle to administrative modernization, but rather a vital condition for digital freedom, transparency, and democratic citizenship.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Implementation of the DORA regulation

National framework under development and pending approval

Portugal is currently in the process of implementing Regulation (EU) 2022/2554, known as the Digital Operational Resilience Act (DORA), which establishes a harmonized framework for digital resilience in the financial sector. In 2025, the European Securities and Markets Authority (ESMA) listed Portugal as being "non-compliant by default," due to the lack of formal designation of the national competent authorities responsible for DORA's supervision and enforcement.

However, this process is actively underway. In September 2025, the Portuguese government submitted to Parliament the Draft Law No. 34/XVII/1, aimed at defining the national implementation framework for DORA.

The draft law designates the national competent authorities for DORA's implementation: Banco de Portugal for the banking system, the Portuguese Securities Market Commission (CMVM) for capital markets, and the Insurance and Pension Funds Supervisory Authority (ASF) for the insurance and pensions sector. These three authorities are required to cooperate closely in carrying out their supervisory responsibilities.

The draft law introduces a sanctioning regime for ICT risk management breaches, including inadequate disclosure, lack of cooperation, or governance failures, and sets administrative fines of up to €5 million for major institutions and €2.5 million for smaller entities.

Once approved by Parliament, the law will still require complementary regulation from the three supervisory authorities to finalize Portugal's adoption of the DORA framework.

Transposition of the NIS2 Directive

Legislative progress, key steps, and cybersecurity enhancements

Portugal experienced a delay in transposing Directive (EU) 2022/2555, NIS2, originally due by 17 October 2024, due to a complex legislative process affected by political instability and the need for approval by the Assembly of the Republic and promulgation by the president. This delay exposed the country to potential EU sanctions.

In October 2025, a key step toward compliance was achieved when the Assembly of the Republic approved Draft Law No. 7/XVII/1 (GOV), published as Law No. 59/2025 in the Official Gazette on 22 October 2025, authorizing the government to implement the transposition.

The legislative process in Portugal now continues through the following stages:

- Finalization of the text in Committee;
- Publication in the Official Journal of the Assembly of the Republic;
- Promulgation by the President of the Republic (20 days for promulgation, or 8 days if a request for constitutional review is submitted);
- Ministerial endorsement; and
- Publication in the Official Gazette.

Directive NIS2 strengthens EU cybersecurity by imposing stricter requirements for risk management, incident reporting, and resilience in critical sectors such as energy, transport, healthcare, digital infrastructure, and public administration. It also introduces clearer obligations, stronger supervisory powers, and harmonized enforcement, ensuring a higher common level of protection against cyberthreats.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cybersecurity overview – Portugal and the European Union

According to the 2024 report of the Portuguese Ministry of Foreign Affairs, the year marked significant progress in cybersecurity at both the European and national levels, reflecting a continued effort to strengthen digital resilience and collective response to cyberthreats.

At the European level, three major legislative instruments entered into force:

- Cyber Resilience Act – establishing horizontal cybersecurity requirements for products with digital elements;
- Cyber Solidarity Act – enhancing the EU's capacity to detect, prepare for, and respond to cybersecurity incidents; and
- The amendment to the Cybersecurity Act – extending its scope to managed security services.

Portugal actively supported these developments and contributed to the Council Conclusions on ENISA and the Future of Cybersecurity, which highlighted the agency's growing role and called for deeper cooperation and prioritization of tasks among EU member states.

At the national level, work progressed on several key initiatives, including:

- New National Cybersecurity Strategy, defining strategic priorities and objectives;
- National Plan for Large-Scale Cyber Crisis and Incident Response; and
- National Cybersecurity Reference Framework, aimed at identifying and sharing best practices.

A public consultation on the new Cybersecurity Legal Regime, held from 22 November to 31 December 2024, gathered nearly 150 contributions from civil society, reflecting growing national engagement in cybersecurity governance.

Overall, 2024 was a year of consolidation and preparation, strengthening cooperation at the EU level and laying the groundwork for Portugal's upcoming regulatory and strategic developments in 2025.

Cybersecurity updates in Portugal – September 2025 report

In 2024, cybersecurity incidents in Portugal increased significantly. The National Cybersecurity Center (CNCS) recommends strategic actions to mitigate risks and strengthen digital resilience. General recommendations include:

- Fostering sectoral and regional cybersecurity communities to share threat indicators;
- Correlating threat identification with mitigation actions, including human and technological capacity-building; and
- Raising awareness among citizens and employees about best cybersecurity practices.

To address the main cybersecurity threats identified in Portugal, the following recommendations should be implemented:

- Phishing and social engineering: Raise employee awareness, conduct simulated attacks, and monitor compliance with defined security policies;
- Online fraud: Verify the legitimacy of requested bank transfers, use virtual wallets or temporary cards for supplier payments, check supplier websites (prefer HTTPS), and enforce security policies;
- Ransomware: Maintain backups in secondary, disconnected locations, keep systems, applications, and antivirus software up to date, segment networks, avoid unsafe websites, and prohibit unknown USB devices, all monitored via security policies;
- Vulnerability Exploitation: Maintain an updated asset inventory, perform risk analyses to identify and categorize vulnerabilities, and implement formal processes for receiving submissions of vulnerabilities from internal and external sources; and
- DDoS attacks: Monitor resource metrics and history, ensure sufficient computing capacity, and implement redundancy mechanisms in systems supporting critical services.

The CNCS offers key resources and tools to support cybersecurity, including frameworks, guides on risk management and multi-factor authentication, and platforms such as Cibercheckup, Webcheck, and C-Academy.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Portugal takes AI copyright battle to Brussels

Defense of creators and cultural rights in AI regulation

In May 2025, Portugal raised the issue of copyright protection and transparency in AI use at the EU Council of Ministers for Culture in Brussels. The country highlighted the need for AI development to respect the rights of creators and preserve cultural diversity.

Portugal stressed that general-purpose AI models, which are trained on large amounts of content such as books, music, films, and images, should not use protected material without the explicit consent of rights holders. Musicians, writers, filmmakers, and other creators should be fairly compensated if their work is used in AI training.

Portugal presented three key proposals to the EU: (i) AI systems should only use protected content with clear permission from the creators, (ii) all contracts involving AI and cultural content should be transparent and fair, and (iii) the use of data in AI training should be fully traceable through reliable identifiers like ISBNs for books or ISRCs for music.

By taking this stance, Portugal aims to safeguard artists' rights, ensure a fair digital ecosystem, and influence the shaping of future EU AI regulations, emphasizing that the growth of AI must not come at the expense of cultural richness and fundamental rights.

Relation between EDPB Opinion and CNPD alert on AI data processing

The European Data Protection Board (EDPB) Opinion 28/2024 on the use of personal data in AI models provides a comprehensive framework for addressing data protection challenges throughout the AI lifecycle. It clarifies key aspects such as the conditions under which models can be considered anonymous, the potential reliance on legitimate interest as a legal basis for processing, and the implications of using illicitly obtained data in model development. The EDPB Opinion aims to align data protection principles with the upcoming AI Act, promoting a consistent, risk-based approach across the EU.

In this context, the Portuguese Data Protection Authority (CNPD) issued an alert concerning the use of personal data by Meta for training its AI systems, including chatbots and language models. The CNPD warned that Meta plans to process public user data from Facebook, Instagram, and WhatsApp, and reminded data subjects of their right to object under the GDPR. The authority also announced cooperation with other European supervisory authorities to assess the compliance of these processing activities with EU data protection law.

The CNPD's alert is therefore closely aligned with the principles outlined in the EDPB Opinion. While the Opinion provides the theoretical and legal framework for assessing data processing in AI, the CNPD's intervention represents its practical application at the national level, ensuring that AI model training practices, such as Meta's, are evaluated in light of the GDPR and the guidance set at the European level

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Implementation of the AI Act regulation

The AI Act (Regulation (EU) 2024/1689) is an EU regulation and is therefore directly applicable in Portugal without the need for national transposition. Portugal has published a roadmap for the application of the AI Act on the Digital Government portal, and the regulation officially entered into force on 1 August 2024. In compliance with Article 77 of the AI Act, Portugal has published the list of national entities responsible for supervising the protection of fundamental rights under the AI Act by 2 November 2024.

However, some challenges remain. Although the regulation is applicable, Portugal has not yet designated a single national AI regulator with full supervisory powers across all sectors. Only seven EU member states had officially done so as of September 2025, and Portugal was among those with delays.

The obligations under the AI Act are being phased in, meaning that rules for high-risk AI systems and general-purpose AI models will only fully apply in the coming years (e.g., August 2025, August 2026, and August 2027). While the national strategy for AI (AI Portugal 2030) is in place, sector-specific implementing rules, enforcement mechanisms, and detailed national guidance are still under development.

For organizations operating AI systems in Portugal, this means that AI Act obligations already apply, and preparations should be underway for upcoming deadlines, such as those in February 2025. Stakeholders need to monitor which national authority will lead supervisory activities, how sector oversight will be implemented, and follow national guidance while remembering that the regulation is directly applicable. The current delay in full operational supervision offers a window for proactive compliance readiness, but this window may shorten as national enforcement structures are established.

AI Act implementation in Portugal roadmap

- **1 August 2024:** Regulation enters into force.
- **2 November 2024**: Publication of the list of entities supervising the protection of fundamental rights (Article 77 of the AI Regulation).
- **From 2 February 2025:** Application of Chapters I and II.
- **By 2 May 2025:** Development of Codes of Practice for GPAI (Article 56(9)).
- **By 2 August 2025**:
  - GPAI models must comply with the Regulation (Chapter V);
  - Governance – identification of National Competent Authorities, Notifying Authorities, and Market Surveillance Authorities (Chapter VII); and
  - Definition of fines and penalties (Recital 179).
- **From 2 August 2025:** Every two years, EU member states report to the Commission on the financial and human resources available to National Competent Authorities, including an assessment of their adequacy; the Commission transmits this information to the board for review and possible recommendations (Article 70(2)).
- **By 2 February 2026:** Deadline for the Commission to provide guidance on the practical application of Article 6 for High-Risk AI Systems.
- **From 2 August 2026:** Application of the remaining parts of the regulation, except Article 6(1).
- **From 2 August 2027:**
  - Application of Article 6(1) for High-Risk AI Systems (Article 113);
  - Providers of GPAI models placed on the market before 2 August 2025 must meet all obligations by this date (Article 111(3)); and
  - AI systems that are components of large-scale IT systems (Annex X) placed on the market/in service before this date must comply by 31 December 2030 (Article 111(1)).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

On 28 January 2025, marking Data Protection Day, the CNPD announced the creation of a priority channel on its website to handle urgent complaints from children and young people regarding online content involving extreme violence, particularly against minors and young women.

This initiative aims to provide faster and more effective protection for children in the digital environment and will be accompanied by a draft law to be submitted to Parliament, inspired by the Spanish model where removal orders must be executed within 48 hours. The CNPD also reaffirmed its proactive stance in AI regulation, advocating that supervision of AI involving personal data should fall under its remit as Portugal's independent data protection authority.

Cybersecurity

Portugal has taken a decisive step to strengthen its digital security with the publication of Law No. 59/2025, authorizing the transposition of the EU NIS2 Directive (EU 2022/2555). Published in the Diário da República on 22 October 2025, the law sets a 180-day timeline for full transposition.

NIS2 significantly raises cybersecurity requirements for essential and important entities across multiple sectors, including energy, transport, health, digital infrastructure, and public administration. As a result, organizations will need to enhance risk management, incident reporting, and governance practices to comply with the updated EU cybersecurity framework.

AI

In the context of the AI Act (EU Regulation 2024/1689), Portugal is actively preparing for implementation, though full operational supervision has been delayed.

The Administrative Modernization Agency currently represents Portugal at the EU level, but there is a strong likelihood that Autoridade Nacional de Comunicações (ANACOM) will become the single point of contact (SPOC) responsible for overseeing compliance with the AI Act.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Romania

Contacts

Georgiana Singurel

Partner, Reff & Associates (member of the Deloitte Legal network)

gsingurel@reff-associates.ro

Maria-Silvia Axinescu

Counsel, Reff & Associates (member of the Deloitte Legal network)

maxinescu@reff-associates.ro

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Public institutions and data protection compliance

Unlawful video surveillance and improper processing of personal data by public institutions

The National Supervisory Authority for Personal Data Processing (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)) continues to monitor compliance across all sectors, including public institutions, and has applied several sanctions for breaches of data protection rules:

- Warnings applied to Highschool Vasile Conta from Târgu Neamț for unlawful and excessive video surveillance, including in restrooms. ANSPDCP applied two warnings after finding that the school processed personal data through a video and audio surveillance system that also captured images in restrooms and that access to footage was available to unauthorized persons, including the school principal via a personal device. The authority ordered the school to revise internal procedures, ensure limited and secure access to recordings, and allocate monitoring screens only to authorized personnel. Under the applicable national law, if the corrective measures are not fully implemented, ANSPDCP may subsequently impose a fine ranging from RON 10,000 to RON 200,000 (Source: Comunicat_Presa_07.02.2025).
- Warnings applied to the local police of Miercurea-Ciuc and the local police of Craiova for unlawful processing of personal data through body-cam systems. ANSPDCP found that local police officers recorded images and audio using portable body-cam devices without a legal basis or statutory authorization for such processing. The authority ordered both local police departments to ensure that data processing operations carried out through body-cam systems comply with the principles of legality, fairness and transparency, and to bring surveillance activities in line with GDPR requirements (Source: Comunicat_Presa_07.05.2025).

ANSPDCP role in upholding data processing principles

Continuous oversight of controllers' adherence to data processing principles

Throughout 2025, there was an observed increase in the number of fines applied by ANSPDCP in cases of breaches of security. Some notable examples include:

- Fines totaling €25,000 applied to the political party AUR for unauthorized disclosure and unlawful processing of personal data. ANSPDCP found that vulnerabilities in the party's mobile app aur.mobi allowed unauthorized access to the personal data of supporters and members, including identification and political information. Additionally, data collected via semnezsivotez.ro and semnezsivotez.org was processed without a valid legal basis and included categories of data not relevant to the declared purposes. The authority ordered AUR to ensure the implementation of appropriate security and data minimization measures (Source: Comunicat_Presa_07_07_2025).
- Fine of €40,000 applied to Orange Romania S.A. for failure to properly handle data erasure requests and for excessive collection of personal data. ANSPDCP found that the operator did not properly respond to a data subject's request for erasure and retained unnecessary personal data, including scanned ID documents, collected during an unsuccessful subscription process, and ordered Orange to provide a complete response to the erasure request, delete the unlawfully stored data, and ensure that personal data collected prior to contract conclusion are limited to what is necessary and based on a valid legal ground (Source: Comunicat_Presa_27_01_2025).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

ANSPDCP role in breaches of security

- Fine of €15,000 applied to UniCredit Bank S.A. for inadequate testing of IT systems leading to unauthorized disclosure of client data. ANSPDCP found that two separate incidents occurred due to the bank's failure to properly test new applications and communication tools before deployment, resulting in unauthorized disclosure of personal and financial data of clients, including account details and card transaction information. The authority ordered UniCredit to implement a comprehensive testing plan for all applications involving personal data processing, ensuring that functionalities are validated in a secure test environment before production use (Source: Comunicat_Presa_03_02_2025).
- Fine of €20,000 applied to Webrasoft S.R.L. following a cyberattack resulting in unauthorized access to client data. ANSPDCP found that the operator's online invoicing platform was the target of a cyberattack that allowed illegal access to the customer database, exposing personal data such as names, addresses, CNPs, phone numbers, emails, and bank account details. The authority ordered Webrasoft to implement a logging system to record all access attempts and errors on its servers, retain logs for at least 30 days, and ensure regular back-ups to strengthen the company's data security framework (Source: Comunicat_Presa_04_03_2025).
- Fine of €20,000 applied to PRIMONET RO S.R.L. following a cyberattack affecting customer payment data. ANSPDCP found that a security breach on the company's e-commerce platform led to unauthorized access to cardholder information, including card numbers, CVC codes, holder names, and expiration dates, which resulted in unauthorized financial transactions and monetary losses for several customers. The investigation revealed that the company was using an outdated version of its online platform and had not implemented sufficient technical and organizational measures to ensure an adequate level of data security. The authority ordered the operator to implement a comprehensive logging and backup system to monitor all access attempts to its e-commerce platform (Source: Comunicat_Presa_25_09_2025).
- Fine of €25,000 applied to E.ON Energie România S.A. following a personal data breach affecting user accounts. ANSPDCP found that unauthorized access to a significant number of user accounts resulted in the exfiltration of email addresses and passwords, creating a high risk of potential financial harm. The investigation revealed that the company had not implemented adequate technical and organizational measures to ensure an appropriate level of security. The authority ordered E.ON to implement multi-factor authentication for all users and adopt additional security measures to prevent unauthorized access (Source: Comunicat_Presa_09_10_2025).
- Fine of €15,000 applied to S.P.E.E.H. Hidroelectrica S.A. following a personal data breach caused by a technical error. ANSPDCP sanctioned the company after identifying that a personal data breach occurred during the launch of its application, due to a technical error and insufficient prelaunch testing in a simulated environment. The incident resulted in the loss of integrity and availability of personal data, as well as unauthorized disclosure and access to the data of a significant number of individuals. The authority ordered the operator to implement a structured testing plan in a controlled environment simulating real-use conditions before deploying any new components or applications involving personal data processing (Source: Comunicat_Presa_31.01.2025_1).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Transposition of the NIS2 Directive in Romania

Cybersecurity framework established by GEO 155/2024

On 30 December 2024, Romania transposed the NIS2 Directive into national law through Government Emergency Ordinance No. 155/2024 (GEO 155) regarding the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace. The provisions of GEO 155 apply to all organizations, including businesses and suppliers, that provide essential or important services to the European economy and society.

Key provisions introduced by GEO 155 include:

- Registration: Essential and important entities must register with the National Directorate of Cybersecurity (the DNSC). Registration entails the obligation to submit a risk level assessment and to conduct a self-assessment of cybersecurity risk management maturity;
- Risk analysis: Entities must implement technical, operational, and organizational measures to identify, assess, and manage security risks related to the networks and information systems they use. These measures must include internal policies, incident management, and business continuity planning;
- Corporate responsibility: Corporate management must oversee, approve, and receive training on cybersecurity measures and risk mitigation processes;
- Incident reporting: Entities must establish procedures to report major incidents via the National Platform for Cybersecurity Incident Reporting (PNRISC) and, where applicable, to inform service recipients about incidents and corrective measures; and
- Sanctions: GEO 155 provides for fines ranging from RON 5,000 to €10 million, or up to 2% of the annual turnover, whichever is higher.

Secondary regulations implementing GEO 155/2024

DNSC issues the first orders for the implementation of GEO 155/2024

Designated as the competent authority for implementing and enforcing GEO 155, DNSC has adopted the first two pieces of secondary legislation detailing the registration process, the evaluation criteria and the risk assessment methodology applicable to essential and important entities.

Specifically, the following acts were published in 2025:

- DNSC Director's Order No. 1/2025 – approving the Requirements concerning the notification process for registration and the method of transmitting information; and
- DNSC Director's Order No. 2/2025 – approving the Criteria and thresholds for determining the degree of disruption of a service and the Methodology for assessing the risk level of entities.

On 20 August 2025, the above-mentioned DNSC orders specifying the registration process and the means of evaluating the criteria regarding the company profile and for evaluating the risk level were published in the Official Gazette. The 30-day term for registration started at that date, therefore entities should have notified the DNSC in order to register as an essential/important entity with the authority by now.

Furthermore, on 23 October 2025, DNSC published the draft order approving the implementation norms and the risk-based prioritization methodology for supervision, verification and control activities, expected to enter into force by the end of 2025.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

AI Act implementation in Romania

Designation of national authorities under Article 77 of the AI Act

In accordance with Article 77 paragraph 2 of the AI Act, EU member states are required to identify the national public authorities responsible for supervising or enforcing compliance with obligations under EU legislation protecting fundamental rights, including the right to nondiscrimination, in connection with the use of high-risk AI systems listed in Annex III of the Regulation.

Following this requirement, the Authority for the Digitalization of Romania (ADR) published a press release announcing the list of national authorities notified to the European Commission, as follows:

- The Ombudsman (Avocatul Poporului);
- The National Authority for Consumer Protection (ANPC);
- The National Council for Combating Discrimination (CNCD);
- The National Agency for Equal Opportunities between Women and Men;
- The National Supervisory Authority for Personal Data Processing (ANSPDCP);
- The National Authority for the Protection of Children's Rights and Adoption;
- The Ministry of Labor and Social Solidarity/Labor Inspection;
- The National Audiovisual Council (CNA); and
- The Permanent Electoral Authority.

(Source: Lista autorităților publice naționale care supraveghează sau asigură respectarea obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale, în conformitate cu art. 77 al Regulamentului privind Inteligența Artificială – ADR)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Further secondary legislation under GEO 155/2024 on cybersecurity

Upcoming DNSC orders detailing risk management and operational requirements

Following the adoption of the first two DNSC Director's Orders, additional implementing acts are expected to be published to detail the requirements for several aspects, namely:

- Risk management measures and maturity level assessment;
- Conducting audits;
- Supply chain management; and
- Management and CISO training courses.

These acts will complete the operational framework necessary for the effective implementation of the NIS2 Directive in Romania.

Designation of the national notifying authority

Pending step in Romania's implementation of the AI Act

Under the AI Act, EU member states are required to designate or establish national notifying authorities responsible for setting up and conducting the procedures for the assessment, designation, and notification of conformity assessment bodies, as well as for monitoring their activity. These notified bodies play a key role in the conformity assessment process for high-risk AI systems.

While Romania has already communicated to the European Commission the list of national authorities responsible for safeguarding fundamental rights in the context of AI use, the designation of the national notifying authority remains pending, and is expected to be completed in 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Serbia

Contacts

Mirjana Mladenović

Director, Deloitte Legal Serbia

mimladenovic@deloittece.com

Igor Denčić

Senior Manager, Deloitte Legal Serbia

idencic@deloittece.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Activities of the Commissioner for Personal Data Protection in 2024

Scope of the commissioner's activities: In 2024, the Commissioner for Information of Public Importance and Personal Data Protection formed 3,372 cases and successfully resolved 4,110 cases in the field of personal data protection. The commissioner completed 864 inspections (706 regular and 158 extraordinary), of which 790 were conducted onsite. During these inspections, 59 corrective measures were imposed and one prohibition on data processing was issued. The most frequently inspected entities were public enterprises (35.4%).

Misdemeanor liability: The commissioner submitted seven requests for initiating misdemeanor proceedings and issued 2 misdemeanor orders.

Data protection officers: In 2024, 535 controllers submitted information about their data protection officers, bringing the total number of controllers that have fulfilled this obligation to 6,315.

Processing of citizens' complaints: The commissioner processed 284 complaints (228 new and 56 from the previous period), of which 267 were resolved. The most common reasons for complaints were refusal of requests for exercising rights (129), failure to act upon requests (51), and partial compliance with requests (47). The most frequently violated rights were the right to access data (66.1%) and the right to erasure of personal data (32.2%).

The commissioner also identified the most significant shortcomings of the local law, including unclear provisions, transcribed mechanisms that do not exist in the domestic legal system, inadequate transposition of the "police directive" which created two parallel data processing regimes, inappropriately elaborated procedural provisions regarding the commissioner's handling of complaints, inconsistency with the "ne bis in idem" principle, absence of mutual notification obligation between competent authorities, excessive number of paragraphs in articles, excessive exemptions from application, and failure to harmonize other laws.

Balkan Data Protection Initiative confronts "Meta" and "X" privacy practices

The Commissioner for Information of Public Importance and Personal Data Protection issued a statement regarding the numerous inquiries from citizens with requests for exercising rights related to the protection of personal data processed by Meta Platforms Inc. (owner of social networks Facebook, Instagram, WhatsApp) and its privacy policy adopted on 26 June 2024.

Meta's privacy policy is available in Serbian and contains information for users about mechanisms through which they can effectively exercise their privacy rights. This includes a contact form in the section "How to contact Meta if you have questions."

Meta has introduced a "privacy center" as a central point where users can better understand the company's practices and make informed decisions about their privacy. The "privacy center" was created to enable users to make privacy choices that suit them and to explain how they can manage their privacy on Facebook, Instagram, Messenger, and other Meta products. Meta's "privacy center" is also available in Serbian, which allows easier access and use of these tools for users from Serbia.

Additionally, at the third meeting of the Privacy4Balkans initiative held on 30 October 2025, in Belgrade, personal data protection authorities from Bosnia and Herzegovina, Montenegro, Serbia, and newly joined North Macedonia agreed on joint actions against companies "Meta" and "X" for unauthorized processing of data for artificial intelligence development and failure to appoint local data protection officers. The meeting, attended by directors and high representatives of all four national data protection bodies, resulted in the announcement of signing a memorandum of understanding and establishing a coordinated regional approach to addressing privacy protection issues for western Balkan citizens in the digital space.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Action Plan for the Implementation of Personal Data Protection Strategy

The Action Plan for the period 2025-2027 has been adopted as a key mechanism for implementing the Personal Data Protection Strategy for the period 2023-2030, which will enable systematic implementation of all planned measures to improve the protection of personal data of citizens of the Republic of Serbia.

This plan envisages concrete steps to increase the capacity of the commissioner, introduce specialized training, establish a more efficient system of penalties for offenders, and amend relevant regulations, including the Law on Personal Data Protection.

Special emphasis is placed on strengthening institutional capacities, improving cooperation among state bodies, and aligning domestic practices with European standards in the field of data protection, all with the aim of ensuring a higher level of privacy protection for citizens in the digital environment.

It is expected that the activities implemented from the Action Plan will contribute to a significant reduction in the number of cases of unauthorized data processing and increase public awareness about the importance of personal data protection.

The Strategy and the Action Plan for its implementation represent a response to the growing challenges in the field of personal data protection in the era of digitalization and artificial intelligence development.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

The new Law on Cybersecurity

The new Law on Information Security (Cybersecurity) came into force on 31 October 2025. It establishes a stronger institutional framework and aligns regulations with European standards (the NIS2 Directive and the EU Cybersecurity Act). The law introduce a new institution, the Office for Information Security (the Office), which will be active from 1 January 2027, and its task will be to coordinate responses to serious incidents and manage the National Center for the Prevention of Security Risks in ICT systems (the National CERT). The most significant provisions of this law:

- ICT systems of special importance are divided into priority and important categories, with precise categorization by activities. Priority systems include energy, banking, healthcare, water supply, digital infrastructure, nuclear facilities, electronic communications, content delivery networks, and other critical segments.
- Operators can be legal entities, individuals (entrepreneurs, freelancers), and scientific research organizations that meet the criteria set forth in the bylaw. The competent minister may designate additional operators whose system interruption would significantly impact the state and economy.
- Basic obligations of all operators include the implementation of technical and organizational protection measures in accordance with national and international standards, adoption of risk assessment and ICT system security acts, regular verification of security act implementation, reporting of serious incidents, and submission of annual statistical reports on incidents.
- Reports of incidents that significantly compromise information security must be made without delay or within 24 hours at the latest through the portal of the Ministry of Information and Telecommunications or the Office. Incidents are classified into four levels: low, medium, high, and very high.
- For low-level incidents, the operator can respond independently, with possible recommendations from the Office. For medium incidents, the Office is required to provide recommendations, while for high-level incidents, the Office convenes an operational team and the government's coordination body. In cases of very high-level incidents, the government declares an information security crisis and assumes primary responsibility for incident resolution, while the operator implements mandatory measures.
- During high and very high-level incidents, operators must submit reports every 24 hours, and for medium incidents every three days. The final report must be submitted within 15 days after the incident's resolution. Additionally, once a year, by 28 February detailed statistical data on all incidents must be submitted through the National CERT.
- The Ministry of Information and Telecommunications maintains a registry of operators, conducts inspections, and receives incident reports until the Office becomes operational.
- The .rs domain registry and the list of authorized registered bodies are now legally established. The Ministry of Defense remains responsible for approving cryptographic products for classified data and verifying protection against compromising electromagnetic radiation.
- Professional supervision will be conducted from 1 January 2027, to evaluate risk management, technological procedures, and the implementation of protection measures. In case of deficiencies, the inspector may order corrections or initiate misdemeanor proceedings. Misdemeanor liability provides for fines ranging up to 2 million dinars for priority systems and up to 1 million dinars for important systems, while penalties for individuals are lower.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Amendments to the Personal Data Protection Law: Focus on AI and new technologies

The Ministry of Justice has formed a special working group to prepare amendments to the Law on Personal Data Protection from 2018, as numerous deficiencies have been observed in practice that hinder its implementation. Commissioner emphasizes that AI is one of the most important reasons for amending the law, because when the European regulation was adopted in 2016, and local law in 2019, such a rapid development of technologies and artificial intelligence could not have been foreseen.

The draft of the new law will comprehensively regulate the field of personal data protection, with a special focus on provisions related to information technologies, video surveillance, biometric data, and AI. It is necessary to precisely determine the application of the law so that it also covers controllers and processors who do not have headquarters in the territory of Serbia but process personal data as part of activities in our territory.

It is necessary to more clearly define the terms “competent authority” and “punishable offenses”, as well as to create a special chapter for the processing of personal data carried out by competent authorities for special purposes. The new law will more precisely regulate matters relating to codes of conduct, issuance of certificates, and the transfer of data to other countries and international organizations, as well as the complaint procedure.

The commissioner emphasizes that Serbia has an opportunity to be ahead of the EU regarding the regulation of AI, which particularly endangers children between the ages of 12 and 18. It is necessary to further regulate the processing of genetic and biometric data for the purpose of unique identification of natural persons, as well as the processing of data through video devices and artificial intelligence.

Development of regulatory framework for AI in Serbia: Between European model and innovation

The Republic of Serbia adopted the Strategy for the Development of Artificial Intelligence for the period 2025-2030 in January 2025, which serves as the foundation for the upcoming Law on Artificial Intelligence. A multidisciplinary working group has been formed that uses the European AI Act as a reference model in drafting the law, classifying AI systems into four risk categories, from minimal to unacceptable. For high-risk systems in the fields of healthcare, education, and security, strict regulatory measures are envisaged, while certain systems such as social scoring are completely prohibited.

The previous Ethical Guidelines for AI Development from 2023 established moral principles but could not sanction abuses, making the enactment of legislation necessary. Serbian regulations will apply to all companies operating in the domestic market, regardless of origin, balancing data protection and innovation promotion. IT sector representatives emphasize that Serbia has a unique opportunity to develop more flexible legislation compared to the EU, which could attract companies that consider European regulations too restrictive.

Special attention in the law will be given to copyright protection, privacy, and adaptability to future technological changes. Due to the rapid development of technology, Serbian legislators anticipate regular revisions of the law to respond to new challenges while enabling competitiveness for domestic companies in the global artificial intelligence market.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Singapore

Contacts

Joanna Yap

Managing Director, Sabara Law LLC (member of the Deloitte Legal network)

joayap@sabaralaw.com.sg

Gretchen Su

Director, Sabara Law LLC (member of the Deloitte Legal network)

gretchensu@sabaralaw.com.sg

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Privacy Enhancing Technologies (PETs) Adoption Guide

In July 2025, the Infocomm Media Development Authority (IMDA) released the PETs Adoption Guide, which incorporates key practical lessons and case studies from the PETs Sandbox developed by IMDA in 2022.

The PETs Sandbox enabled companies to collaborate with PET solution providers to develop use cases and pilot PETs with technological, financial and regulatory support from IMDA. The lessons learned have now been integrated into the adoption guide.

The guide provides two key resources: the "PETs Use Case Evaluation Tool," designed to help organizations identify and assess suitable PET solutions for their specific business needs, and an "Implementation Checklist." which highlights key considerations for organizations throughout the PETs adoption journey, from evaluation to gradual implementation.

The guide is currently in its first draft and is intended to serve as a living document that IMDA will update periodically based on industry feedback and new use cases from the PETs Sandbox. IMDA is currently inviting feedback from industry participants.

Data Protection Trustmark and Singapore Standard 714

The Data Protection Trustmark (DPTM) is a voluntary certification that allows organizations to demonstrate that they have robust data protection policies in place to manage personal data in accordance with the relevant framework. The Trustmark is based on the Personal Data Protection Act (PDPA), as well as international benchmarks and best practices. According to the Personal Data Protection Commission (PDPC), it may serve as a mitigating factor in enforcement actions arising from data breaches.

In June 2025, the DPTM was incorporated into the Singapore National Standards as SS 714:2025 – Data Protection Trustmark, enhancing the level of recognition for organizations that have obtained DPTM certification. The revised DPTM includes:

- Updated language that clarifies the requirements for organizations seeking certification;
- A streamlined certification process that allows organizations to work with a single certification body;
- Assessments conducted by bodies overseen by the Singapore Accreditation Council; and
- Annual surveillance audits to enhance confidence in an organization's data protection practices.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Landmark High Court Decision on Deemed Consent and Actionable Loss under the PDPA

In August 2025, the Singapore High Court found that a charity breached its obligation to protect an individual's data by revealing their identity to the person they had complained about. The claimant had sent an email to a registered charity using their full name and personal email, complaining about a representative of the charity for allegedly making discriminatory comments in a separate social media group. During the investigation, the charity disclosed the claimant's name and email to the subject of the complaint, stating that it would be best if they responded directly.

The claimant brought a private action claim against the charity under the PDPA. The High Court considered whether the charity could rely on the exception of deemed consent and the investigation exception, as well as whether the claimant suffered actionable losses.

The court clarified that deemed consent is always subject to the purpose limitation obligation and an overarching standard of reasonableness. In this case, the disclosure of the claimant's name and email to the subject of the complaint could not have been anticipated by the claimant since it was not necessary for the purpose of the investigation. As the disclosure was not necessary, the court also found that the charity could not rely on the investigation exception.

Accordingly, the court found that the charity had breached its data protection obligations under the PDPA.

However, the court found the charity was not liable to compensate the claimant as the intervening retaliatory actions by the subject of the complaint constituted a break in the chain of causation, and the claimant did not demonstrate any actionable harm suffered directly due to the actions of the charity.

ASEAN Guide on Data Anonymization

In January 2025, during the fifth ASEAN Digital Ministers' Meeting, the ASEAN Guide on Data Anonymization was released. The guide is intended to provide information and guidance on basic data anonymization. It offers a general introduction to data anonymization and common techniques. It is primarily aimed at governments and industry organizations that process personal data and are located in ASEAN member countries. It will also benefit professionals in risk assessment and compliance, who may need to understand the capabilities and limitations of anonymization techniques within the context of their specific domains.

The guide is divided into three parts. Part 1 outlines the purpose and scope of the guide, the benefits of anonymization, and the current data protection landscape in ASEAN. Part 2 explains key concepts and terminology related to data anonymization and describes typical scenarios in which these techniques are applied. Part 3 provides an overview of anonymization techniques and explains the key steps that must be undertaken during the data anonymization process.

The anonymization techniques are suitable for data in which each record pertains to and represents a specific individual. The guide focuses on tabular and similarly structured data, typically stored in Excel sheets, SQL databases, JSON format, and similar structures.

Joint guide to ASEAN MCCs and RIPD MCCs

In January 2025, during the fifth ASEAN Digital Ministers' Meeting, the joint guide to ASEAN MCCs and RIPD MCCs was released. The guide aims to provide guidance on the use of the ASEAN MCCs and the Ibero-American Data Protection Network's (RIPD) MCCs. These are model data protection clauses that can be incorporated by data exporters and importers into their contractual agreements when transferring data across borders.

The purpose of the guide is to assist companies and organizations operating in the ASEAN and Ibero-American regions in understanding the similarities and differences between the respective contractual clauses, thereby facilitating contractual negotiations and compliance with applicable data protection laws. The guidance will also help organizations meet the requirements of the contractual clauses themselves.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Joint Guide to ASEAN MCCs and RIPD MCCs

In January 2025, during the fifth ASEAN Digital Ministers' Meeting, the joint guide to ASEAN MCCs and RIPD MCCs was released. The guide aims to provide guidance on the use of the ASEAN MCCs and the Ibero-American Data Protection Network's (RIPD) MCCs. These are model data protection clauses that can be incorporated by data exporters and importers into their contractual agreements when transferring data across borders.

The purpose of the guide is to assist companies and organizations operating in the ASEAN and Ibero-American regions in understanding the similarities and differences between the respective contractual clauses, thereby facilitating contractual negotiations and compliance with applicable data protection laws. The guidance will also help organizations meet the requirements of the contractual clauses themselves.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Public consultation on securing agentic AI – An addendum to the Guidelines and Companion Guide on Securing AI Systems

In October 2025, the Cyber Security Agency of Singapore (CSA) released a guide specifically on securing agentic AI. The guide serves as an addendum to the broader Guidelines on Securing AI Systems and the Companion Guide on Securing AI Systems released by CSA in October 2024. The addendum is currently a draft version, released for public consultation, and is expected to be finalized in the coming year.

The addendum was issued proactively by the Singapore government in response to growing interest in agentic AI and its potential risks. It has been developed jointly with industry, government, and international partners to support organizations in securing their agentic AI systems. The addendum is designed to be read alongside the AI Guidelines and Companion Guide and is intended to:

- Outline how risks can be identified and assessed based on the capabilities of the respective agentic AI systems; and
- Provide practical controls to mitigate identified risks across the AI's developmental lifecycle. This will be supplemented by practical examples illustrating how the addendum should be applied across different scenarios and levels of system autonomy, including applications such as app development, automated client onboarding systems, and automated fraud detection systems.

Singapore Cyber Landscape 2024/2025

In September 2025, the CSA released a publication reviewing Singapore's cybersecurity situation and the overall threat landscape.

The publication analyzes multiple data sources and developments to identify common cyberthreats in Singapore's cyberspace. It includes case studies of incidents in Singapore, aimed at raising public awareness among stakeholders and the general public, while also offering practical and actionable insights.

Notably, the report highlighted the adoption of new technologies and their potential impact on cyberspace. This includes artificial intelligence, cloud services, the Internet of Things, and hypervisor attacks.

The report also outlined key challenges and vulnerabilities that must be addressed to ensure Singapore's cyberspace remains secure. These include specific threats such as the human element being a weak link due to social engineering, supply chain vulnerabilities where reliance on third parties can lead to cascading effects, and the convergence of physical and digital domains producing tangible impacts. It also highlights more indirect threats, including the ongoing cyber talent shortage requiring continuous investment, and the unpredictable evolution of threats driven by new technologies, necessitating agility and constant adaptation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Quantum-Safe Handbook and Quantum Readiness Index

In October 2025, the CSA issued the Quantum-Safe Handbook and Quantum Readiness Index to help organizations prepare for the emerging risks posed by quantum computing. The two documents are currently drafts which are open for public consultation, with feedback invited from stakeholders.

While quantum technology promises major advances across sectors such as logistics, finance, and healthcare, it also introduces the "quantum threat," whereby sufficiently powerful quantum computers could break existing cryptographic systems and compromise secure communications, transactions, and data integrity. To address this risk, the CSA has emphasized the need for organizations to begin transitioning to quantum-safe cryptographic solutions early, as the migration process is complex and requires long-term planning, resource allocation, and coordination across systems and products.

The Quantum-Safe Handbook was jointly developed by the CSA, GovTech, and IMDA, in collaboration with technology companies, cybersecurity consultancies, and professional associations. It provides practical guidance for organizations, particularly Critical Information Infrastructure (CII) owners and government agencies, to assess risks and plan their transition.

The accompanying Quantum Readiness Index is a self-assessment tool that enables organizations to evaluate their level of readiness, identify priority action areas, and facilitate discussions with management to secure support for quantum-safe migration.

Guidance for Organizations During Ransomware Incidents

In October 2024, Singapore and the United Kingdom, under the Counter Ransomware Initiative (CRI), jointly released the Guidance for Organizations During Ransomware Incidents. The guidance reflects a coordinated global effort to reduce the impact of ransomware and discourage ransom payments, which reached record highs in 2023. It seeks to ensure that organizations recognize that paying a ransom to ransomware actors:

- Does not guarantee the end of an incident or the removal of malicious software from their systems;
- Provides incentives for criminals to continue and expand their activities;
- Provides funds that criminal actors can use for illicit purposes; and
- Does not guarantee that organizations will recover their data.

The guidance provides a holistic framework for organizations to manage ransomware incidents responsibly, including advance preparation through business continuity planning, prompt reporting to authorities, and careful evaluation of all response options before considering payment.

It also emphasizes the importance of seeking legal and expert advice, as ransom payments may be unlawful in certain jurisdictions, particularly when sanctioned entities are involved. In addition, it calls for post-incident reviews and stronger cybersecurity resilience, including backup management, network segmentation, and regular system audits.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Agentic Risk and Capability Framework

In July 2025, GovTech released the Agentic Risk and Capability Framework (ARC), developed by its Responsible AI team. The ARC builds on existing frameworks to enable organizations to govern agentic systems effectively and provides practical guidance for assessing and mitigating the associated risks. Notably, the ARC structures the identified risks into a single coherent and actionable framework by differentiating between baseline and capability risks and their corresponding controls.

Baseline risks are associated with the components common to all agents, such as large language models (LLMs), tools, instructions, and memory. They also include common design considerations, particularly how agents are networked and assigned different roles within the system. The ARC framework provides two lists of baseline controls, one shorter and one longer, allowing organizations to implement the shorter list for all systems or the longer list as best practice or for mission-critical systems.

Capability risks are defined as the additional capabilities granted to agentic AI systems beyond the common components and design patterns, enabling them to perform their intended tasks. The ARC framework categorizes these capabilities, identifies the specific risks associated with each, and suggests corresponding technical controls to mitigate those risks.

The framework is designed for real-world implementation, taking into account the practical constraints faced by organizations as well as the competing priorities of governance teams and AI developers. It provides detailed, step-by-step guidance on how governance teams can apply it at an organizational level and how AI developers can use it to manage safety and security risks at a system level.

Global AI Assurance Sandbox

In July 2025, the IMDA and the AI Verify Foundation (AIVF) launched the AI Assurance Sandbox, a global initiative providing a testing ground for builders or deployers of Generative AI applications to have their systems assessed by specialist technical testers. The AI Verify Foundation was established by IMDA in June 2023 to facilitate collaboration and contributions from the global open-source community in developing AI Verify testing tools.

The objective of the sandbox is to reduce testing-related barriers to Generative AI adoption by offering practical guidance and access to specialist testing partners, as well as to provide inputs into the development of technical testing standards for Generative AI applications, supporting the growth of a viable AI assurance market.

The sandbox builds on the Global AI Assurance Pilot, also launched by IMDA and AIVF in February 2025. The pilot focused on testing the reliability of end-to-end Generative AI applications, rather than the commonly tested safety of foundation models. To achieve this, it brought together AI deployers from diverse industries and specialist technical testers from around the world, concluding with a report outlining broad recommendations on Generative AI system testing.

The sandbox seeks to apply the lessons learned from the pilot and continue pairing Generative AI deployers with specialist technical testers in a similar manner.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Lawyer ordered to pay S$800 for citing AI-generated cases

In the case of *Tajudin bin Gulam Rasul v Suriaya bte Haja Mohideen* [2025] SGHCR 33, heard in June 2025, a lawyer cited a fictitious case generated by Generative AI. The error was discovered by the opposing counsel, who flagged that they could not locate the case in any legal databases. In response, the offending lawyer initially amended the submissions, attributing the error to clerical and typographical mistakes. However, during the hearing, when pressed by the court, he admitted that the authority was entirely fictitious and generated by AI.

The lawyer apologized, stating that the work had originally been prepared by a junior lawyer, but he had failed to properly check their work before submission. The opposing counsel sought compensation for costs, arguing that they had spent unnecessary time and effort attempting to locate the fictitious case and had been the first to alert the court.

Ultimately, the court ruled that the improper use of AI was "improper," "unreasonable" and "negligent," particularly given that state courts had issued guidance on the proper use of Generative AI in preparing court documents. The lawyer was also admonished for failing to make an initial disclosure and for attempting to downplay the seriousness of the breach. The court emphasized that the misconduct was not solely a matter of wasting judicial time, but also of deception that could "in the eyes of the public, cast a shadow over the legitimacy and honor of the legal profession."

The court ordered the lawyer to pay S$800 to the opposing counsel for the costs incurred due to the fictitious citation. The order demonstrates the court's firm stance that AI-generated authorities will not be tolerated and that lawyers bear personal responsibility to comply with their professional duties.

Expanded ASEAN Guide on AI Governance and Ethics – Generative AI

In January 2025, during the fifth ASEAN Digital Ministers' Meeting, the ASEAN guide on AI governance and ethics for Generative AI was released. It is intended to supplement the ASEAN guide on AI governance and ethics issued in 2024. The guide outlines the opportunities and risks of Generative AI and recommends a range of policy actions that ASEAN decision-makers can take to ensure responsible adoption.

The guide provides guidance on the six Generative AI risks identified in the earlier ASEAN AI guide, as well as on frontier and systemic risks arising from the long-term evolution of advanced Generative AI models not yet present in ASEAN. The identified risks are:

- Mistakes and anthropomorphism;
- Factually inaccurate responses and disinformation;
- Deepfakes, impersonation, and other fraudulent or malicious activities;
- Infringement of intellectual property rights;
- Privacy and confidentiality concerns; and
- Propagation of embedded biases.

For each risk, the guide sets out a range of policy recommendations for ASEAN to consider, promoting the trusted and responsible use of AI while mitigating the risks. The recommendations draw on leading global practices and emphasize the importance of a coordinated, pro-innovation regional approach.

Finally, the guide illustrates how these recommendations can be implemented through detailed use cases featuring public and private institutions across ASEAN that have adopted responsible Generative AI practices. One example is the Responsible AI Internal Programme spearheaded by Accenture across the ASEAN region.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Proposed Amendments to the Public Sector (Governance) Act

The Ministry of Digital Development and Information (MDDI) is consulting on proposed amendments to the Public Sector (Governance) Act to enable public sector agencies to share data with authorized external partners in the delivery of public services.

The amendments aim to provide a clear legal basis for such data sharing, strengthen safeguards and penalties for misuse, and maintain robust governance for both internal and external use of public sector data. They are also expected to lead to consequential amendments to the PDPA.

Updates to licensing framework for cybersecurity providers

The CSA has proposed updates to the licensing framework for cybersecurity service providers, which are set to take effect progressively from January 2026. Key changes include mandatory cybersecurity and data protection certifications, an extension of license validity from two to five years, simplified renewal and reporting requirements, and a phased implementation timeline.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Slovenia

Contacts

Ana Kastelec

Managing Partner, Deloitte Legal Reff Slovenia

akastelec@deloittelegal.si

Gregor Strojin

Partner, Deloitte Legal Reff Slovenia

gstrojin@deloittelegal.si

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Slovene Constitutional Court Decision No. U-I-9/24 of 25 September 2025

Criminal record retention period

The Slovene Data Protection Authority (in Slovenian: Informacijski pooblaščenec (Slovene DPA)) has submitted a request for a constitutional review of Article 129 of the Slovene Police Tasks and Powers Act (Zakon o nalogah in pooblastilih policije (ZNPPol)).

Upon review, the Slovene Constitutional Court has concluded that the paragraph 1 and the first indent of the paragraph 2 of Article 129 of the ZNPPol **did not**:

- Allow for a request for the erasure of data if their storage was no longer necessary;
- Provide for periodic ex officio verification, which would limit the period of storage of personal data to what was strictly necessary to achieve the purpose of storing personal data; and
- Take into account the nature and gravity of the criminal offense and the distinction between different categories of persons to whom the data in the criminal records related, particularly in view of the presumption of innocence under Article 27 of the Slovene Constitution.

Consequently, the Slovene Constitutional Court ruled that the legislator had **impermissibly interfered with the right of information privacy under the first paragraph of Article 38 of the Slovene Constitution with the contested provisions.**

The Slovene Constitutional Court has further found paragraphs 3 and 4 of Article 129 of the ZNPPol insofar as they related to the record of criminal records to be inconsistent with the Slovene Constitution as they were directly related to the paragraph 1 and the first indent of the paragraph 2 of Article 129 of the ZNPPol and had no independent meaning.

2024 Slovene DPA annual report on personal data protection

In May 2025, the Slovene DPA published its annual report on personal data protection for the year 2024. The report summarizes the authority's key activities in 2024. Some of the most relevant topics addressed by the authority have been digitalization of businesses and AI; additional areas include video surveillance, biometrics, processing of personal data of vulnerable subjects and use of healthcare data.

In 2024, the Slovene DPA had: (i) handled 846 inspection cases, among which 177 were related to the public sector and 669 the private sector, (ii) received 160 data breach notifications, (iii) received 28 complaints regarding access to medical records, (iv) participated in 463 cooperation procedures under Articles 60 and 61 of the GDPR, and (v) initiated 105 minor offence proceedings.

The Slovene DPA has further provided a brief explanation of cases that have been received on numerous reports, complaints, official notifications, or questions, among others:

- The collection of personal data in prize games;
- Video surveillance in schools;
- The publication of judges' personal data on social media and publication of the customer's name in response to an online review;
- Providing home address during online shopping while choosing the option to pick up the goods in person;
- Partial access to the video recording by blurring the personal data of other persons; and
- Access to entire partial telephone number without concealing the last three digits.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Guidelines on personal data transfers to third countries

In January 2025, the Slovene DPA has issued guidelines on personal data transfers to third countries. The guidelines are intended to provide general practical guidance to data controllers in case of personal data transfers to third countries in a clear, understandable, and useful manner. The guidelines further provide data controllers with recommendations on how to comply with the requirements of personal data protection legislation in practice.

In particular, the guidelines explain:

- When the personal data transfer is considered as personal data transfer to third countries;
- The conditions for transfer to third countries;
- The instances when approval from Slovene DPA is needed and when personal data may be transferred to third countries without approval and without other protective measures;
- Personal data transfers based on appropriate protective measures, and derogations in specific cases;
- Other personal data transfers (among public authorities, defined in the Personal Data Protection Act (Zakon o varstvu osebnih podatkov (ZVOP-2)), and transfers to the United States); and
- Practical scenarios based on frequently asked questions.

End of the transitional period for the processing log obligation

On 26 January 2025, the two-year transition period from the entry into force of the ZVOP-2 had expired. During the transitional period data controllers were required to bring their processing logs in line with the requirements of Article 22 of ZVOP-2.

Article 22 of ZVOP-2 specifies who is required to keep processing logs, what actions must be recorded, and how long processing logs must be retained. Processing logs should not be confused with records of processing activities under Article 30 of the GDPR.

Enhanced supervision of compliance with the right to erasure

In March 2025, the Slovene DPA has announced to participate in a coordinated enforcement action in the area of compliance with the right to erasure, specifically in the field of shared mobility, where large amounts of user data, including location data, are processed.

The supervision focuses on the process of handling requests for the erasure of personal data, including an analysis of the conditions and exceptions that data controllers take into account when assessing the legitimacy of erasure.

At the end of the year, the Slovene DPA is set to prepare national report on the situation in the area under investigation, and the results will then be analyzed at the European level to provide a comprehensive overview of the practice of exercising this right in the EU and enable the planning of more targeted follow-up measures at both national and EU level.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Overview of the new Information Security Act (ZInfV-1)

Law for the implementation of the NIS2 Directive

The NIS2 Directive (Directive EU 2022/2555) is transposed into Slovenian legal order with the **Information Security Act** (Zakon o informacijski varnosti (ZInfV-1)) which entered into force on **19 June 2025,** and which establishes a comprehensive national cybersecurity framework. In addition to NIS2 Directive it also implements:

- Regulation (EU) 20 Regulation (EU) 2019/881 (the Cybersecurity Act) concerning the EU Agency for Cybersecurity (ENISA) and the EU cybersecurity certification framework for ICT products, services, and processes;
- 21/887 establishing the European Cybersecurity Industrial, Technology and Research Competence and the Network of National Coordination Centers; and
- Regulation (EU) 2025/38 (the Cyber Solidarity Act), which strengthens the EU's capacity and solidarity for detecting, preparing for, and responding to cyberthreats and incidents.

Key rationale and objectives behind the legislation:

- EU regulatory alignment: The primary purpose is transposing EU Directive 2022/2555 (NIS2) into Slovenian law, replacing the previous framework and ensuring compatibility with European cybersecurity standards.
- National security protection: ZInfV-1 aims to ensure uninterrupted functioning of critical national systems across all security situations and preserve essential social and economic activities during cybersecurity incidents.
- Organizational structure: It establishes a comprehensive national cybersecurity framework with clearly defined roles for the National Competent Authority (Urad vlade Republike Slovenije za informacijsko varnost (URSIV)), CSIRT teams (SI-CERT and SIGOV-CERT), and related bodies.

ZInfV-1 creates a **structured national information security system** with defined supervisory authorities, obligations for essential and important entities, and mechanisms for incident management. Some of the **key legal solutions in ZInfV-1** include:

- Broad entity coverage: Compared to previously valid Information Security Act (Zakon o informacijski varnosti (ZinfV)), ZInfV-1 broadens the scope of entities subject to the law. The law now extends to numerous entities based on specific criteria (minimum 50 employees and €10 million annual turnover/balance sheet), while certain categories like public electronic communications providers, trust service providers, and domain name registries are covered regardless of size.
- Formalized incident management: ZInfV-1 implements structured processes for incident notification, risk assessment, and coordinated response, including requirements for maintaining system logs and using certification schemes.
- Information sharing framework: It creates mechanisms for voluntary information exchange between obligated entities regarding cybersecurity threats, vulnerabilities, and defense techniques.
- Multi-layered cyber defense: The legislation establishes a comprehensive defense approach covering social, logical-technical, and physical dimensions of cyberspace, with provisions for both domestic and international cooperation.
- Enforcement mechanisms: The law creates an inspection regime with proportionate but significant penalties for noncompliance, designed to ensure effective implementation.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

New Critical Infrastructure Act (ZKI-1)

Transposing the EU Critical Entities Resilience Directive (CER) into Slovenian Law

The new **Critical Infrastructure Act** (Zakon o kritični infrastrukturi (ZKI-1)), which entered into force on **18 December 2024**, transposes the EU Directive 2022/2557 (the Critical Entities Resilience Directive (CER)) into Slovenian law. The CER Directive aims to **strengthen the resilience of critical infrastructure** across the European Union.

While the Digital Operational Resilience Act (DORA) focuses specifically on the digital resilience of the financial sector, the CER Directive covers a broader range of sectors and emphasizes overall resilience, including both physical and cyberthreats. Both legal frameworks stress the importance of risk management and continuity of essential services, but DORA is narrowly ICT-focused, whereas CER takes a holistic approach to the protection of critical infrastructure.

ZKI-1 regulates the field of critical infrastructure, which encompasses the **process of identifying and designating critical entities** and critical infrastructure in the Republic of Slovenia. It defines the procedure for identifying critical entities of special European significance, establishes the national framework for the resilience of critical entities and critical infrastructure, and sets out measures to ensure the resilience of critical entities in the provision of essential services. It also defines the powers and tasks of competent authorities and organizations, the national competent authority, and the single point of contact in the field of critical infrastructure, and establishes a framework for decision support, early warning, reporting, data protection, and oversight in the area of critical infrastructure.

By adopting ZKI-1, Slovenia has become one of the **first EU member states** to **transpose the CER Directive** into its national legislation, thereby reinforcing its commitment to a secure, resilient, and reliable critical infrastructure system.

Regulation on the Implementation of the EU Digital Operational Resilience Regulation for the Financial Sector

Transposing the EU Digital Operational Resilience Regulation (DORA) into Slovenian law

The **Regulation on the Implementation of the EU Digital Operational Resilience Regulation for the Financial Sector** (Uredba o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor (Regulation)) entered into force on **26 April 2025**, and transposes DORA into Slovenian law.

DORA, like NIS2, is a regulation aimed at enhancing cybersecurity and resilience, but with a specific focus on the **financial sector**. In relation to NIS2, DORA functions as a ***lex specialis***. DORA establishes rules for the financial sector intended to ensure resilience against both general and sector-specific cyberthreats. These rules cover risk management, reporting of cyber incidents, ICT system testing, and rules for cooperation with external ICT service providers.

The main objectives of the Regulation:

- It establishes the competent authorities responsible for implementing DORA and the authority responsible for conducting penetration testing in Republic of Slovenia;
- Regulates the manner of supervision and reporting of major ICT-related incidents and cyberthreats; and
- Sets out supervisory measures, offences, and fines related to the implementation of DORA in Slovenian law.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Biannual report on cyber incidents, 2025-1

Published in September 2025 by URSIV

URSIV has published its **biannual report on cybersecurity incidents** in September 2025 covering the first half of 2025. The document represents the final report under the previously valid Information ZinfV, with future reports to be prepared according to the new ZInfV-1 legislation that came into effect on 19 June 2025. URSIV functions as Slovenia's national authority for information security, working alongside SI-CERT (Slovenian Computer Emergency Response Team) and SIGOV-CERT (Slovenian Governmental Computer Emergency Response Team) to monitor and respond to cyber incidents across both public and private sectors.

In the **first half of 2025**, URSIV's national CSIRT centers (SIGOV-CERT and SI-CERT) handled **2,786 cybersecurity incidents** – an approximately 15% increase over the second half of 2024. SI-CERT addressed 1,951 incidents (a 24% rise) excluding 3,129 simple phishing cases, while SIGOV-CERT handled 835 incidents (up slightly from 830). Most incidents were low-severity and primarily involved online fraud (691), unauthorized account misuse (189), deceptive e-commerce (165), extortion (121) and unsolicited messages (98). The research-educational sector, government bodies and telecom operators were among the most affected. Reported direct financial losses dropped from €1,821,367 in second half of 2024 to €1,207,998 in first half of 2025, with "other fraud" accounting for €928,715, phishing messages €161,727 and resource misuse €51,018.

URSIV assessed the national cyberthreat level as "medium" same as it is at the EU level, noting ongoing trends in social-engineering fraud, DDoS (i.e., distributed denial of service) targeting electoral processes, supply-chain compromises and AI-driven deepfakes. Organizations are urged to enforce multi-factor authentication, regular software updates, SIEM-based event analysis, rigorous supply chain controls and compliance with DORA and NIS2 guidelines, leveraging SI-CERT's awareness campaigns and URSIV's cybersecurity handbook.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Adoption of legislation to implement the AI Act

In October 2025, the Slovenian National Assembly adopted a comprehensive national legislation implementing the EU AI Act (Regulation 2024/1689/EU).

The Slovenian implementation law (Zakon o implementaciji uredbe (EU) o določitvi harmonizacijskih pravil o umetni inteligenci (ZIUDHPUI)) establishes a regulatory architecture which includes distribution of regulatory responsibilities across specialized national authorities (i.e., these include ministries responsible for the economy, infrastructure, health, and digital transformation, the Public Agency for Medicines and Medical Devices, Slovenian Accreditation and supervisory bodies, The Agency for Communication Networks and Services (AKOS), the Information Commissioner, the Market Inspectorate, the Insurance Supervision Agency, and the Bank of Slovenia), each overseeing AI systems within their respective domains of expertise. **AKOS** serves as the central coordinating authority, facilitating coherent oversight across the regulatory landscape, and as the single point of contact. The law further defines a detailed and tiered sanctioning regime, in line with the national systemic misdemeanor legislation.

A distinguishing feature of Slovenia's approach is the establishment of an independent **National Ethics Council for Artificial Intelligence**. This five-member body, comprising experts from diverse disciplines including law, ethics, technical sciences, and social sciences, is tasked with providing ethical guidance on AI development and deployment, ensuring that technological advancement proceeds in alignment with fundamental societal values.

In the domain of public sector transparency, Slovenia has implemented particularly stringent requirements. Public authorities must publish comprehensive information about their AI systems through a unified information point, including algorithmic principles, impact assessments, and legal remedies available to citizens affected by AI-driven decisions.

The legislation defines responsibilities and a process for the creation of regulatory sandboxes and dedicated communication channels for small and medium enterprises and startups. This balanced approach with innovation support safeguards fundamental rights while fostering technological advancement within a clear regulatory framework.

Adoption of the New Media Act to regulate AI use in Media

On 4 September 2025, the Slovenian National Assembly adopted the new Media Act (Zakon o medijih (ZMed-1)), which entered into force on 18 September 2025.

In accordance with ZMed-1, any program content that has been created in whole or in part using Generative AI systems must be clearly identified and specifically separated from other program content in the media (first paragraph of Article 66 of ZMed-1).

Similarly, any program content that has been created in whole or in part using Generative AI systems must be marked with clear and systematic labels at the beginning and end of the program content (second paragraph of Article 66 of ZMed-1).

Broadcasters must inform users about how they use artificial intelligence systems, especially where the use of such systems may affect the use and understanding of program content, or when using AI systems that enable automated adaptation and creation of content tailored to different target groups (third paragraph of Article 66 of ZMed-1).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

There are no specific legislative developments envisaged in the field of personal data protection. The Slovene DPA will therefore continue to issue opinions and guidelines that are important for the interpretation of the provisions of the locally applicable data protection legislation.

In the coming years, the Slovene DPA is set to take on important role to ensure the level of protection achieved by the GDPR and ZVOP-2 is not lowered due to overlaps with new acts regulating artificial intelligence and digitalization.

Cybersecurity

The most relevant expected developments in cybersecurity in Slovenian law are closely linked to initiatives led by the Government Office for Information Security (URSIV), the national competent authority for information security, whose mission is to enhance resilience against cyberthreats affecting individuals, businesses, government bodies, and society at large. Key developments include:

- Development of a scalable awareness model for older adults in cybersecurity (VIAS-KV) – aimed at improving cybersecurity knowledge and practices among senior citizens;
- “Strengthening and Enhancing Cybersecurity” project – establishing an incident reporting platform and an ISAC platform, implementing a cybersecurity certification system, and developing educational materials for primary and secondary school curricula, as well as sample security documentation and measures for organizations of different sizes; and
- Strengthening the cybersecurity ecosystem in Slovenia (SECIS) – a European initiative to reinforce the National Coordination for Cybersecurity in Slovenia (NCC-SI), establishing it as a central hub for knowledge, capacity development, and collaboration in the field of cybersecurity.

Through these programs, URSIV will actively contribute to enhancing national cybersecurity awareness, resilience, and operational capabilities across multiple sectors.

AI

With the adoption of the implementation law, Slovenia ranks among the leading EU member states in the implementation of the EU AI Act. As of the date of preparation of this publication entry, the implementation law has not yet been published in the Official Gazette of the Republic of Slovenia, therefore, the date of entry into force is still unknown.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Spain

Contacts

Rodrigo González

Partner, Deloitte Legal Spain

rgonzalezruiz@deloitte.es

Carlos de Jorge

Senior Associate, Deloitte Legal Spain

cdejorge@deloitte.es

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Spanish Data Protection Board publishes Strategic Plan 2025-2030

Strategic plan: "Responsible innovation and defense of dignity in the digital era"

The Spanish Data Protection Agency (AEPD) approved its new strategic plan in 2025 after receiving 464 public contributions during the consultation phase. This plan marks a fundamental paradigm shift from a reactive-sanctioning model to a proactive, preventive, and support-oriented approach. Structured around eight guiding principles and seven major action axes, the plan sets the strategic foundation for AEPD's activities over the next five years and redefines both the philosophy and operational approach of the supervisory authority.

Core philosophy – A people-centered vision

The plan is built on the foundational principle that "behind every piece of data is a specific person whose rights and freedoms must be protected." This statement has profound practical implications: AEPD will require that any measure, from the most innovative to the most routine, be evaluated based on its real impact on citizens' lives, paying special attention to vulnerable groups such as minors and elderly people. The objective is to transcend purely legal language to foster a privacy culture based on knowledge and citizen empowerment.

Key strategic initiatives

"AI First" Policy and Privacy Laboratory:

- AEPD is developing in-house technical capacity and its own algorithms to audit complex algorithmic systems and proactively detect risk patterns in sensitive sectors (health, digital education, biometrics).
- This enables directing inspection resources in advance, before violations generate a flood of individual complaints, and sends a clear message to the market that the supervisory authority has the technical capacity to audit the most complex systems.
- Creation of Privacy Laboratory: Collaborative space with universities and research centers functioning as a regulatory sandbox where technology project promoters can simulate real scenarios and test their solutions before market launch.
- Represents a decisive transition from reactive enforcement to a preventive, collaborative approach that fosters privacy by design rather than purely punitive measures.

People-centered approach and proactive supervision:

- Data protection impact assessments (DPIAs) must evolve to incorporate not only GDPR risk analysis but also ethical considerations on social impact and fairness of processing systems.
- Enhanced accessibility in service channels, adapting guides and tools to diverse cognitive and digital needs.
- Intensified transparency requirements in automated decision-making technologies: AEPD will not only require that algorithms used by companies and public administrations be subject to effective human oversight but will also publish ethical principles and clear evaluation criteria for their assessment.
- Organizations must demonstrate proactive risk assessment and verifiable implementation of privacy by design and by default principles, especially for projects involving emerging technologies.
- It will no longer be sufficient to have a robust incident response protocol; demonstrating prevention capabilities becomes crucial.

International leadership and influence:

- Consolidation of AEPD's role as influential player on international stage through active participation in European Data Protection Board (EDPB) and Ibero-American Data Protection Network.
- AEPD not only absorbs best practices but also projects its own vision based on human dignity.
- Driving key European initiatives such as guidelines on age verification on internet.
- Positions Spain as key contributor in shaping global privacy standards.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

AEPD Report on Biometrics – Change of criteria

AEPD legal report of 18 July 2025 on the use of biometrics for access control

Represents one of the most significant changes of criteria of the year. Opens the door to biometric authentication for access control under extremely strict conditions, significantly raising technical and legal burden of proof requirements.

Mandatory conditions:

- **Absolute prohibition** of centralized storage of biometric templates: Templates must remain under exclusive control of the data subject (e.g., secure device in their possession).
- Compliance with National Security Scheme (ENS) at **high level** and conduct **periodic** data protection impact assessments (DPIAs).
- **Consent** recognized as **valid legal basis** for these processing operations.
- **Prohibition maintained**: Use of facial recognition for online exam surveillance, unless enabled by specific regulations.

New AEPD Guidelines published in 2025

Updated Video Surveillance Guide (February 2025)

- Replaces 2019 version with enhanced content aligned with GDPR principles. Addresses complex scenarios including drones, dashcams, and AI-powered systems. Emphasis on proactive accountability and demonstrating compliance. Maximum retention: 30 days with justified exceptions.

Joint Report AEPD-EDPS on Federated Learning (June 2025)

- Roadmap to harmonize AI innovation with GDPR in federated learning systems. Key recommendations include privacy by design, differential privacy, secure multiparty computation, and continuous audits.

Enforcement activity – First semester 2025

AEPD Activity Report: Key enforcement figures (1 December 2024 – 31 May 2025)

Analysis of enforcement resolutions reveals critical areas of noncompliance and priority sectors under special scrutiny.

Key statistics:

- **Collection**: €26.9M total (€31.3M in recognized rights).
- **Data breaches**: 1,211 notifications affecting approx. 54 million data subjects.
- **Most recurring infringements:**
  - Lack of valid legal basis for processing (Article 6 GDPR);
  - Insufficient security measures (Article 32 GDPR); and
  - Failure to inform data subjects (Article 13-14 GDPR).
- **High-risk sectors:**
  - Video surveillance, financial entities, healthcare/pharmacies, public administrations.
- **Notable sanctions:**
  - Insurance company and bank: €5 million;
  - Telecommunications operator: €1.2 million;
  - Sports organization: €1 million; and
  - Occupational health insurer: €1 million.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Royal Decree 255/2025 – Digital ID card

Royal Decree 255/2025 regulating the national identity document

Approved 1 April 2025, this decree formally establishes the digital version of the ID card with full legal effectiveness equivalent to the physical document, and modernizes the citizen identification system, adapting it to European regulatory framework (Regulation EU 2019/1157).

Key data protection aspects:

- The Ministry of Interior (Directorate General of Police) acts as data controller for both physical and digital ID data. The MiDNI application virtualizes the ID on mobile devices through secure real-time communication with national police systems, implementing data minimization by design as it does not permanently store information on the device. Notably, the system provides granular control allowing holders to decide which specific data to display in each verification process.
- The decree mandates secure storage of biometric data (facial image and fingerprints) with qualified electronic certificates for advanced electronic signatures, ensuring compliance with GDPR Article 32 security requirements and Article 9 special categories provisions.
- Organizations face a 12-month adaptation period to accept digital ID as valid identification. However, the creation of this centralized identification infrastructure multiplies integration points and potential vulnerabilities. Entities implementing digital ID verification must conduct specific risk analyses under GDPR Article 35, evaluating not only their own integration security but also inherent risks of interaction with users' mobile devices.

Organic Law 1/2025 – Justice system digitalization

Organic Law 1/2025 on measures regarding efficiency of the Public Justice Service

Published 3 January 2025. While not a data protection law per se, it has indirect but substantial impact by driving deep digitalization of judicial proceedings.

GDPR implications:

- This law necessarily creates new personal data processing flows, including special categories of data under GDPR Article 9 (criminal offences, legal proceedings). Judicial bodies and legal professionals must strengthen technical and organizational security measures to ensure compliance with GDPR Articles 5 (principles), 24 (controller responsibility), and 32 (security of processing) in digitalized judicial environments. Critical focus on guaranteeing confidentiality, integrity, and availability of procedural information throughout the digital transformation of justice administration.

Key case law 2025

National Court Judgment SAN 706/2025 – Right of access to blocked data

Establishes that the data subject's right of access extends even to blocked data. Blocking (retention to address potential legal responsibilities) does not equal deletion; therefore, the individual retains the right to know what information is being retained under this regime, reinforcing transparency principle.

Supreme Court – Consolidation of doctrine (STS 4096/2025, STS 3256/2025)

Rulings on lawfulness of processing, burden of proof in communications, and right to be forgotten. Reinforces case law in line with Constitutional Court doctrine (e.g., STC 58/2018), providing legal certainty in GDPR interpretation within Spanish legal system.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Spanish NIS2 transposition – Cybersecurity Coordination and Governance Law

Draft Law on Cybersecurity Coordination and Governance

Spain missed the 17 October 2024, EU transposition deadline, triggering an infringement procedure by the European Commission. The draft law was approved by the Council of Ministers on 14 January 2025, notified to the EU on 21 February 2025, and is expected to be definitively approved and enter into force throughout 2025.

Spanish-specific extensions:

- Notably, the Spanish draft law adds the **insurance industry** and **private security companies** to the list of critical sectors, demonstrating a risk assessment adapted to the national context and representing a unique expansion beyond the EU directive's minimum requirements.

Governance and enforcement structure:

- National Cybersecurity Center:
  - Created as the single national competent authority with broad powers to ensure compliance. This center will coordinate all control authorities and national CSIRTs (CCN-CERT, INCIBE-CERT, ESPDEF-CERT), creating a unified oversight framework. The center is empowered to conduct inspections and audits of covered entities, and critically, to impose significant sanctions for noncompliance, establishing a robust enforcement mechanism.
  - The center is empowered to conduct inspections of covered entities, and critically, to impose significant sanctions for noncompliance, establishing an enforcement mechanism. This centralized structure represents a shift from the previous fragmented approach, enabling more effective supervision and coordination.

- Information Security Officer (RSI) – A new mandatory role:
  - One of the most disruptive innovations of the draft law is the mandatory designation of an "information security officer" (Responsable de Seguridad de la Información (RSI)). This figure, which can be an individual or a collegiate body, represents a fundamental shift in how organizations must structure their cybersecurity governance.
  - The RSI must meet rigorous requirements:
    - **Specific training and demonstrated technical capacity** in cybersecurity and information security management;
    - **Sufficient level of authority and independence** within the organization to effectively perform their functions without undue interference;
    - **For essential entities:** Additional requirement of **accreditation by the Ministry of Interior**, establishing a formal qualification standard.
  - This mandatory role elevates cybersecurity from a purely technical function to a formal governance position with clear accountability. The RSI serves as the designated point of contact with supervisory authorities and is responsible for overseeing the implementation and maintenance of all cybersecurity measures required by the law.

- Board-level responsibility – The end of plausible deniability:
  - Governing bodies (boards of directors or equivalents) are responsible for approving and supervising implementation of cybersecurity risk management measures and assume **direct personal responsibility in case of noncompliance**. Establishes that **members of management bodies shall be jointly and severally liable for the infringements committed by their entities**. This means that individual board members can be held personally accountable.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Spanish CER transposition – Critical Entities Protection and Resilience Law

Draft Law on Protection and Resilience of Critical Entities

Spain missed the 17 October 2024, EU transposition deadline for Directive (EU) 2022/2557 on the resilience of critical entities. The draft law was approved by the Council of Ministers on 27 May 2025, and will be processed under urgent procedure to expedite transposition. This legislation focuses on **physical protection** of critical entities, complementing the NIS2 cybersecurity framework.

Difference from NIS2 – Designation process

Unlike NIS2 where entities self-designate based on size and sector criteria, under the CER Law **critical entities must be formally designated by the Ministry of Interior**. This represents a more centralized and controlled identification process, where the State Secretariat for Security, through CNPREC, conducts the evaluation and official designation based on criticality criteria including number of affected users, interdependencies with other sectors, market share, geographical area of influence, and importance for maintaining essential services.

Core obligations and measures:

- **Incident notification:** Critical entities must notify the National Center for Protection and Resilience of Critical Entities (CNPREC) of incidents that disrupt or may significantly disrupt the provision of essential services within **maximum 24 hours** from awareness (unless operationally unable). Subsequently, a detailed incident report must be submitted within one month maximum;
- **Security Officer designation:** Critical entities must designate a security officer responsible for implementing and maintaining resilience measures. This officer **must hold a Security Director qualification issued by the Ministry of Interior**.

Institutional framework – New governance structure:

- **National Center for Protection and Resilience of Critical Entities (CNPREC):**

  Creates the CNPREC, dependent on the State Secretariat for Security, which will replace the current National Center for Critical Infrastructure Protection (CNPIC). CNPREC will serve as:

  - Direct interlocutor with all critical entities;
  - Single point of contact for cross-border cooperation with EU member states;
  - Responsible for managing the National Platform for incident notification; and
  - Authority responsible for formal designation of critical entities.
- **National Commission for Protection and Resilience of Critical Entities:** Collegiate body responsible for approving sectoral strategic plans, collaborating in the identification of critical entities, and coordinating between different sectors and government levels. This interinstitutional approach strengthens cooperation between public and private sectors, recognizing that critical infrastructure protection requires joint and coordinated efforts.
- **Complementarity with NIS2:** The CER Law focuses on **physical resilience** while NIS2 addresses **cyber resilience**, creating a comprehensive dual framework for critical entity protection. Organizations falling under both regulations must ensure coordinated implementation of cybersecurity and physical security measures, with both requiring 24-hour incident notification, risk management frameworks, and board-level oversight.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Order PJC/522/2025 – New National Cybersecurity Strategy

Order initiating the procedure for developing Spain's new National Cybersecurity Strategy

Published on 26 May 2025, this order from the National Security Council officially launches the process to develop a new National Cybersecurity Strategy. This is not merely a policy update exercise, but a strategic realignment designed to respond to the current threat landscape, which the 2021 National Security Strategy already identified as one of the country's main risks

The process is led by the National Security Council, which delegates the drafting to its specialized committee, the National Cybersecurity Council. The development follows a structured, multi-phase collaborative approach:

- **Technical working group**: Composed of representatives from various ministerial departments and agencies, responsible for drafting initial versions of the strategy.
- **Expert input**: The Department of National Security will gather contributions from independent experts from civil society, private sector, and academia, demonstrating explicit commitment to a multi-stakeholder approach.
- **Regional coordination**: Draft will be sent to the Sectoral Conference for National Security Affairs, ensuring participation and alignment of autonomous communities and cities in the national strategy.
- **Final approval**: Final draft will be presented by the technical working group to the National Cybersecurity Council, then elevated to the National Security Council for final approval

This strategy provides the conceptual framework and objectives (the why) that give meaning to the legal mechanisms established by NIS2 and CER (the how). It represents Spain's comprehensive vision for national cyber defense, moving beyond reactive compliance toward proactive, coordinated national resilience. The strategy will formally establish cybersecurity as a shared national responsibility, creating the policy foundation that justifies and guides the mandatory cooperation and information sharing requirements embedded in the legislation.

ES-ISAC Health – Collaborative Defense Model

In October 2025, a key initiative for Spanish healthcare cybersecurity materialized: the launch of ES-ISAC Health. This national-level Information Sharing and Analysis Center (ISAC) is a public-private collaboration initiative to strengthen cybersecurity and cyber resilience of the national health system as a whole.

ES-ISAC Health unites forces between:

- **INCIBE (National Cybersecurity Institute)**: Acts as competent authority and facilitator, providing technical infrastructure and coordination; and
- **Private sector associations**: Farmaindustria (pharmaceutical industry), IDIS Foundation (private healthcare), ASPE (health equipment and technology), and FENIN (medical technology companies).

This creates a trusted forum where different healthcare sector actors can securely share, analyze, and exchange cyber intelligence in a structured manner.

The ISAC functions as a trusted environment for sharing threats and vulnerabilities specific to healthcare, indicators of compromise (IoCs), adversary tactics and techniques, security recommendations, and real-time threat intelligence. By aggregating and anonymizing threat data from multiple healthcare organizations, ES-ISAC Health enables collective defense more effective than individual organizational efforts.

ES-ISAC Health should be viewed as a **pilot project and template for future sector-specific ISACs**. Given the success model combining INCIBE's technical capacity with private sector knowledge, this collaborative framework will likely be replicated in other high-criticality sectors such as energy and transport. INCIBE's central role positions it as the natural facilitator for creating future ISACs, converting them into the operational mechanism to fulfill information sharing objectives mandated by NIS2. What begins as voluntary collaboration in 2025 may evolve into mandatory participation for critical entities in their respective sector ISACs.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Spanish AI Act – Draft Law on adequate use and governance of AI

Draft Law for the good use and governance of artificial intelligence (Approved March 2025)

The main legislative vehicle for adapting Spanish law to the EU AI Regulation is the Draft Law for the good use and governance of artificial intelligence, approved by the Spanish government in March 2025. This text goes beyond direct transposition, establishing the applicable sanctioning regime and defining the national governance architecture, anticipating certain aspects to provide greater legal certainty to the Spanish technological ecosystem.

The future law has broad scope affecting the entire value chain: providers introducing AI systems into the Spanish market, deployers (companies and public administrations) using them in their processes, as well as importers and distributors.

- One of the most notable innovations is the obligation to guarantee traceability of AI-generated content, an anticipated and reinforced application of the AI Act's transparency requirements. This measure responds to growing concerns about disinformation and algorithmic manipulation, establishing clear legal obligation for developers, platforms, and media. Emphasis in this area is evidenced by designation of bodies like the Central Electoral Board to supervise systems that could interfere with democratic processes, suggesting Spanish legislator is focused on AI risks to public debate and electoral integrity.
- Spain seeks to position itself at the forefront of digital rights with introduction of a "right to disconnection or market withdrawal" for AI systems that have caused serious incidents. This right, novel in the European Union, would allow competent authorities to prohibit or restrict commercialization of a system following a complaint, anticipating the right to claim that the AI Act contemplates generally from 2026. This proactive action, analogous to Spain's contribution in recognizing the "right to be forgotten," demonstrates a political strategy to influence development of digital rights in Europe beyond mere regulatory compliance.

Spanish AI Supervisory Authority (AESIA)

- Spain anticipated the European obligation to designate a national supervisory authority with creation of the Spanish Agency for AI Supervision (AESIA), the first body of its kind in Europe. Based in A Coruña, AESIA began in-person operations in February 2025, marking the beginning of active AI supervision in the country.
- Throughout 2025, AESIA has been immersed in consolidation process, aiming to reach staff of approximately 30 professionals in its first year. Its organizational chart is structured into specialized subdirectorates in areas such as reports and infrastructures, and certification, evaluation and training.
- AESIA's competencies are broad, encompassing market supervision of the AI Act and sanctioning powers, to advisory, training, and innovation promotion functions through initiatives like testing environments (sandboxes). It acts as Spain's notifying authority and single point of contact with the European AI Office, centralizing communication and coordination at EU level.

Dual supervision model – AESIA and AEPD

The Spanish supervisory framework is configured as a "dual oversight" model, where AESIA and the Spanish Data Protection Agency (AEPD) share responsibilities from complementary angles:

- **AESIA**: Supervises the AI system as a "product" or "service" introduced to market. Focus on product safety, compliance with technical requirements, risk management, robustness, and documentation under AI Regulation.
- **AEPD**: Supervises "processing" of personal data performed by AI system. Focus on protection of fundamental rights and freedoms, lawfulness of processing, data minimization, data subjects' rights under GDPR. AEPD maintains intact competence to supervise and sanction any personal data processing by AI systems that violates GDPR, even before full AI Act application.

This dual structure, while logically founded on respective competencies, generates notable complexity for companies potentially facing inspections from both agencies on same AI system. Success depends on formalization of efficient collaboration protocols still under development throughout 2025. Additional sectoral regulators may intervene (CNMC for digital platforms, Bank of Spain for credit scoring, Central Electoral Board for electoral processes).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

First EU Regulatory Sandbox – Operational April 2025

The most prominent initiative is the AI regulatory testing environment (Sandbox), the **first in the European Union**, launched by the Spanish government in late 2024 and activated in April 2025. This controlled space allows select group of companies to test their high-risk AI systems under direct supervision of authorities (including AESIA), receiving personalized guidance to align products with AI Act requirements before they become fully enforceable.

12 selected pilot projects (April 2025)

The Spanish government selected 12 companies and their respective AI systems from 44 applications, covering wide range of high-risk sectors:

- **Access to essential services**: Creditworthiness assessment (Dedomena AI), emergency 112 transcription (CITIC Foundation);
- **Biometrics**: Age verification (Veridas), facial recognition surveillance (Herta Security);
- **Employment**: CV job matching (InfoJobs), freelance-project matching (Shakers);
- **Critical infrastructure**: Transport safety monitoring (Imotion Analytics), electrical grid cybersecurity (Loradix RED);
- **Machinery**: Language model assistant for operators (Airbus);
- **Medical devices**: Sleep treatment platform (Bit&Brain), automated patient follow-up (Tucuvi Care); and
- **In vitro diagnostics**: Metabolic disease prevention (Made of Genes).

Participation does not exempt from legal compliance but offers direct dialogue channel with regulator and opportunity to influence technical guidance development serving as reference for entire Spanish and European ecosystem.

Regional AI initiatives – The autonomous communities mosaic

Galicia – Europe's first regional AI law. Law 2/2025, of 2 April for the development and promotion of artificial intelligence in Galicia

This is the **first regional regulation in Spain and Europe** dedicated entirely to AI, its main objective is to regulate the design, acquisition, and use of AI in the Galician regional administration and its public sector, promoting human-centric, safe, and reliable AI. The law:

- Establishes obligations for Galician public sector: impact assessments requirement, transparency guarantees, human oversight, and mitigation of discriminatory bias;
- Has a particular emphasis on promoting use of Galician language in AI systems, addressing linguistic diversity concerns often overlooked in broader AI regulation;
- Fosters public-private collaboration through innovation public procurement;
- Although application scope focuses on Galician administration, it seeks to serve as reference and attract investments to the region's technological ecosystem; and
- Acts as a pioneering model that other regions may follow.

Basque country – Grant programs and NextGenerationEU funding

- Through agency SPRI, the Basque government launched the program "Applied Artificial Intelligence and Data Strategy 2024-2025," funded with NextGenerationEU funds.
- Recent diagnosis by BAIC (Basque Artificial Intelligence Center) reveals only 12% of regional agents are currently aligned with European regulation, indicating significant journey ahead for regulatory adaptation.

Community of Madrid - AI use cases subsidies

The Ministry of Digitalization approved subsidy call for "artificial intelligence use cases" aimed at SMEs with tax domicile or activity in the region.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Expected legislative developments in Spain 2025-2026

Spain faces a critical 18-month period where several major legislative initiatives will move from draft to final approval and implementation, fundamentally reshaping the compliance landscape for Spanish organizations across all critical sectors.

Major legislative approvals expected:

- **Definitive approval of Spanish NIS2 Law** (Cybersecurity Coordination and Governance Law): Expected late 2025/early 2026 following urgent parliamentary procedure initiated January 2025.
- **Definitive approval of Spanish CER Law** (Protection and Resilience of Critical Entities Law): Expected late 2025/early 2026 following urgent procedure initiated May 2025.
- **Approval of Spanish AI Law** (Good Use and Governance of Artificial Intelligence): Transposition of draft approved March 2025, final approval expected throughout 2025-2026.
- **Publication of New National Cybersecurity Strategy:** Process formally initiated May 2025 (Order PJC/522/2025), publication expected throughout 2026 after multi-stakeholder consultation.

Regulatory development and implementation:

- **Implementing regulations**: Development of secondary regulations specifying concrete **first official designations.** CNPREC (National Center for Protection and Resilience of Critical Entities) conducting evaluations and officially designating critical entities under CER framework – unlike NIS2's self-designation, CER requires formal government designation.
- **RSI accreditation process**: Ministry of Interior establishing and implementing accreditation system for information security officers (RSI) required for essential entities under NIS2.
- **Critical entity catalogues**: Publication of National Catalogue of Critical Entities identifying which specific organizations fall under CER.

Expected enforcement and operational developments 2025-2026

As legislative frameworks are approved, Spain will rapidly transition from policy development to active enforcement and operational implementation, reshaping the cybersecurity, AI governance, and data protection landscape.

Enforcement and supervision milestones:

- **First enforcement actions under NIS2**: Initial inspections and sanctions expected throughout 2026.
- **AESIA's first supervisory actions**: Spanish AI Authority beginning active market surveillance and sanctions under AI Act, focusing on high-risk systems and prohibited practices.
- **AEPD intensified AI supervision**: Data Protection Agency escalating enforcement against AI systems violating GDPR, including prohibited practices under AI Act involving unlawful personal data processing.
- **First board-level sanctions**: Landmark cases testing joint and several liability of board members under NIS2, establishing precedent for personal accountability of executives.

Data protection – AI intersection developments:

- First coordinated actions where same AI system faces sanctions from both agencies – AESIA for AI Act violations (inadequate risk management, missing documentation) and AEPD for GDPR violations (unlawful processing, lack of legal basis).
- AEPD enforcement following CJEU April 2025 ruling requiring meaningful explanations of algorithmic logic in credit scoring, employment, and insurance.
- Following July 2025 AEPD criteria change, expected wave of inspections against organizations using centralized biometric storage or lacking proper safeguards.
- Publication of coordinated guidelines on conducting DPIAs for high-risk AI systems and AI-data protection intersection.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Sweden

Contacts

Michelle Smed

Manager, Deloitte Legal Sweden

msmed@deloitte.se

Julia Bergman

Consultant, Deloitte Legal Sweden

julbergman@deloitte.se

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The Swedish Authority for Privacy Protection issues decisions on cookie banners

The Swedish Authority for Privacy Protection (IMY) has investigated the use of cookie banners by three companies following complaints regarding their methods of obtaining user consent. All three companies have received reprimands for inadequate cookie banner practices.

The first company was criticized for failing to provide sufficient information on how users can withdraw their consent and for not clearly communicating the rights under the General Data Protection Regulation (GDPR). IMY emphasized that withdrawing consent must be as easy as giving it, and that this right and ease of withdrawal must be available at the time consent is obtained. Although visitors could manage their preferences, the process to withdraw consent was deemed insufficiently accessible.

The second company was criticized for employing misleading design in its cookie banners. The “accept all cookies” option was presented as a prominent green button, while the “choose your cookies” option appeared as a less visible gray-black link. The IMY concluded that the design of the cookie banner reinforced the impression that users should click the green button to accept cookies, thereby undermining the ability to provide informed and voluntary consent.

The third company was criticized for processing personal data without a lawful basis. While the company cited legitimate interest as the legal basis, it failed to provide adequate justification.

These findings confirm that misleading cookie banners with unclear information or barriers to withdrawing could violate the GDPR.

New video surveillance legislation

As of 1 April 2025, a new legislation regarding video surveillance entered into force. The new legislation removes the obligation to obtain a permit from the Swedish Authority for Privacy Protection (IMY); consequently, public entities wishing to conduct video surveillance no longer need to seek such approval. Instead, the new legislation underscores the importance of documenting the legal basis used for the video surveillance, including the documented legitimate interest assessment, as part of the accountability principle under the GDPR. The amendment aims to streamline and expedite the process for implementing video surveillance.

This change does not affect the balance between the interest in surveillance and the right to privacy. However, the responsibility for assessing this balance has shifted from the supervisory authority during the permit application process to the organization itself.

For cases where a permit for video surveillance was previously granted, such permits are now obsolete. Instead, the organization performing the surveillance must evaluate, prior to commencing video surveillance, whether the interest in surveillance outweighs the interest in privacy. Should circumstances change, a new assessment must be conducted. Additionally, the data controller is required to maintain a register of ongoing surveillance activities. IMY retains its supervisory responsibilities while also taking on an enhanced role in offering guidance regarding specific locations and certain types of video surveillance.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Access to criminal records and GDPR: Swedish Supreme Court guidance on personal data confidentiality

In early 2025, the Supreme Court of Sweden issued two rulings concerning the relationship between Swedish constitutional protection and the GDPR. The decisions establish that the GDPR is relevant when determining whether personal data contained in criminal judgements should be subject to confidentiality, even within the constitutionally protected domain.

The first case concerned a news agency that had requested a large number of judgements and other documents in criminal cases from a Court of Appeal. The Court of Appeal disclosed the documents subject to confidentiality under the Public Access to Information and Secrecy law, which forms part of Swedish constitutional law, limiting the news agency's ability to further disclose or utilize the information. In its reasoning, the Court of Appeal referred to the GDPR and case law from the CJEU. Such conditional disclosure is standard practice in Sweden, allowing authorities to balance public access to official documents with the protection of personal data and other legitimate interests. The Supreme Court only amended the Court of Appeal's decision by adjusting the confidentiality provisions to enable the news agency to continue its journalistic activities to a greater extent, including by publishing editorially processed news content. The second case involved a company that provides information for background checks but also engages in journalistic activities to some extent. The outcome was the same in that case.

The Supreme Court's rulings create obstacles for companies with publishing licenses to obtain criminal judgements for the purpose of providing information from them for background checks.

The Swedish Authority for Privacy Protection provides comprehensive guidance on data protection impact assessments

The Swedish Authority for Privacy Protection (IMY) has continued to provide guidance on data protection impact assessments (DPIAs), which must be conducted in accordance with Article 35 of the GDPR. The primary purpose of this guidance is to assist organizations in navigating the DPIA process and to reduce uncertainty surrounding regulatory compliance. The guidance is specifically designed for organizations that process personal data and require support in preparing such assessments.

IMY outlines a 10-step process for conducting a DPIA, with each step thoroughly explained. To facilitate implementation, IMY has developed templates and Excel spreadsheets to assist at every stage of this process. Legal interpretative guidance is provided to help entities gain a deeper understanding of the regulatory requirements and implications.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Sweden’s implementation of the NIS2 Directive through a new cybersecurity law

On 14 October 2025, a proposal was announced for a new Swedish cybersecurity law to implement the NIS2 Directive. The new legislation is expected to come into effect on 15 January 2026, replacing the current cybersecurity law. Compared to the existing framework, the new law will encompass a broader range of sectors, thereby affecting a greater number of operators in both private and public sectors. In line with the NIS2 Directive, the proposal stipulates that medium-sized entities will fall within the scope of the law. Additionally, entities may still be subject to the law if they are the sole supplier in Sweden.

The new legislation emphasizes that the primary objective of the new legislation is to achieve a high level of cybersecurity. Generally, the entire operations of an organization will be covered by the law, not only the areas providing essential or digital services. Both public and private operators within the designated sectors will be required to implement measures to protect their network and information systems, as well as to report significant incidents. The new law affects a total of 18 sectors, consistent with the directive’s distinction between sectors of high criticality and other critical sectors, including government authorities, with the exception of judicial courts.

The new legislation imposes several obligations on operators, who will be required to register with the relevant supervisory and implement security measures for network and information systems that are both appropriate and proportionate to the risks posed.

Overall, the new cybersecurity law introduces a significantly more comprehensive and stringent regulatory framework for cybersecurity in Sweden, featuring a broader scope of application, clearer requirements for security measures, and more robust sanctioning powers than the previous legislation.

Sweden's National Cybersecurity Strategy for 2025-2029

Sweden's National Cybersecurity Strategy for 2025-2029 was published 20 March 2025. It sets out the Swedish government's comprehensive approach to cybersecurity. The strategy has been developed to address national needs whilst also aligning with the NIS2 Directive.

The document begins by outlining various threats and vulnerabilities that currently affect Sweden's cybersecurity landscape. To address these challenges, the strategy is organized around three fundamental pillars that provide direction for Sweden's cybersecurity efforts. Pillar A focuses on establishing systematic and effective cybersecurity work across relevant sectors and organizations. Pillar B emphasizes the development of enhanced knowledge and skills in cybersecurity, recognizing that human expertise is crucial to maintaining robust defenses. Pillar C concentrates on building the capability to both prevent cybersecurity incidents before they occur and manage them effectively when they do happen.

Beyond these three pillars, the strategy establishes specific goals designed to achieve measurable progress during the five-year period and directly respond to the threats and vulnerabilities identified in the analysis. These goals aim to create tangible improvements in Sweden's overall cybersecurity posture and resilience. An important component of the strategy is the accompanying action plan, which contains concrete activities that correspond to the government's strategic direction and fulfil the requirements set out in the NIS2 Directive. This action plan is not static but will be updated on an ongoing basis to ensure it remains relevant and responsive to the evolving cybersecurity landscape.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Sweden's strategic framework for implementing the AI Act

In early October 2025, the government announced Sweden's intended approach to implementing the AI Act. The proposal aims to designate national competent authorities in accordance with the AI regulation, outline the necessary measures to ensure enforcement and sanctions in the event of breaches, and assess the prerequisites for establishing one or more regulatory sandboxes for AI. Additionally, it seeks to recommend the extent of Sweden's participation in the AI regulation's proposed implementation support and innovation-promoting initiatives. The Swedish government will also present legislative proposals and other necessary measures required to fulfil the obligations set out in the AI Act.

The report proposes consolidating the Swedish provisions needed to complement the AI Act into a new act and a new ordinance. It further recommends that terms and expressions used in this new complementary legislation carry the same meaning as those in the AI Act. Moreover, a system comprising eleven supervisory authorities and two notifying authorities will be established to collectively support market surveillance, market control, governance, and compliance monitoring. The legislator also proposes granting these authorities the power to impose sanctions and fines. Furthermore, the proposal suggests that Swedish authorities themselves may be subject to sanctions.

Sweden intends to maintains the minimum requirements and does not extend the implementation of the EU rules beyond what is mandated by the AI Act. The legislation is expected to come into force on 2 August 2026, the date by which EU member states are required to apply all provisions of the AI Act.

National guidelines for Generative AI in public sector

The Swedish Authority for Privacy Protection (IMY), in collaboration with the Swedish Agency for Digital Government (Digg), has issued national guidelines concerning the use of Generative AI within the public sector. These guidelines aim to assist regions, authorities, and municipalities in ensuring the responsible and informed use of Generative AI, while clarifying how it should be employed to fulfil operational needs. In total, the guidelines comprise 18 recommendations across seven key areas.

Although developed specifically for the public sector, these guidelines are equally applicable to other types of organizations. They include recommendations to establish an AI policy, procure Generative AI in compliance with public procurement law, and ensure that the use of Generative AI adheres to data protection regulations. This includes clarifying accountability for AI usage and outlining how associated risks should be managed.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Expansion of the Swedish Authority for Privacy Protection's regulatory sandbox program

The Swedish Authority for Privacy Protection (IMY) is significantly expanding its regulatory sandbox initiative to support innovation projects navigating complex GDPR compliance issues. Following a significant government budget allocation until 2028, IMY will be able to provide in-depth guidance to a greater number of projects than in previous years.

The regulatory sandbox focuses on projects involving new technologies, particularly AI, or novel applications of existing technologies. This expansion reflects the growing need for data protection guidance as digitalization accelerates across Swedish society. Current projects in the sandbox include exploring AI-assisted recording and transcription of social services conversations in a Swedish municipality and developing privacy-secure methods for sharing traffic data to enhance road safety.

The initiative demonstrates Sweden's proactive approach to balancing innovation with robust data protection, providing organizations with expert support to ensure that technological advancement and GDPR compliance can be achieved simultaneously. The next intake opens in March 2026.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Switzerland

Contacts

Paul de Blasi

Partner, Deloitte Legal Switzerland

pdeblasi@deloitte.ch

Elisabeth Everson

Manager, Deloitte Legal Switzerland

eeverson@deloitte.ch

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Guidelines on reporting data security breaches and informing data subjects

Under the Federal Act on Data Protection (FADP), the controller shall notify the Federal Data Protection and Information Commissioner (FDPIC) of any breach of data security that is likely to result in a high risk to the data subject's personality or fundamental rights as quickly as possible. In certain situations, the controller must also notify the data subject affected by the breach.

These guidelines, first published in February 2025, provide practical insights on both the reporting to the FDPIC and the notification to the data subject, addressing topics such as the contents of the report, the interpretation of "high risk" within the meaning of the relevant provision, and an overview of the possible sanctions.

The publication is available here.

Factsheet on forms provided to patients during consultations

The factsheet addresses, in substance, three issues: the essential distinction in terms of data protection between requirements relating to the duty to provide information and those relating to consent, secure data communication, and the principle of proportionality.

You can read the document here.

Guidelines on data processing using cookies and similar technologies

In Switzerland, the use of cookies in applications and on websites is governed by the Telecommunications Act (TCA) as well as the FADP. These guidelines cover the provisions of the FADP, including their regulatory relationship to the special provision of Article 45(c) TCA, which aims to protect the privacy and informational self-determination of users and constitutes a special public-law standard for otherwise unnoticed 'telecommunications' processes.

The FDPIC's cookies guidelines, first published in January 2025 and amended in October of the same year, cover topics such as responsibility, general information obligations, permissibility of non-essential cookies, duty to provide for an active opt-in and an ongoing revocation banner, or overriding private interests.

The full document can be found here.

Factsheet on forms relating to apartment leasing requests

The collection and processing of data by the lessor or a real-estate agent regarding potential lessees is in principle authorized, insofar as the data collected is relevant for choosing (by using objective criteria) a suitable lessee.

The factsheet provides information on various topics, including consent, overriding private interest, and different data protection principles in the specific context of a lessee-lessor relationship. Additionally, the document contains guidance on the personal data that can be requested in this context.

The document is not available in English at the time of writing; you can however access it in German, French and Italian.

The FDPIC signs the first Memorandum of Understanding (MoU) with a foreign supervisory authority

On 18 September 2025, Switzerland and the United Kingdom signed a MoU to strengthen cooperation between their national data protection authorities, aimed at facilitating the exchange of experiences, best practices, and collaboration.

More information, including a link to the MoU, is available here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The Federal Council wishes to strengthen the rights of users in the digital space via a new law on communication platforms and search engines

The Federal Council aims to enhance user rights in the digital space by introducing a new law targeting very large online platforms and search engines such as Facebook, X, TikTok, and Google. This legislation seeks to establish clear rules to ensure fairness and transparency, including requirements for platforms to provide easy reporting mechanisms for unlawful content, explain content removals or account blocks, and implement internal complaints and dispute resolution processes. It also mandates transparency in advertising and recommendation systems, public advertising archives, and access for authorities and researchers to platform data. Stakeholders are invited to provide feedback by 16 February 2026.

The press release is available here.

FDPIC 2024/2025 Annual Report

The Office of the FDPIC has expanded its resources by around 30% to address data protection violations under the FADP, which came into force on 1 September 2023. It has clarified its enforcement approach through initial supervisory proceedings, some of which are now subject to judicial review by higher courts. Challenges have also arisen regarding procedural aspects, such as public disclosure of supervisory actions and fee determinations.

Public demand for administrative transparency remains high, with a nearly 30% increase in access requests to federal authorities. Despite a 53% rise in mediation requests causing processing delays, the FDPIC successfully resolved 76% of mediations through mutual agreement. The office has also criticized federal authorities' attempts to limit transparency in administrative processes.

The press release and the link to download the report can be found respectively here and here.

New FDPIC rulings

Under Article 49 FADP, if the FDPIC identifies violations of data protection provisions during an investigation, they can impose administrative measures according to Article 51 FADP. Per Article 57(2) FADP, the FDPIC must publicly disclose findings and rulings in cases of general interest. The data controller can separately challenge both the measure and its public disclosure before the Federal Administrative Court. The published rulings include only those cases where publication was uncontested or upheld by a final court decision.

In the course of 2025, two new rulings (available in German only) have been added to the FDPIC's database, which can be found here, and concern (i) the legal deadlines for processing data subject requests and the communication of the processed data as such, and (ii) the disclosure of personal data on the internet.

The FDPIC files a criminal complaint against Add Conti GmbH

Following complaints about Add Conti GmbH's marketing practices, the FDPIC launched an investigation on 4 June 2025 and formally requested the company's cooperation, which was ignored despite reminders and a grace period. The company is accused of collecting personal data of individuals in Germany without their consent and sharing it with German firms for advertising, while failing to respond to information and deletion requests. On 14 August 2025, the FDPIC filed a criminal complaint for breach of cooperation obligations.

The official communication is available here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Various new freedom of information recommendations and judgments

Under the Freedom of Information Act, which regulates the principle of public access to administrative activities (i.e., the principle of freedom of information), anyone is entitled to access official documents without having to substantiate the reason for the request. The rationale is to promote transparency and comprehensibility of administrative activities. If applicants or consulted third parties disagree with how an authority handles an access request, they can ask the FDPIC to mediate.

If the parties cannot reach an agreement, the FDPIC will issue a written recommendation, published in a database available here.

Further to the freedom of information procedure described above, following a recommendation by the FDPIC, the relevant authority may issue a ruling which can then be appealed.

In 2025, various new judgments of the Federal Administrative and the Federal Court have been published in this context. They can be found respectively here and here.

The Federal Administrative Court confirms the practice of the FDPIC

The Bürgerforum Schweiz association conducted a "Pfarrer-Check" (Priest Check) online campaign, collecting contact details of priests and church workers to send them a questionnaire aimed at assessing their religious views. The association maintained an online database tracking who received and responded to the questionnaire but refused to delete data of individuals who requested removal, despite being included without consent. The FDPIC found that the association violated the principle of proportionality by publishing data on individuals who were merely registered or contacted, as this information was neither reliable for determining religious beliefs nor necessary to show survey representativeness.

On 9 April 2024, the FDPIC prohibited the association from processing the data. Bürgerforum Schweiz appealed, but the Federal Administrative Court dismissed the appeal on 6 October 2025.

The official communication as well as the links to the FDPIC's ruling and the decision of the court can be found here.

The EU Entry/Exit-System (EES) in operation in the Schengen area

The EES electronically records travelers' personal and biometric data to enhance border security and manage stay durations. Given the sensitive nature of this data, the FDPIC has developed template letters to help data subjects easily exercise their rights to access and control their information.

Additional information and the relevant links are available here.

Voice recognition: FDPIC concludes its investigation

The FDPIC concluded its investigation into PostFinance's use of voice recognition for authentication on 16 May 2025, ruling that the company must obtain explicit consent before creating voiceprints and delete any voiceprints created without such consent. While it is clear that voiceprints, as sensitive biometric data, require careful handling due to their unique and irrevocable link to an individual's identity, it remains to be seen whether the Federal Administrative Court will follow the FDPIC's requirement for an explicit pre-approval on appeal.

The FDPIC's communication has been published here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

The new situation report of the Federal Intelligence Service

Published in July 2025, the Federal Intelligence Service's (FIS) report titled "Switzerland's Security 2025" explores topics such as the relationship between the United States and China, as well as the geopolitical situation in other parts of the world, terrorism, violent extremism, or cyberattack threats. On this last point, the FIS insists on the importance of Switzerland assessing its security situation in the global context and points out that its strategic radar is currently tracking 15 crisis hotspots simultaneously. Cyberattacks are considered to pose a significant threat for operators of Switzerland's critical infrastructure.

The official press release, including a download link for the report and the situation radar tool 2025 can be found here.

Digital Switzerland Advisory Board: Cybersecurity in Switzerland today

At the Digital Switzerland Advisory Board meeting on 30 October 2025, representatives from government, business, academia, and civil society discussed the current state of national cybersecurity measures. The focus was on information security within the National Cyberstrategy (NCS), emphasizing cybersecurity as a cornerstone of digitalization and a key priority of the Digital Switzerland Strategy for 2025. The meeting highlighted the importance of cybersecurity in maintaining trust in digital services and infrastructure, as well as its role in the Federal Council's broader security policy.

Discussions centered on raising awareness, everyday protection measures, and ensuring authorities' operational capacity during crises, while also exploring ways to strengthen Switzerland's international cybersecurity standing. Participants stressed that cybersecurity is not just a technical issue, but also a societal and strategic challenge. Rapid implementation of NCS measures and accessible information for public and private sectors were identified as crucial for success. The meeting demonstrated Switzerland's strong partnerships and commitment to addressing digital challenges with foresight and determination.

The press release is available here.

Cyber start-up challenge 2025

Pometry Ltd, a London-based start-up, has won the Cyber-Defence Campus of armasuisse's annual cyber start-up challenge with its innovative real-time graph analytics technology.

The competition, organized by armasuisse's Cyber-Defence Campus since 2019, promotes collaboration between research, industry, and government by offering start-ups the chance to showcase and implement their technologies within the Federal Department of Defence, Civil Protection and Sport (DDPS). Pometry Ltd will now develop a proof of concept for the DDPS, supported by an order worth up to CHF 100,000.

You can read more in the relevant press release here.

The 2025 National Cybersecurity Conference

In September 2025, around 250 representatives from the fields of politics, public administration, business, and academia discussed the key challenges in ensuring digital security in Switzerland. The focus of the discussion was on whether clear legal requirements are necessary for strengthening cyber resilience, or if companies, public authorities and private individuals should be responsible for taking their own measures.

The relevant press release is available here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Negotiating mandate for the recognition of electronic signatures

The Federal Council tasked the Federal Department of the Environment, Transport, Energy and Communications, together with the Federal Department of Foreign Affairs, with preparing a negotiation mandate with the EU regarding mutual recognition of electronic signatures. Currently, the EU does not recognize Swiss electronic signatures, nor does Switzerland recognize those from the EU.

Mutual recognition would ensure that electronic certificates issued by an EU member state are valid in Switzerland and vice versa. This would benefit both parties by promoting digitalization and the reliable cross-border use of electronic signatures, addressing needs expressed by customs authorities and the public procurement sector. The departments involved will define the negotiation mandate within a year.

The relevant publication can be accessed here.

Digital Switzerland Strategy: Information and cyber security

Information security and cyber security form one of the pillars of the Digital Switzerland Strategy and fall under the responsibility of the National Cyber Security (NCSC). Three continuously updated related measures are part of the pillar, *viz.* (i) security in the automated driving sector, (ii) promotion of ethical hacking, and (iii) implementation of mandatory reporting for cyberattacks.

The relevant updates are published here.

The NCSC's ongoing updates and coordinated cyber incident response

On its website, the NCSC publishes the current incidents (such as current phishing campaigns), and statistics of reports received, as well as hot topics. The homepage is available here.

Amongst the key updates of 2025 is the NCSC developing a concept for coordinated cyber incident response. The press release, including a download link for the concept, is available here.

The Federal Chancellery's Cloud Enabling Büroautomation (CEBA) project

The aim of the CEBA project is to replace the Office product suite currently used in the Federal Administration's workplace systems, "Microsoft Office LTSC Professional Plus 2021," with the cloud-based solution "Microsoft Office 365."

The FDPIC has accompanied the project from a supervisory perspective, with a focus on ensuring a thorough data protection impact assessment, pushing for the examination of alternatives, and emphasizing the need to assess risks related to foreign access and reliance on dominant cloud providers.

Additional information has been published on the FDPIC's website here.

Stablecoins and crypto – consultation launched

The Federal Council launched a consultation on 22 October 2025 to amend the Financial Institutions Act. The proposed changes include introducing a "crypto-institution" license for cryptocurrency services with tailored regulatory requirements. The reform seeks to maintain Switzerland's competitive edge in fintech and blockchain, align with international standards, and strengthen consumer protection. The consultation period ends on 6 February 2026.

The press release with download links for the relevant documentation can be found here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

The sixth National Cyber Security Event 2025

On 25 November 2025, the sixth National Cyber Security Event, organized by SIX, the Swiss Risk Association, and the Swiss Finance Institute, took place in Zurich. Addressing the latest updates shaping Switzerland's cyber resilience, this event looked at the current situation in Switzerland in the context of the overall geopolitical situation, assessed the impact of AI agents on cybersecurity operations, and explored risks tied to blockchain and smart contracts.

More information is available here.

Switzerland's Digital Sovereignty report approved by the Federal Council

During its meeting on 26 November 2025, the Federal Council approved a report defining Switzerland's digital sovereignty. It highlights Switzerland's current strengths, including risk management, promotion of open-source software, a hybrid multi-cloud strategy, and trustworthy infrastructures like e-ID. Recognizing rapid global digitalization and geopolitical challenges, the Federal Council has mandated an interdepartmental working group to continuously assess security and foreign policy impacts on digital resources, coordinate measures, and propose further action to enhance the availability, confidentiality, and protection of Switzerland's digital assets.

Read the press release and download the report here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

"AI search" on Fedlex

Fedlex, the publication platform for federal law, has launched a new "AI search" functionality earlier this year. While Fedlex has had a keyword search available, the "AI search" provides a search technique that does not simply find results based on exact words but attempts to understand the meaning or intent of the user's query.

The "AI search" can be found here; a practical guide is available here.

Switzerland signs the Council of Europe Convention on Artificial Intelligence

The Council of Europe's AI Convention sets binding standards for transparency and non-discrimination in the field of artificial intelligence. The Federal Council took the decision to ratify the Convention and make the necessary amendments to Swiss law on 12 February 2025.

The relevant press release has been published here.

In this context, the Federal Council had mandated a baseline legal analysis, a sectorial analysis and an analysis of other countries' regulatory landscape in order to get an overview of the possible regulatory approaches to AI; the publication and report can be found here.

Publication of report on EU data policy monitoring

A report published in February 2025 analyses the impact of the EU Digital Policy on Switzerland. It points out, *inter alia*, that areas like artificial intelligence and cybersecurity may present additional market access barriers for Swiss companies. The next detailed analysis is planned for early 2027.

The relevant press release and a link to the report are available here.

The Federal Administration has defined the principles governing its use of AI strategy

The strategy lays down the bases for the Federal Administration's digital transformation and will be followed by an implementation plan listing both existing and newly identified measures, which should be presented to the Federal Council by the end of 2025.

The document summarizing the strategy use of AI systems in the Federal Administration has been published here; various factsheets on the topic can be found here.

This development is part of the Digital Switzerland Strategy measure "Strategy for the use of AI systems in the Federal Administration," see here.

Apertus: Switzerland's very own language model

On 2 September 2025, Switzerland's first large-scale, open, multilingual language model – Apertus – was released.

The model is to serve as a building block for developers and organizations for future applications, including chatbots, translation systems, and educational tools. Its distinctive feature is openness – its development process, architecture, model weights, training data, and recipes are openly accessible and fully documented.

The press release is accessible here; the full tech report and information on how to access Apertus can be found here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The use of intelligent video surveillance cameras at automatic checkouts: FDPIC closes its preliminary investigation

The FDPIC has closed its preliminary investigation into Coop Group's use of AI surveillance cameras at self-service checkouts, deciding not to open a formal investigation. The inquiry, prompted by the media in February 2025, found that the cameras, which notify customers via pictograms that said cameras were equipped with software capable of detecting customers who did not scan all their products, do not recognize faces or analyze purchasing habits.

After reviewing Coop's explanations on the cameras' operation, data processing, transparency measures, and legal compliance, the FDPIC concluded that the use of these AI-equipped cameras complies with the FADP and poses no increased risk to individuals' data privacy. Consequently, the case was closed without further action.

The official communication is available here.

Update on the current data protection legislation being directly applicable to AI

In the last edition, we reported on the FDPIC confirming that the current data protection legislation applies to AI-supported data processing. On 8 May 2025, the FDPIC published an update on the topic, emphasizing that existing data protection laws already require transparency, user consent, and safeguards for digital self-determination in AI applications, including rights to object to automated decisions and to know when interacting with AI. High-risk AI processing is permitted only with appropriate protections and impact assessments, while practices undermining privacy, such as real-time facial recognition or social scoring, are prohibited.

More information can be found here.

The training of the AI Grok: FDPIC closes its preliminary investigation

The FDPIC has concluded its preliminary investigation into the use of personal data from X to train the AI Grok. Following concerns raised in early summer 2024, the FDPIC engaged with Twitter International Unlimited Company (TIUC), the operator of X, to assess the transparency of data processing and the availability of opt-out options for users. TIUC appointed a Swiss representative and disclosed details about using public posts to train AI models, including generative models.

Since 16 July 2024, TIUC has provided users with an opt-out option in the data protection settings, allowing them to prevent their posts from being used for AI training. The FDPIC found that this measure complies with the FADP requirements and aligns with similar provisions in the EU. Responsibility for managing the use of personal data for AI training lies not only with TIUC but also with X users, who must utilize the available settings to control their data.

The FDPIC has published its communication on this topic here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Introduction of SwissGPT

One of the measures of the Digital Switzerland Strategy action plan is the introduction of SwissGPT as an alternative to the widely-used GPT portals, operated predominantly from the United States and China, and unregulated. The idea behind SwissGPT is a solution originating from Switzerland and operated in its own data centers, ensuring data protection compliance.

AlpineAI is responsible for bringing SwissGPT to life, with the recommendation for nationwide use of the solution currently being scheduled for 2026.

For more information and regular updates, see here.

Draft legislation to implement the Council of Europe Convention on Artificial Intelligence

Following ratification of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law in February 2025, the Federal Council has tasked the Federal Department of Justice and Police with preparing a preliminary draft legislation for external consultation by the end of 2026. The draft shall take into consideration the parallel efforts of preparing a non-legally binding measures implementation plan (see the following update below).

For more information and regular updates, see here.

Implementation plan for non-legally binding measures under the Council of Europe AI Convention

The decision of the Federal Council on 12 February 2025 to regulate AI (see the previous section of this update) is guided by three key principles, including development of non-legally binding measures in parallel with formal legislation. The Federal Council has issued an instruction to formulate a plan for such measures by the end of 2026. This initiative is being developed in tandem with the initiative focused on legally binding measures (see the previous update above).

For more information and regular updates, see here.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Taiwan

Contacts

Henry Tsai

Partner, Deloitte Legal Taiwan

hentsai@deloitte.com.tw

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Amendments on the Personal Data Protection Act (PDPA)

On 12 August 2022, the Taiwan Constitutional Court (TCC) made a judgement 111 Hsien-Pan-13 (Case on the National Health Insurance Research Database), in which the TCC explicitly stated that the PDPA and other pertaining regulations were insufficient of independent supervisory instruments on data protection. Therefore, the TCC required competent authority to ensure relevant legal mechanisms be established to fulfill the right to protection of personal data under the Constitution within a grace period of three years.

With request form the judicial branch, the Executive branch, on 5 December 2023, incepted the Preparatory Office of the Personal Data Protection Commission. On 27 March 2025, the Executive Yuan proposed draft amendments of PDPA and Personal Data Protection Commission Organizational Act (PDPCOA). While the PDPCOA is still under examination of the Legislative Yuan, the Legislative Yuan passed the amendment of PDPA on 17 October 2025, with a core purpose of strengthening a comprehensive independent supervisory mechanism with enforcement powers and building a robust data governance in the era of widely use AI application. Below are the important keys of the amendment:

- Establishment of a data protection officer (DPO)

Article 18 of the amendment requires government agencies to appoint a DPO, designated by the head of the agency from among suitable personnel, to strengthen internal oversight of personal data protection. The responsibilities of the DPO include promoting and supervising data protection practices within the agency and its subordinate units, ensuring compliance with the PDPA, conducting internal assessments, and coordinating with the PDPC on supervisory matters. The legislative intent emphasizes the need for a dedicated officer to bridge the gap between policy and implementation, thereby ensuring that public authorities handle personal data responsibly

- New requirements for data breach notification and reporting

The current PDPA requires government agencies and nongovernment agencies to notify the data subject upon personal data leakage.

However, failure to notify does not come with sanctions that forces agencies to comply. To address this problem, Article 12 of the amendment stipulates when agencies “become aware that the personal data held has been stolen, altered, damaged, lost, or disclosed”, they *shall* notify the data subjects. Moreover, under leakage of certain data, the agencies must report competent authority and adopt immediate and effective measure to prevent expansion of data leakage. Regarding failure to comply with the above regulations, nongovernment agencies will face fines up to NTD$200,000.

- External supervisory mechanism

Under the current law, there are no provisions governing external supervisory mechanisms or administrative inspection to government agencies. In light of TCC Judgement 111-Hsien-Pan-13, which requires strengthened oversight of the lawfulness and reliability of personal data collection and use, this amendment introduces a new chapter 3-1 divided into two sections: supervision on government agencies and on nongovernment agencies.

Under Article 21-1 of the amendment, government agencies shall report to their superior authorities or supervisory bodies on the implementation of personal data protection management measures and shall be subject to guidance and audits. Where deficiencies or areas for improvement are identified in the audited agency’s practices, the audited agency must submit an improvement report to the auditing authority. When necessary, the auditing authority may require the audited agency to provide further explanations or adjust. This is based on the inherent hierarchical administrative supervision within the public sector, while Article 21-2 of the amendment grant supervising power which derives from the external independent agency. In addition to this, the amendments also establish administrative inspection and disciplinary action, sanctions, or penalties when personnel fails to act in accordance with the provisions of PDPA. With respect to administrative inspections of nongovernmental entities, the amendment introduces provisions requiring the competent authority to consider the characteristics of each industry, including the nature of operations, business models, and the use of data, to assess different levels of risk and to establish a differentiated review mechanism consistent with the principle of proportionality.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Amendments of the Cyber Security Management Act

The Cyber Security Management Act (the Cyber Act) was enacted in 2018, aiming to actively promote national cybersecurity policies and accelerate the establishment of a secure national cyber environment.

To strengthen the overall legal framework for national cybersecurity, promote inter-agency cooperation and regional joint defense, effectively implement cybersecurity management and protection for regulated agencies and critical infrastructure, and advance mechanisms for the capacity building of cybersecurity personnel. The Administration of Cyber Security under the auspices of Ministry of Digital Affairs (MODA), on 4 July 2024, proposed a draft on the Cyber Act amendments. On 29 August 2024, the Legislative Yuan pass the Cyber Act amendment. The main points of the amendment is discussed as below:

- Clearly defined authorities and responsibilities

Articles 2 and 5 of the new Cyber Act designate MODA as the new competent authority, responsible for overall coordination and implementation of Taiwan's cybersecurity legal framework, whereas the Administration for Cyber Security under its supervision executing and handling national cybersecurity affairs. The new Cyber Act provides a clearer line to differentiate responsibility for competent authorities, thereby enhancing accountability, improving inter-agency cooperation, and ensuring more effective enforcement of national cybersecurity policies. The Executive Yuan, as the competent authority under the old Cyber Act, is now solely responsible for determining the overall national cybersecurity strategy.

- Public–private sector joint defense cooperation

To enhance society's overall capacity to respond to cybersecurity incidents, Article 4 requires government to establish support mechanisms to assist private institutions in addressing major cybersecurity events and to strengthen societal cyber resilience. Furthermore, Article 25 authorizes the competent authority to carry out administrative investigations into major cybersecurity incidents concerning designated nongovernmental entities, to determine their root causes.

- Mandatory appointment of cybersecurity specialists

The new Cyber Act requires government and specific nongovernment agencies to appoint a cyber security officer and dedicated cybersecurity personnel subject to suitability reviews. The appointee must be considered in accordance with the applicable level of cybersecurity responsibility, strengthening and enhancing the professional expertise of cybersecurity staff, and ensuring mobilization and support in response to major cybersecurity incidents.

According to Article 12 of the new Cyber Act, government agencies should appoint a cyber security officer who shall be responsible for promoting and supervising cybersecurity-related affairs within the agency. Furthermore, Article 18 stipulates that government agencies should appoint dedicated cybersecurity personnel in charge of cybersecurity operations and incident response. The competent authority shall properly plan and promote professional training programs for such dedicated personnel and encourage them with reward mechanism.

- Stricter management measures

The new Cyber Act introduces a new provision (Article 11) prohibiting government agencies from downloading or installing products that may endanger national cybersecurity. This measure aims to reduce supply chain risks and strengthen overall national cyber defense. It marks the first time that the government has, at the statutory level, explicitly restricted the use of high-risk cybersecurity products, thereby ensuring the security and reliability of public sector information systems.

As for specific nongovernment agency, Article 27 does not impose an outright prohibition on downloading or installing products that may endanger national cybersecurity. However, such agencies are still required to comply with security rules corresponding to their assigned level of cybersecurity responsibility. Once the Ministry of Digital Affairs or the Administration for Cyber Security designates certain products or services as harmful to national cybersecurity, non-designated government agencies are likewise prohibited from using them.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Enactment of the Fundamental Act on Artificial Intelligence (AI Act)

The Executive Yuan proposed a draft on Fundamental Act on Artificial Intelligence on 28 August 2025, which is currently under examination of the Legislative Yuan. In consideration of the national circumstances, this Act aims at encouraging technological innovation, while safeguarding human rights, and upholding national and cultural values. According to Article 3 of the draft, the Executive Yuan established foundational standards functioning as benchmark and guiding posts, serving as the core principles for AI development and deployment.

The seven principles include:

- Sustainability: AI development and application shall consider social equity and environmental sustainability, reduce potential digital divides, and enable citizens to adapt to the transformations brought by artificial intelligence.
- Human autonomy: AI shall support human autonomy, respect fundamental rights and cultural values, allow human oversight, and uphold a human-centric approach aligned with the rule of law and democratic principles.
- Privacy protection and data governance: Personal data privacy shall be safeguarded through data minimization principle and leakage prevention, while promoting the opening and reuse of nonsensitive data under constitutional privacy guarantees.
- Security: During the development and application of AI, cybersecurity protections shall be established to guard against threats and attacks, thereby ensuring system robustness and safety.
- Transparency and explainability: AI outputs shall include appropriate disclosure or labeling to assess risks, understand impacts on rights and interests, and therefore enhance trustworthiness in AI.
- Fairness: AI development and application shall minimize risks of algorithmic bias and discrimination, ensuring that no specific group is subjected to unfair outcomes.
- Accountability: All actors in AI development and application shall bear corresponding responsibilities, including internal governance and external social accountability.

The Act establishes the fundamental principles for AI research, application, and governance, with the dual objectives of encouraging technological innovation and aligning with international standards, while balancing intellectual property rights and personal data protection. This initiative anchors the nation's strategic development direction, with the goal of building Taiwan into an AI Island and elevating its position as a key driver of global AI development.

Moreover, to achieve the above goals, the AI Act focused on encouraging innovation and ensure human rights by promoting relevant articles. Regarding **encouraging innovation**, Article 4 of the draft requires the government to actively promote incentives and subsidies for research, development, and application, as well as fiscal preferential measures. Article 6 encourages the government to foster public–private partnerships and international cooperation to facilitate exchange and utilization, while Article 14 paragraph 1 promotes data openness and usability to achieve innovation and collaboration. Furthermore, with respect to enhancing citizens' literacy and overall capacity in AI, Article 6 paragraph 2 promotes international exchange of AI talent, and Article 7 calls for strengthening public awareness and literacy in AI. Finally, Article 5 establishes a regulatory sandbox for AI research, development, and application services, and Article 11 paragraph 2 provides for the relaxation of usage restrictions on high-risk AI prior to deployment.

With respect to **safeguarding human rights**, in order to ensure that the intensity of AI governance is proportionate, Articles 9 and 15 stipulate that the government shall establish a risk classification framework and implement tiered, risk-based management measures as required for risk management. Article 11 further requires the establishment of responsibility and redress mechanisms for high-risk AI applications. In addition, the draft mandates that AI must be subject to evaluation: Article 8 provides that the government shall develop tools and methods for verifying the authenticity of AI, while Article 10 requires strengthening the verifiability of AI-driven decisions. From the perspective of human rights protection, given the potential significant impacts of AI on labor rights and personal data privacy, Articles 12 and 13 specifically address these concerns.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

Now that the amendment of the Personal Data Protection Act has been passed by the Legislative Yuan, the Executive Yuan will, in coordination with the progress of the Personal Data Protection Commission Organizational Act under legislative review and after considering the necessary administrative preparations, separately designate the effective date of the new PDPA. Prior to the official establishment of the Personal Data Protection Commission, the Preparatory Office will continue to examine personal data protection issues arising in the digital era and plan for the next phase of amendments to the PDPA.

Another area to monitor is how the final law defines the criteria for data breach reporting. Key questions remain about what thresholds will trigger notification duties, the timelines within which reports must be made, and the precise information that must be disclosed to both regulators and affected individuals. These details will directly affect the compliance burden on both public and private entities.

The transition of oversight powers also deserves attention. At present, many sectoral regulators and local governments enforce data protection in their respective fields, but the amendments envision a gradual transfer of authority to the PDPC. During this transition period, collaboration between the PDPC, sector regulators, and local governments will be essential to ensure consistent enforcement and avoid regulatory overlap or gaps.

Finally, the role of the PDPC in regulating cross-border data transfers will be significant. As international data flows expand—particularly in the context of AI applications and global cloud services – the way Taiwan's new authority addresses adequacy, safeguards, and restrictions will shape its integration into the global data protection landscape. Accordingly, the Preparatory Office will issue relevant subordinate regulations and public notices. Equally important will be the PDPC's approach to harmonizing the new centralized regime with existing sector-specific rules in finance, healthcare, insurance, and other industries, which may require supplementary regulations to maintain coherence.

Cybersecurity

In the coming year, Taiwan's cybersecurity legal framework is expected to undergo significant strengthening as the amended Cybersecurity Management Act advances through the Legislative Yuan. The revisions designate the Ministry of Digital Affairs as the competent authority, supported by the Administration for Cyber Security, and expand its supervisory powers. Key developments include stricter reporting obligations for major cybersecurity incidents, with fines of up to NT$10 million for noncompliance; mandatory appointment and suitability reviews of dedicated cybersecurity personnel; and enhanced oversight of critical infrastructure and supply chain security, including potential restrictions on high-risk products and services. In the coming year, we can expect the law will be followed by subordinate regulations clarifying personnel qualifications, audit procedures, and incident response protocols, marking a shift toward a more institutionalized, tiered, and enforceable cybersecurity governance system.

AI

The Legislative Yuan is expected to deliberate on the draft "Fundamental Act on Artificial Intelligence" and enter committee negotiations. If passed, relevant ministries (such as the Ministry of Digital Affairs, National Science and Technology Council, Ministry of Economic Affairs, and Financial Supervisory Commission) will subsequently formulate subordinate regulations and ministry-level governance guidelines. These may cover areas such as differentiation on AI risk classification, transparency, data governance, model security and testing principles, as well as compliance pathways, certification, and audit mechanisms for industry sectors.

Since the Act regulates on a broader framework in terms of artificial intelligence application and governance, we can foresee competent ministries promulgate regulations pertinent to specific industries in using artificial intelligence at work force. Therefore, companies that already employ AI in their operations, as well as those planning to adopt it, should closely monitor and comply with the latest government updates and guidance.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Thailand

Contacts

Niorn Yukolthong

Partner, Deloitte Legal Thailand

nyukolthong@deloitte.com

Sutthika Ruchupan

Counsel, Deloitte Legal Thailand

sruchupan@deloitte.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Thailand's PDPC levied major fines on data controllers and data processors

Overview

- Historically, the Personal Data Protection Committee (PDPC) issued relatively few major fines, reflecting a measured enforcement approach.
- In 2025, the PDPC issued at least five significant fines across both private and public entities, demonstrating a clear shift toward more active and assertive enforcement.
- Importantly, these cases show that the PDPC now holds public-sector agencies accountable alongside private organizations, making it clear that no entity is exempt from PDPA compliance.
- The fines underscore the need for organizations to strengthen technical and organizational safeguards, vendor oversight, and data protection governance to avoid penalties.
- Overall, 2025 marks a turning point in Thailand's data-protection enforcement landscape, signaling that compliance is now being rigorously monitored and enforced.

Summary of cases

On 1 August 2025, the PDPC announced that it imposed a total of approximately THB 14.5 million in administrative fines under the Personal Data Protection Act B.E. 2562 (PDPA) across five cases involving public and private sector organizations. The key points of these cases are summarized below:

- Government agency data leak (200,000+ data subjects)
  - Cause: Weak security controls, weak passwords, no data processing agreement (DPA)
  - Penalties: Fines of THB 153,120 each for the agency and its system developer
- Hospital medical record disposal failure (1,000+ records)
  - Cause: Contractor failed to properly destroy sensitive documents; inadequate oversight
  - Penalties: Hospital fined THB 1,210,000 and the contractor was fined THB 16,940 (total THB 1,226,940).
- Computer retailer breach
  - Cause: Lack of adequate security measures
  - Penalties: THB 7 million
- Cosmetic company breach
  - Cause: Failure to maintain proper security safeguards
  - Penalties: THB 2.5 million
- Toy reseller and its processor breach
  - Cause: Insufficient data security protections
  - Penalties: Toy reseller fined THB 500,000 and processor was fined THB 3 million

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The prescription of subordinate laws by the PDPC

In 2024, the PDPC introduced several new legislations to further clarify the enforcement of the PDPA, as provided below:

Summary of PDPC legislation 2025

- Rules on the Review and Certification of Personal Data Protection Policies Within the Same Affiliated Business or Group of Undertakings, B.E. 2568 (2025) (PDPC Rules on Policies Within the Same Group).
  - PDPC Rules on Policies Within the Same Group added provisions that govern the submission, review, certification, and supervision of binding corporate rules (BCRs) under Section 29 of PDPA – allowing a corporate group to transfer personal data within affiliated entities under an approved BCR, even if destination countries are not yet "whitelisted" under Section 28.
  - It sets out two BRC categories, one for data controllers and another for data processors.
  - It also provided an expedited review process for applicants with existing BCRs certified under EU/UK GDPR or other recognized jurisdictions.
- Notification of the Personal Data Protection Committee on State Agencies Required to Appoint Data Protection Officers (No. 2) B.E. 2568 (2025) (PDPC Notification on State Agency DPO).
  - The PDPC Notification on State Agency DPO added to the first PDPC Notification on State Agency DPO and expanded the range of state agencies required to appoint a data protection officer (DPO), now extending the obligations to additional tiers of local state agencies.
- Notification on Exemption for Data Controllers who are SME B.E. 2567 and Notification on Exemption for Data Processors who are SME B.E. 2567 (PDPC Notifications on Exemption for SME).
  - A small and medium-sized enterprise (SME) is defined under the Thai Small and Medium Enterprises Promotion Act B.R. 2561 (2018) based on number of employees and annual revenue, with thresholds varying by sector.
  - The PDPC recognized that full PDPA obligations – particularly record-keeping requirements – can be disproportionately demanding for SMEs with limited resource, therefore, the PDPC Notifications on Exemption for SME introduce specific exemptions for SME data controllers and SME data processors under the PDPA, focusing primarily on relieving smaller organizations from the obligation to maintain a record of processing activities (RoPA);
  - The notifications clarify that the exemptions do not apply where the SME is required to appoint a DPO, conducts high-risk or non-occasional processing, or processes sensitive personal data. All other PDPA obligations – including security measures, data-subject rights handling, and breach notifications – continue to apply.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

The Netherlands

Contacts

Sebastiaan ter Wee

Partner, Deloitte Legal Netherlands

sterwee@deloitte.nl

Marlieke Bakker

Senior Manager, Deloitte Legal Netherlands

mabakker@deloitte.nl

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Company fined €30.5 million for unlawful facial recognition database

A US-based company providing facial recognition services has been fined €30.5 million for unlawfully collecting and using biometric data from billions of images scraped from the internet, including those of Dutch citizens. The company created a searchable database of facial images and biometric identifiers without consent or transparency and failed to respond to access requests. As the violations continue, the Dutch Data Protection Authority (DPA) has ordered the company to stop processing data and imposed periodic penalty payments of up to €5.1 million. It is also considering holding the company's directors personally liable. (September 2024)

DPA issues guidance to improve data breach notifications

After reviewing over 50 major breaches from 2023 affecting around 10 million people, the Dutch DPA found that many organizations failed to properly inform affected individuals. Warnings were often delayed, unclear or overly complex. To improve this, the Dutch DPA published practical recommendations and example texts urging organizations to act quickly, use plain language and clearly explain what data was exposed and what victims can do. (September 2024)

Facial recognition use at holiday parks found unlawful

Eight Dutch holiday parks were found to have violated privacy law by using facial recognition for access to swimming pools and playgrounds. Visitors were often not informed that participation was voluntary or that they could use an alternative such as a wristband or access card. In some cases, consent was not requested at all or was unclear. Several parks also failed to inform guests about how their data was processed, how long it was stored and who could access it. (October 2024)

Discriminatory algorithm used in student fraud detection

An investigation by the Dutch DPA found that an algorithm used to detect fraud in student housing grants was discriminatory and therefore unlawful. The system assigned risk scores to students based on education type, distance from their parents' address and age, without objective justification or evaluation. Students in vocational education, those living closer to their parents and younger students were more likely to face inspections. The Dutch DPA concluded that this led to direct and indirect discrimination and urged immediate corrective action for affected students. (November 2024)

Streaming service fined €4.75 million for poor privacy information

A large streaming service has been fined €4.75 million for failing to properly inform customers about how it processed their personal data between 2018 and 2020. The company provided insufficient and unclear information on key aspects such as the purposes and legal bases for data use, data sharing with third parties, data retention, and international transfers. The investigation began after complaints from a privacy organization in Austria and was coordinated with other European regulators. The company has since updated its privacy notice and improved transparency. (December 2024)

Online retailer fined €40,000 for unlawful use of cookies

A large Dutch online retailer has been fined €40,000 for unlawfully processing personal data through cookies without obtaining explicit consent from website visitors. The company assumed users agreed to cookies and used pre-ticked boxes in its consent settings. This case reflects the DPA's broader focus on cookie compliance. (December 2024)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Investigation into data transfers to China amid AI chatbot concerns

The Dutch DPA has launched an investigation into the transfer of personal data to China amid concerns about a Chinese AI chatbot. The Dutch DPA warns that personal information entered by users is stored on servers in China, raising questions about compliance with EU rules for international data transfers. Such transfers are only permitted when sufficient safeguards are in place to protect users' privacy. (February 2025)

European regulators to review compliance with the right to erasure

European privacy regulators will jointly examine how organizations comply with rules on the right to have personal data deleted. In the Netherlands, the Dutch DPA will review various organizations through questionnaires to assess how they handle deletion requests in practice. The initiative is part of a coordinated project under the European Data Protection Board (EDPB). The data protection authorities aim to identify common shortcomings, as complaints often concern organizations that fail to respond or delete data in time. (March 2025)

Organizations warned over misleading cookie banners

The Dutch DPA has ordered 50 organizations to adjust misleading cookie banners or stop intrusive tracking of website visitors. The action follows a large-scale scan of 10,000 websites for possible violations, with the regulator planning to issue similar warnings to around 500 organizations each year. Companies that fail to comply may face further investigation and fines. The first letters went to web shops, media companies and insurers, highlighting recurring problems such as cookies placed before consent, pre-ticked boxes and hidden reject buttons. Since 2024, the Dutch DPA has increased inspections to ensure websites request valid consent and has published guidelines to help organizations design compliant cookie banners. (April 2025)

Social media platform fined €530 million for data transfers to China

The Irish Data Protection Commission, in coordination with the Dutch DPA and other European regulators, has imposed a €530 million fine on a large social media platform for transferring personal data of European users to China without adequate protection. The company failed to demonstrate that user data stored in China was properly safeguarded and did not clearly inform users about these transfers. This is the platform's third GDPR fine for privacy violations involving European users. (May 2025)

Credit scoring company fined €2.7 million for privacy violations

The Dutch DPA has fined a credit scoring company €2.7 million for unlawfully processing personal data and failing to inform individuals properly. The company created credit reports for clients such as telecom providers, online retailers, and landlords using data from various sources including payment histories, debts, and bankruptcies. The DPA found that this information was processed without sufficient justification and transparency. The company has accepted the decision and will delete its Dutch database later this year. (October 2025)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

AFM issued final publication on DORA supervision

In January 2025, the Dutch Authority for the Financial Markets (AFM) released its final publication in a series on the Digital Operational Resilience Act (DORA). The update outlined what financial institutions could expect from supervisory activities in 2025 and encouraged firms to complete the implementation of DORA requirements ahead of the 17 January 2025 deadline. The AFM stressed that firms should already be applying the regulatory and implementing technical standards, even though some elements were still awaiting formal adoption by the European Commission.

The publication described the AFM's intended supervisory approach, including reviews, incident reporting via the new DORA portal and requirements related to license applications. It also noted that some institutions may be designated for extensive threat-led penetration tests (TLPTs), with the AFM supporting firms in preparing and carrying out these tests. (January 2025)

Intelligence agencies warn about cyber group 'Laundry Bear'

The Dutch intelligence and security agencies AIVD and MIVD published an analysis in May 2025 detailing the activities of the cyber group known as Laundry Bear. The actor has been active against western governments since 2024 and was previously linked to the cyberattack on the Dutch police in September 2024. The report outlines Laundry Bear's focus on military and government institutions, defense contractors, social organizations and digital service providers.

According to the agencies, the group uses common intrusion methods such as password spraying, session cookie theft and so-called living-off-the-land techniques. The AIVD and MIVD urged organizations in these and related sectors to apply the recommended protective measures, noting that the tactics used are relevant to a broad range of targets. (May 2025)

Government submits Cybersecurity Act (Cbw) to Parliament

In June 2025, the Dutch government submitted the draft Cybersecurity Act (Cbw) to the House of Representatives. The proposal aims to implement the EU NIS2 Directive and is scheduled to enter into force in **the second quarter of 2026**, depending on the pace of the parliamentary process. Until the act takes effect, organizations are not yet subject to legal obligations under NIS2, although certain rights already apply through directly effective provisions, such as receiving assistance from a computer security incident response team (CSIRT).

The government is currently preparing secondary legislation, including a general administrative order and ministerial regulations that will specify sectoral rules such as incident-reporting thresholds. Organizations may currently register voluntarily through the national cybersecurity portal to access NCSC services if the center acts as their sectoral CSIRT. (June 2025)

DDoS attacks around NATO summit

Multiple Dutch organizations were targeted by a wave of distributed-denial-of-service (DDoS) attacks coinciding with the NATO summit in The Hague earlier this year. The incidents initially affected several municipalities and later extended to the transport sector. Most attacks were claimed by the pro-Russian hacktivist group NoName057 (16). Websites and online services experienced temporary disruptions, but no data breaches or intrusions were detected.

According to the National Cyber Security (NCSC), the attacks fit a broader pattern of politically motivated activity observed in the run-up to the summit. The center monitored developments closely in coordination with national and international partners and provided guidance to potentially affected organizations. The impact of the attacks remained limited and largely symbolic. (June 2025)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Recommendation for sectoral and coordinated AI supervision

AI supervision in the Netherlands should be organized at sector level, with central coordination across regulators. This is the key recommendation put forward by the Authority for Digital Infrastructure (RDI) and the Dutch DPA. Under their advice, existing sectoral regulators would continue overseeing AI within their own domains, making use of their established expertise and mandates.

The RDI and the Dutch DPA would act as coordinating and expert bodies, supporting and advising other regulators and facilitating cooperation between them. The aim is to prevent fragmented oversight and to give organizations clarity about what is expected under the AI Act. (November 2024)

Guidance published to support AI literacy in organizations

The Dutch DPA has published guidance to help organizations improve AI literacy among employees who develop or use AI systems. From 2 February 2025, the EU AI Act requires organizations to ensure that staff working with AI have the knowledge and skills to apply it responsibly at technical, practical, social, and ethical levels. The guidance outlines a four-step approach: identify AI systems, set goals, implement actions, and evaluate progress. It emphasizes that AI literacy is an ongoing process and an essential element of responsible AI deployment. (January 2025) Later, the Dutch DPA also published additional guidance on this topic that specifically provides steps organizations can take to build AI literacy within the organization. (October 2025)

Report warns of risks in AI chatbot applications

The Dutch DPA has published the fourth AI and Algorithm Risks Report Netherlands (RAN), outlining key trends, risks, and governance issues in the use of AI and algorithms. This edition pays particular attention to AI chatbot applications for friendship and mental health, which, according to the DPA's research, often provide unreliable or harmful responses. The tested apps blurred the line between human and AI interaction, included addictive design features, and failed to direct users to professional help during crises.

Beyond the chatbot findings, the report reflects on the broader state of AI governance in the Netherlands. It notes progress in developing AI and algorithm frameworks and growing awareness of fundamental rights risks, but also finds that algorithm registration remains insufficient, limiting oversight of high-risk applications. The report further stresses the need for balanced policies that support innovation while safeguarding public values and calls for stronger control measures to keep pace with rapid technological developments and better incident management. (February 2025)

Dutch regulatory sandbox proposed

The RDI and Dutch DPA published a proposal for the implementation of a regulatory sandbox in the Netherlands. This proposal provides a basis to launch a regulatory sandbox which is expected to happen before August 2026, in line with the requirement under the AI Act for EU member states to launch at least one AI regulatory sandbox as of August 2026. (March 2025)

The Dutch DPA shared its vision on Generative AI

The Dutch DPA shared their vision on Generative AI, which includes its vision on how to implement it lawfully and responsibly. (May 2025)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Guidelines published to improve algorithm registration

The Dutch DPA has called for mandatory registration of algorithms used by public authorities and published eight practical guidelines to help organizations get started. Most public bodies have yet to document the AI and algorithmic systems they use, with only about 1,000 algorithms registered so far. The DPA states that national registers remain essential to show how algorithms are used in practice and serve a different purpose from the EU database for high-risk AI systems. (July 2025)

Report warns for risks in AI emotion recognition

The Dutch DPA has issued its fifth AI and Algorithms Report Netherlands (RAN), focusing on AI and emotion recognition. The report concludes that using AI to detect emotions is dubious and risky, as such systems rely on contested assumptions about how emotions arise and can be measured. These applications pose ethical and privacy concerns, including the risk of discrimination and erosion of human autonomy.

The Dutch DPA examined emotion recognition in customer service interactions, wearables such as smartwatches, and language models. It urges extreme caution with these technologies, noting that it is often unclear how AI systems recognize emotions or whether their outcomes are reliable.

Beyond the theme of emotion recognition, the report calls for a comprehensive, democratically grounded national AI strategy. It emphasizes the importance of trustworthy AI, oversight, and education, recommending that a fixed percentage of innovation funding be reserved for internal controls, external audits, and regulatory supervision. (July 2025)

Guidance published on human oversight in AI decisions

The Dutch DPA has published guidelines on meaningful human involvement in algorithmic decision-making. The guidelines aim to help organizations ensure that algorithmic decisions are not made solely by automated systems, but instead through a careful and lawful process with genuine human oversight. The publication provides practical guidance and examples addressing people, technology, process, and governance.

The Dutch DPA has also announced plans to further clarify key GDPR concepts related to automated decision-making, such as when an individual is significantly affected, and what information must be provided to those concerned. (July 2025)

Chatbots must not fully replace human customer service

The Dutch DPA and the Authority for Consumers and Markets (ACM) have jointly stated that organizations using chatbots must always give customers the option to speak with a human and clearly indicate when interactions are automated. According to the regulators, chatbots should be transparent, fair, and must not provide misleading or evasive information.

Their statement follows a rise in complaints about poor service quality and privacy risks related to Generative AI. Both authorities are going to pay closer attention to the use of chatbots, while new EU rules under the AI Act, taking effect in August 2026, will further strengthen transparency obligations for AI-driven customer services. (October 2025)

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

The implementation of the EU NIS2 Directive in the Cybersecurity Act

The implementation of the EU NIS2 Directive into the Dutch Cybersecurity Act (in Dutch: Cyberbeveiligingswet) is scheduled to enter into force in **the second quarter of 2026**, depending on the pace of the parliamentary process. The government is currently preparing secondary legislation, including a general administrative order and ministerial regulations that will specify sectoral rules such as incident-reporting thresholds. Organizations may currently register voluntarily through the national cybersecurity portal to access NCSC services if the center acts as their sectoral CSIRT.

The official designation of Dutch supervisory authorities under the AI Act

The AI Act prescribes that EU member states should designate supervisory authorities on 2 August 2025. Currently, there is only a recommendation on how the AI supervision should be organized in the Netherlands (see the update on slide 277). Based on answers provided by the (former) State Secretary for internal relations (with the responsibility for digitalization) in response to questions from the Dutch House of Representatives, designation of the supervisory authorities requires national implementation legislation. The State Secretary stated that it was foreseeable that the legislation would not be finalized before the aforementioned deadline, due to many stakeholders that need to be involved in the process.

The Dutch government ranked AI as priority three on its National Digitalization Strategy

The Dutch government aims to accelerate on AI in a responsible manner where transparency, safety and democratic control plays a central role. The government aims, among other things, to develop (auditable) standards and procurement guidance for AI use by public authorities, to explore if a government-wide AI competence center can be established and to develop and use AI (GPT-NL and other large language models) for prioritized government use cases. This strategy has been last updated in September 2025, prior to the Dutch elections in October 2025.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Türkiye

Contacts

Ceren Savaşçı

Manager, Deloitte Türkiye

csavasci@dlhukuk.com

Mustafa İriboz

Associate, Deloitte Türkiye

miriboz@dlhukuk.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Guidance on the Processing of Special Categories of Personal Data

The Turkish Personal Data Protection Authority (the Authority) published the Guidance on the Processing of Special Categories of Personal Data on 26 February 2025. The guidance aims to clarify the Personal Data Protection Board's (the Board) approach regarding the conditions under which special categories of personal data may be processed, and to assist data controllers in determining the correct legal bases under the Personal Data Protection Law No. 6698 (PDPL) following the recent amendments. It also explains the obligations that must be fulfilled in order to ensure compliance with the PDPL in processing activities involving sensitive data.

Exemption criterion updated for VERBIS Registration for data controllers whose main activity involves processing special categories of personal data

With its decision dated 4 September 2025 and numbered 2025/1572, the Board updated the Data Controllers' Registry Information System (VERBİS) registration exemption criteria applicable to data controllers whose main activity involves the processing of special categories of personal data.

Under the updated criteria, data controllers whose main activity is the processing of personal data are exempt from the obligation to register with the VERBİS if they employ fewer than 10 employees and have an annual financial balance sheet total of less than TRY 10 million.

As a result, data controllers whose main activity involves the processing of special categories of personal data, such as medical practices, pharmacies and laboratories are also covered by this exemption, provided that they meet the criteria.

Updated Guidance on the Processing of Biometric Data

The Turkish Personal Data Protection Authority published the updated Guidance on the Processing of Biometric Data on 25 March 2025. The guidance reiterates that biometric data constitutes a special category of personal data and provides detailed explanations on the definition and classification of biometric data in line with the EU General Data Protection Regulation (GDPR). In this context, the Authority notes that biometric data must:

- Reveal an individual's unique physical, physiological or behavioral characteristics through processing; and
- Be capable of identifying or authenticating that individual.

The guidance explains that physical characteristics such as fingerprints, retina, palm prints, facial features or iris patterns constitute physiological biometric data, while behavioral indicators such as gait, typing patterns or device interaction habits qualify as behavioral biometric data.

The updated guidance sets out the conditions that must be met for the lawful processing of biometric data, including necessity, proportionality, suitability for the intended purpose, purpose limitation, data minimization and storage only for as long as required. It also emphasizes that biometric data must be deleted without delay once the purpose no longer exists. Data controllers are required to provide transparent information notices, and where explicit consent is needed, individuals must be fully informed about both the subject and the consequences of their consent.

The guidance also underscores the need to document compliance, justify the choice of biometric modality, avoid collecting genetic data unless strictly necessary and specify maximum retention periods in data retention and destruction policies. The final section of the guideline sets out the administrative and technical measures expected from data controllers when processing biometric data.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Public announcement regarding standard contracts for cross-border transfers

On 5 February 2025, the Turkish Personal Data Protection Authority (the Authority) published a public announcement on key issues to consider when executing standard contracts (SSC) for cross-border transfers of personal data. The announcement reiterates that SSCs serve as an "appropriate safeguard" mechanism within the new transfer framework and therefore must be prepared and submitted in strict compliance with the PDPL and secondary legislation.

The Authority emphasizes that SSCs must be signed either by the transfer parties themselves or by individuals duly authorized to represent and bind those parties. Signatures must comply with the formal requirements of the Turkish Code of Obligations, and signature authority documents submitted to the Authority must clearly identify the individuals who have signed. SSCs signed by unauthorized persons or with incomplete documentation will be deemed invalid. Where SSCs are executed in more than one language, both parties must sign the Turkish version; in dual-column contracts, signatures must appear specifically under the Turkish text.

Moreover, it emphasizes that executed contracts must be notified to the Authority within five business days following the signing date, and that the contract text must maintain consistency in terms of language, party details and content. The announcement provides much-needed clarity on procedural aspects of SSC adoption following the 2024 PDPL amendments and the subsequent secondary legislation.

Finally, the Authority underlines that SSCs may not be back-dated and that, apart from selecting among alternative clauses, parties may not modify the standard text. Any addition, deletion or alteration outside the permitted alternatives will render the SSC non-compliant and unable to serve as an appropriate safeguard for international data transfers.

Administrative fine notifications to be delivered via the Revenue Administration's E-Notification System

The Authority announced that administrative fine notifications will now be delivered through the Ministry of Treasury and Finance Revenue Administration's E-Notification System, established under the Tax Procedure Law No. 213. Notifications will be deemed served on the fifth day following their arrival in the recipient's electronic mailbox.

For data controllers who are not taxpayers, the previous notification procedures will continue to apply.

Public announcement on fulfilling the obligation to inform within the scope of mediation activities

On 13 January 2025, the Authority issued a public announcement addressing the fulfilment of the obligation to inform within the context of mediation activities carried out under Law No. 6325 on Mediation in Civil Disputes.

The announcement explains that the informational duty under Article 11 of the Mediation Law is distinct from the obligation to inform stipulated in Article 10 of the PDPL. Accordingly, mediators must provide two separate notifications: one concerning the mediation procedure itself, and another concerning the processing of personal data under the PDPL. The Authority underlines that mediators act as data controllers when processing parties' personal data and are therefore subject to all obligations under the PDPL, including transparency, data minimization, security and purpose limitation requirements.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Updated Cookie Practices Guidance published

In July 2025, the Turkish Personal Data Protection Authority (the Authority) republished its updated Cookie Practices Guidance, originally issued in 2022. The guidance provides comprehensive explanations on the use of cookies and similar technologies in desktop and mobile websites and web-based applications.

It outlines the legal bases applicable to each type of cookie, the principles of obtaining explicit consent where required, transparency obligations, cookie categorization and the expectations for compliant cookie management tools. The revisions reflect the Authority's increasing focus on user autonomy, avoiding dark patterns, and ensuring that consent mechanisms offer equal-level access to choices without pre-selected options.

Updated sectoral guidance for the banking sector

The Authority updated the Banking Sector Good Practices Guidance to align it with the 2024 amendments to the PDPL.

The updated version provides detailed explanations on the conditions for the processing and transfer of both sensitive and non-sensitive personal data in the banking sector, including examples illustrating the application of adequacy decisions, appropriate safeguards such as SSCs and binding corporate rules (BCR), and derogations for exceptional transfers. The revisions aim to support financial institutions in adapting their compliance frameworks to the post-amendment regime and to clarify sector-specific data protection expectations.

Principle Decision of the Board on the prohibition of obtaining explicit consent via SMS

The Board's Principle Decision dated 10 June 2025 and numbered 2025/1072 was published in the Official Gazette on 26 June 2025. Although the Authority had previously issued similar announcements, this decision provides clearer guidance on the processing of personal data through SMS verification codes sent during processes such as payments, registrations, account creation or membership initiation.

According to the decision, data controllers must inform individuals clearly and in advance about the purpose of the SMS verification code and the consequences of entering the code. This information must be provided both before the transaction and through accessible links or statements included in the SMS content.

The Personal Data Protection Board prohibits the use of a single SMS verification step to simultaneously collect membership approval, explicit consent for data processing or marketing permission. Each purpose must be presented separately, and consent must be obtained individually.

The informational obligation and the explicit consent process must also be handled independently. Where verification codes are used to obtain marketing consent, the consent must fully meet PDPL requirements.

Marketing consent cannot be a condition for receiving a product or service. Individuals must be informed that the service will be provided even if the code is not shared and that any preferences given through the code can later be changed. Finally, data controllers should train staff involved in these processes, periodically review their practices and ensure continuous compliance. Non-compliance may lead to administrative fines under Article 18 of the PDPL.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Türkiye's first binding cybersecurity law enters into force

The Cybersecurity Law No. 7545, published in the Official Gazette numbered 32846, on 19 March 2025, represents Türkiye's first comprehensive and binding regulatory framework governing cybersecurity. With the increasing digitalization of critical services, this law aims to establish a coherent and centralized structure for preventing, detecting and responding to cyberthreats. It introduces core definitions such as cybersecurity, cyberspace and cyber incidents, in order to create a unified terminology for public and private sector actors.

This law establishes the Cybersecurity Presidency, responsible for regulatory development, coordination and oversight, and the Cybersecurity Council, tasked with determining national priorities. Organizations offering digital services or processing data through information systems are subject to various obligations, including the implementation of technical and organizational measures, timely notification of vulnerabilities or incidents, cooperation with the presidency and compliance with future technical standards and guidelines. In certain sectors, the use of certified cybersecurity products and the employment of authorized experts will be mandatory.

The law is backed by both administrative and criminal sanctions, ranging from fines of up to TRY 10 million to imprisonment for obstructing audits or operating without proper authorization. Secondary legislation expected within one year is anticipated to clarify certification processes, audit criteria and specific sectoral obligations, making early preparation critical for companies seeking compliance.

Presidential Decree establishing the Cybersecurity Presidency published

The Presidential Decree on the Cybersecurity Presidency (Decree No. 177) was published in the Official Gazette on 8 January 2025. The Decree formally establishes the Cybersecurity Presidency (the Presidency) as a public legal entity affiliated with the Presidency of the Republic and sets out its organizational structure, functions, powers and responsibilities. The primary objective of the Presidency is to strengthen Türkiye's national cybersecurity posture, protect critical infrastructure and enhance the State's resilience against cyberthreats. The decree stipulates that, until the relevant units within the Presidency become operational, the duties assigned to the institution will be carried out by the competent public authorities under a transitional arrangement.

The decree details the core mandates of the Presidency, including:

- The development and coordination of national cybersecurity policies, strategies and action plans;
- The organization of awareness and training initiatives;
- The enhancement of the domestic cybersecurity ecosystem and support for competitive product and technology development;
- Participation in national and international exercises and events;
- The creation of emergency response and crisis management plans; and
- The provision of opinions regarding incentives to be granted by public authorities in the cybersecurity field.

The Presidency's organizational structure consists of the President and several service units. The decree also authorizes the president and senior managers to delegate certain powers in writing, without relieving the delegating authority of ultimate responsibility.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Recommendations on personal data protection in AI

The Turkish Personal Data Protection Authority (the Authority) published key recommendations on its official LinkedIn account regarding the protection of personal data in the context of AI. The recommendations emphasize the importance of safeguarding fundamental rights and freedoms as AI technologies continue to evolve and are increasingly deployed across various sectors.

The Authority highlights that AI systems should be designed with a human-centric approach and that all algorithms must remain accountable from a data protection perspective. It also stresses the need for participatory risk assessments involving individuals and groups likely to be affected by AI applications, the avoidance of decisions based solely on automated processing, and the preference for anonymization where possible. The recommendations further underline the importance of privacy-by-design principles, maintaining meaningful human oversight, ensuring data minimization and accuracy, conducting privacy impact assessments for high-risk processing activities, and supporting education and awareness-raising efforts on privacy in AI environments.

Ministry of National Education publishes AI Ethics Recommendations

The Ministry of National Education published the AI Ethics Recommendations booklet as part of its Education AI Policy Document and Action Plan (2025-2029). The booklet aims to guide the safe, ethical and responsible integration of AI technologies into the education system. It seeks to increase awareness among education stakeholders, promote a culture of responsible use and encourage a more critical approach to emerging AI technologies.

In addition to general principles, the publication provides specific recommendations for developers, producers and service providers under the headings of Data Protection and Privacy, Transparency and Explainability, Human Oversight and Control, Child Safety, Ethical and Pedagogical Alignment, Accessibility and Inclusiveness, Collaboration with Third Parties, and Ethical Obligations. The booklet also includes tailored guidance for students, teachers, administrators and parents to support ethical and informed use of AI in educational environments.

AI policy developments in Türkiye

The Parliamentary Research Commission established to assess the opportunities, risks and regulatory needs of AI completed its work on 13 May 2025. During its mandate, the commission examined AI from legal, ethical, economic and sector-specific perspectives, evaluating its impact across healthcare, defense, education, agriculture, labor markets and the justice system.

The commission highlighted Türkiye's need to strengthen digital infrastructure, develop qualified human capital, enhance public-private cooperation and adopt clear, future-proof regulations as part of a national AI strategy.

Türkiye currently lacks a dedicated AI law; while existing frameworks such as data protection, obligations law and intellectual property rules provide partial coverage, significant gaps remain. The commission also discussed the implications of the EU AI Act, the evidentiary challenges posed by deepfakes and the need for updated IP rules and safeguards against algorithmic bias.

Economically, AI was highlighted as a tool for improving tax compliance, detecting informal activity, managing financial risks and boosting productivity. Strengthening scientific infrastructure, supporting domestic technologies and enhancing academia-industry collaboration were identified as key priorities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Alignment of the PDPL with the GDPR

According to the Medium-Term Program for 2026-2028, published by the Cybersecurity Presidency on 7 September 2025, Türkiye has placed digital governance, data protection and technological sovereignty at the center of its strategic agenda. The program confirms that the ongoing alignment of the PDPL with the GDPR will be completed by the third quarter of 2026.

Beyond the PDPL-GDPR alignment, the program outlines a comprehensive roadmap for strengthening Türkiye's digital and legal infrastructure. Planned initiatives include the preparation of a national data governance framework, the development of a National Data Strategy and Action Plan, and the introduction of an Open Data Law to support data-driven decision-making while ensuring privacy and security.

Expected regulations Under the Cybersecurity Law

Secondary legislation to be introduced is expected to provide further clarity on the implementation of the Cybersecurity Law. Upcoming regulations are likely to detail certification processes, audit and inspection procedures, authorized product requirements, incident notification standards and the obligations applicable to high-risk sectors and critical infrastructure operators.

The new rules are also anticipated to define the criteria for licensed cybersecurity service providers, approval mechanisms for cross-border sales of cybersecurity products and the procedural steps for reporting mergers, share transfers or organizational changes to the Cybersecurity Presidency.

Potential regulatory developments in AI

As Türkiye aims to play a more active role in the global AI ecosystem, further legislative and regulatory initiatives are expected. The work of the Parliamentary Research Commission signals a growing focus on establishing clearer rules on AI governance, ethical safeguards, accountability frameworks and sector-specific standards.

Building on this momentum, the Medium-Term Program for 2026-2028 adopts a detailed approach to AI development, deployment and oversight. It foresees expanding AI research clusters and centers, improving access to high-performance computing, supporting the creation of domestic AI models and updating Türkiye's National AI Strategy. AI-based systems will be deployed for market surveillance, product traceability and capital markets oversight, while cooperation between universities, research institutions and the private sector will be strengthened.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Ukraine

Contacts

Anton Bychkov

Senior Manager, Deloitte Legal Ukraine

anbychkov@deloittece.com

Mykhailo Koliadintsev

Manager, Deloitte Legal Ukraine

mkoliadintsev@deloittece.com

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

Ukraine moves toward EU Data Protection standards: Draft Law No. 8153 adopted in first reading

The Parliament has adopted in the first reading Draft Law No. 8153 "On Personal Data Protection" (the Draft Law No. 8153), which is intended to replace the current law enacted in 2010. The adoption of the Draft Law No. 8153 in the first reading indicates that the Parliament has endorsed its main principles and overall structure of the law.

Further refinement will take place during the preparation for the second reading, which will involve a detailed article-by-article discussion and amendments to specific provisions. However, no public information is currently available regarding the timeline for the second reading.

The final adoption of the Draft Law No.8153 is expected upon completion of this process.

One of the key innovations introduced by Draft Law No. 8153 is the establishment of a specialized independent authority – the National Commission for Personal Data Protection and Access to Public Information. This body will replace the current supervisory model, under which the relevant powers are exercised by the Ukrainian Parliament Commissioner for Human Rights (Ombudsman).The creation of such an authority aligns with the GDPR, which require the establishment of supervisory authority. At the same time, the related Draft Law "On the National Commission for Personal Data Protection and Access to Public Information" No. 6177 (the Draft Law No. 6177) – has already been developed, submitted to the Parliament, but has not yet been considered. The Parliament has not yet announced when the first reading of the Draft Law No. 6177 is expected to be considered.

Overall, the adoption of Draft Law No. 8153 in the first reading marks an important step in Ukraine's readiness to modernize its data protection framework.

Ukraine's progress in personal data protection

Ombudsman Report 2024 highlights

Throughout 2024, the activities of the Ombudsman in the field of personal data protection were aimed at strengthening compliance control, raising public awareness, and ensuring an effective response to cases of unlawful data processing.

As part of its supervisory activities, the Ombudsman conducted 103 inspections of enterprises, institutions, and organizations across various sectors. The greatest attention was paid to the education, environmental protection, land management, and public administration sectors – including statistical agencies, ministries, and financial and utility institutions. Based on the results of these inspections, 85 compliance orders were issued to eliminate identified violations.

Typical infringements included incorrect or unlawful determination of legal grounds for data processing, insufficient information provided to data subjects regarding the purpose and scope of processing, absence of internal data protection policies or data deletion procedures, and failure to maintain records of processing operations.

Also, the Ombudsman reported that as of August 2025, 1,134 complaints regarding violations of the right to personal data protection had been received.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Adoption of the law related to the security of state digital resources

General description

In direct response to the unceasing and systematic cyberattacks against its state and critical infrastructure, Ukraine adopted the landmark Law "On Amendments to Certain Laws of Ukraine Regarding the Protection of Information and Cyber Protection of State Information Resources and Critical Information Infrastructure Objects“ (the Law No. 4336-IX).

This law, which came into force in April 2025, represents a transformation of the state's cyber defense posture from a passive to an active model. The Law No. 4336-IX, establishes a clear, unified national system for cyberattack response, defining the roles, functions, and interaction mechanisms for all state structures and introducing new tools for crisis response.

An important provision is the mandatory requirement for all government bodies and critical infrastructure entities to have qualified cybersecurity specialists on staff. Furthermore, the law mandates a unified system for the exchange of information about cyber incidents.

From static compliance to active risk management

The law's most profound impact is its replacement of the outdated model of the Complex System of Information Protection with a more flexible system of risk management. CSIP system was a legacy of Soviet-era thinking, a static, certification-based regime focused on "checking boxes" and producing paper documentation to obtain a certificate of conformity.

This process was not only a significant barrier to innovation – making it difficult for state bodies to adopt modern technologies like cloud computing – but it also provided a false sense of security, as a certificate was valid for years, regardless of the evolving threat landscape.

The new risk-oriented approach, coupled with independent assessment of cyber protection, is aimed to fundamentally change this culture. It shifts the paradigm from static, one-time compliance to continuous, active security management.

This shift unblocks the path for government and critical infrastructure to use modern, agile technologies, but it also places a continuous, active security burden on them and, crucially, on their private-sector suppliers.

Private sector mandates via supply chain

This legislation is not limited to the state authorities. The law applies explicitly to objects of critical information infrastructure (that could be in the state, municipal and private property) and grants new powers to involve specialists from the private sector in incident response. This effectively extends the law's reach deep into the private sector supply chain.

If a private technology company – such as a cloud provider, a data center, or a software developer – provides services to a state-owned bank, an energy company, or a government agency, they are now a component of this national cyber defense system. They will be both legally and contractually obligated to meet these new standards and participate in the national system for exchanging information about cyber incidents.

The Law No. 4336-IX uses the powerful lever of state procurement to uplift the cyber-hygiene of the entire private sector ecosystem that services the state, making cybersecurity a mandatory condition of doing business with the public sector.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

Ukraine joined the Council of Europe Framework Convention on AI and human rights, democracy and the rule of law

Ukraine's accession to the Council of Europe Convention is a preemptive move that sets the legal and ethical boundaries for the nation's AI industry. The document outlines principles that the state must follow in shaping legislation and applying AI products in the public sector: respect for human dignity, transparency, nondiscrimination, privacy protection, reliability, and safety.

The convention's principles will indirectly apply to businesses: the state should create initiatives for the private sector to help companies incorporate these principles into their product development. For example, the Ministry of Digital Transformation should launch the Council of Europe's HUDERIA methodology, which aims to assist in assessing AI products for compliance with human rights, democracy, and the rule of law.

Importantly, the convention does not apply to the use of AI in defense.

The document was developed over three years by representatives of Council of Europe member states, other participating countries, and business and civil society stakeholders. Ukraine actively contributed to the convention's development as a member of the Council of Europe's Committee on Artificial Intelligence.

Recommendations on usage of AI in different areas

The Ministry of Digital Transformation of Ukraine published several guidelines and recommendations:

- Guidelines for responsible AI use: Intellectual property rights issues;
- Guidelines for the responsible implementation and use of AI technologies in higher education institutions;
- Guidelines for responsible development of systems using AI technologies;
- Tips for responsible use of AI by public servants; and
- Guidelines on the responsible use of AI for lawyers.

These sectoral recommendations and guidelines are part of the roadmap for regulating AI in Ukraine and have been developed to provide professionals with practical guidance on the responsible use of AI in their professional activities.

The purpose of these recommendations is to promote the responsible implementation and use of AI systems, as well as to disseminate relevant international practices, principles, and approaches to the responsible application of AI systems, ensuring confidentiality and adherence to professional ethical standards.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

Data protection

Update of the current legislative framework

The change of legislative framework and its alignment with EU regulations will be in focus. Draft Law No. 8153 and Draft Law No. 6177 are the most relevant and expected developments.

Cybersecurity

Expected NIS2 Directive harmonization

Although Ukraine is not a member of the EU, and therefore the Network and Information Security Directive 2 (NIS2 Directive) is not part of Ukrainian law, the Ukrainian authorities are well aware of its provisions and requirements, and its provisions are to some extent reflected in national legislation and cybersecurity systems.

Moreover, taking into account the processes of Ukraine's integration into the European Union, the government is actively involved in the development of regulations to implement the provisions of the NIS2 Directive which should be presented soon.

AI

National AI Strategy

The Strategy for the Development of Artificial Intelligence in Ukraine until 2030 (the National AI Strategy) was presented in November 2025. This national strategy outlines an ambitious mission for Ukraine to join the top three AI countries in the world by 2030.

The National AI Strategy makes it clear that the Ukrainian government intends to be the primary "super-client" for the domestic AI industry. The planned integration of AI into the "Diia" government application, which is used by millions of citizens, along with applications in defense and medicine, represents a massive procurement and innovation signal.

The government want to be the first large-scale local entity to demand that its AI vendors comply with the new rules. The government's procurement standards should, by default, require vendors to demonstrate adherence to the Council of Europe Convention's "Assessment of Impact" principles and the EU AI Act's risk-based approach.

Ukraine is following a phased path to legislation, beginning with a period of voluntary self-regulation in 2024-2025, which will be followed by the drafting and adoption of a full legislative framework harmonized with the EU's AI Act, expected to commence in 2026-2027.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

United Kingdom

Contacts

Paul O'Hare

Partner, Deloitte Legal UK

pohare@deloitte.co.uk

Luke Golding

Director, Deloitte Legal UK

lgolding@deloitte.co.uk

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

The Data (Use and Access) Act 2025

The Data (Use and Access) Act (DUAA) received Royal Assent and came into force on 19 June 2025, with a phased introduction of its provisions taking place between June 2025 and June 2026.

The DUAA introduces significant reforms to the UK's data protection framework, aiming to stimulate the growth of digital verification services and provide greater flexibility for certain data processing procedures. It amends key legislation, including the UK GDPR, the Data Protection Act 2018, and Privacy and Electronic Communications Regulations 2003.

Key changes to the existing UK data protection regulatory regime introduced by the DUAA include:

- **Subject access requests (SARs):** Organizations have been granted increased flexibility regarding SARs. The DUAA introduces a "stop the clock" mechanism, allowing organizations to pause the one-month response time if they require further information from the requestor or the payment of a fee (in cases where the request is manifestly unfounded or excessive). In addition, Article 15(1) UK GDPR has been amended to permit controllers to provide information based only on a 'reasonable and proportionate search'. The interpretation of 'reasonable and proportionate' is expected to be a subject of considerable debate.
- **Automated decision-making (ADM)**: Restrictions on the use of personal data in ADM have been relaxed. Organizations will gain greater flexibility to use personal data in ADM systems (i.e., by relying on legitimate interests, as opposed to gaining explicit consent) provided they implement certain safeguards. These safeguards include providing information about significant decisions made, enabling challenges to such decisions, and enabling human intervention. The previous, more restrictive, regime will continue to apply to high-risk ADM, such as that involving special category personal data.
- **Complaints procedures:** The DUAA introduces a new right for data subjects to complain if they are concerned that their rights under the UK GDPR have been infringed. Organizations are now required to establish procedures to handle complaints and to facilitate the making of complaints (including by making an electronic complaints form available).
- **Changes to the Information Commissioner's Office (ICO):** The DUAA introduces changes to the ICO, which is to be replaced with a new 'Information Commission.' This new body will adopt a revised structure intended to provide a more consensus-based decision-making model, replacing the single person-led authority with a board of directors and a chair. The restructure is expected to take place in 2027 and aims to align the Information Commission with other UK regulatory bodies.
- **Cookies:** Following the theme of flexibility, consent requirements for cookies are being relaxed where the privacy risk to users is low. This includes cookies used to obtain statistical information and cookies used to correctly display a website.
- **Recognized legitimate interests:** The DUAA has introduced "recognized legitimate interests," a non-exhaustive list of activities that may constitute a legitimate interest for processing personal data. Examples given include direct marketing (provided broader legal restrictions are also complied with), intra-group transmissions of personal data for administrative purposes, and ensuring the security of network and information systems.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant data protection updates?

EU-UK adequacy decision

The European Commission's adequacy decisions for the UK, covering the EU GDPR and the Law Enforcement Directive, are due to expire on 27 December 2025. However, recent developments suggest optimism for their renewal.

On 22 July 2025, the European Commission published two draft adequacy decisions indicating its view that the UK continues to ensure a level of protection for personal data that is essentially equivalent to European standards. These drafts propose extensions of the adequacy decisions until December 2031.

Subsequently, on 20 October 2025, the European Data Protection Board (EDPB) adopted opinions on the European Commission's two draft adequacy decisions. The EDPB's opinion was broadly approving of the UK's efforts to mirror EU data protection standards but requested that the European Commission further considers recent developments, including changes introduced by the Data (Use and Access) Act 2025 concerning cookies and the structure of the Information Commissioner's Office.

These developments indicate that, even with the introduction of The Data (Use and Access) Act 2025, the European Commission continues to view the UK's data protection standards as essentially equivalent to those in the EU. The adequacy decision, however, still requires approval from representatives of EU member states and formal adoption by the European Commission.

Video-sharing platform rules repealed: Online Safety Act 2023

The four-year regime for video-sharing platforms (VSPs) was repealed on 25 July 2025. This VSP regime had served as a temporary solution while the UK government implemented the new online safety regime. VSPs now fall under the broader scope of the Online Safety Act 2023.

UK government publishes final online safety priorities

On 2 July 2025, the UK government published its final statement of strategic priorities (SSP) for online safety, under the Online Safety Act 2023.

The SSP outlines the following key priorities:

- Implementing safety by design to proactively prevent harm;
- Increasing the transparency and accountability of online platforms;
- Maintaining regulatory agility to keep pace with changing technology and user behavior;
- Building an inclusive and resilient online society of well-informed users; and
- Supporting continued innovation in safety technologies.

The UK regulator, Ofcom, is required to have regard to the SSP when exercising its regulatory functions in the context of online safety.

Joint Committee on Human Rights and the Regulation of AI

On 25 July 2025, the House of Commons Joint Committee on Human Rights launched an inquiry into "Human Rights and the Regulation of AI." The inquiry's primary focus is to examine how AI may affect human rights and to assess whether additional legal frameworks are required. The inquiry also seeks to investigate:

- How AI can affect human rights, particularly concerning privacy, data protection, data usage, discrimination and bias; and
- The existing legal frameworks for the protection of human rights in the context of AI.

The deadline for feedback was 5 September 2025. The results of this inquiry are expected within the next few months.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Cyber Growth Action Plan 2025

The UK's cybersecurity sector is experiencing rapid growth, a trend commensurate with the escalating risk of risk of cyberthreats. To assist in addressing those risks, the University of Bristol and Imperial College London, commissioned by the government's Department for Science, Innovation and Technology, developed The Cyber Growth Action Plan and an accompanying roadmap. These initiatives aim to strengthen the UK's cybersecurity sector.

The plan's development was informed by 93 interviews conducted with a diverse group of stakeholders, including representatives from large technology vendors, cyber research scientists, and security technologists. The resulting recommendations are structured around three core pillars: culture, leadership, and places and include:

Culture

- **Support Growth journeys:** Government should review the incentives and validation routes available to cyber businesses, to make it easier for businesses to navigate the complexity of meeting cyber demand.
- **Stimulate informed demand:** Government and regulators should set high expectations for quality reporting of cybersecurity risks, consulting on mandatory use of cyber essentials and encouraging use of cyber insurance, to stimulate growth and the prioritization of cybersecurity.

Leadership

- **Appointment of a UK cyber growth leader:** This role would provide expertise and ensure accountability in driving the plan forward.
- **Appoint growth leaders in places of cyber strength:** Appointing place-based, industry-experienced leaders who can drive cyber growth initiatives and outcomes in key regions.
- **Expand the NCSC role:** Government should expand and appropriately resource the National Cyber Security (NCSC) to help drive cyber growth.

The role of places

- **Develop futures-oriented communities:** Place-based leaders should foster a community comprising CISOs, academia, industries and government to share experiences and perspectives on emerging cyber challenges across the UK.
- **Places to nurture distinct tech areas:** The UK should cultivate place-based cyber strengths, with each contributing to the overall success of cyber growth.
- **Places to provide safe environments:** Safe havens should be set up with infrastructure and data for stakeholders to explore, create and test solutions to cyber challenges.

The government is considering the plan and intends to respond formally in the publication of the next National Cyber Strategy. The strategy is set to be published before the end of 2025.

Codes of practice

In 2025 the UK government published:

- The '**Cyber Governance Code of Practice**,' a set of guidelines created to address cybersecurity risks. The code has been created by the government to support boards and directors in their governance of cybersecurity risks. It is complemented by the 'Cyber Governance Training' and the 'Cyber Security Toolkit for Boards,' both designed to assist board members and directors in implementing the Code effectively; and
- The '**Code of Practice for the Cyber Security of AI**.' Aimed at stakeholders across the AI ecosystem (including developers and system operators), the code was created to address the specific cybersecurity risks associated with AI systems. It sets out the security requirements for the entire AI lifecycle and is to be used by the European Telecommunications Standards Institute (ETSI) to help create a global standard for AI security.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant cybersecurity updates?

Governments response to ransomware consultation

On 22 July 2025, the government published its response to feedback received from a public consultation aimed at gathering opinions on potential legislation to tackle ransomware.

The consultation ran from 13 January to 8 April 2025, specifically seeking views on three legislative proposals:

1. **A targeted ban on ransomware payments** for all public sector bodies, including local government and Critical National Infrastructure (CNI) owners and operators;
2. **A ransomware payment prevention regime**, requiring all victims of ransomware to report and engage with relevant authorities, including the reporting of any intention to make a ransomware payment; and
3. **Creation of a ransomware incident reporting regime** which would include a mandatory reporting requirement.

More than 70% of survey respondents were in favor of the targeted ban on ransomware payments for public sector bodies, local government and CNI owners and operators. However, concerns were raised regarding potential exemptions to the ban and the widening of the ban to CNI and public sector supply chains. There was also positive feedback concerning a mandatory reporting system for ransomware incidents. Nevertheless, views were mixed on the effectiveness of a ransomware payment prevention regime, particularly given its requirement for victims to report their intention to make a payment.

Following the consultation, the government is expected to further develop the three proposals outlined above, clarifying any potential bans, proportionate penalties, and the most appropriate approach for supply chains.

Urgent advice from the UK government to leading UK companies on cybersecurity

On 13 October 2025, the UK government wrote to leading UK firms, including those listed in the FTSE100 and FTSE250, providing advice on how to enhance their security against the escalating threat of cyberattacks.

The letter outlined three suggestions to improve their resilience against cyberthreats:

1. Prioritizing cyber risk at Board level, utilizing the Cyber Governance Code of Practice;
2. Sign up to the NCSC's Early Warning service; and
3. Requiring Cyber Essentials within supply chains.

The letter underscored the increasing frequency and sophistication of cyberattacks in the UK as a growing concern. It concluded by promising that the forthcoming 'Cyber Security and Resilience Bill' will further strengthen protection against cyberattacks.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

AI regulation

Copyright and AI public consultation

The UK government conducted a public consultation on copyright and AI from December 2024 to February 2025, aimed at clarifying the application of current UK copyright laws to meet its objectives for driving AI innovation whilst protecting the rights of those in the creative industries. As part of its consultation, it proposed four potential approaches to dealing with the copyright issues arising from the use of copyrighted material by AI developers to train AI models:

- Do nothing and maintain the status quo: copyright and related laws remain as they are;
- Strengthen copyright by requiring the licensing of copyrighted material – in all cases;
- Introduce a broad data mining exception allowing data mining on copyright works – including for AI training – without the rights holder's permissions; and
- Introduce a broad data mining exemption allowing AI developers to train on material to the extent that rights holders have not expressly reserved their rights i.e., by opting-out of the use of their works (the option favored by the UK government).

Another key proposal was the removal of copyright protection for computer-generated works, (UK copyright law, unlike the laws of some other jurisdictions, allowing copyright protection for works generated solely by computers), and providing that the copyright is owned by the human who made the arrangements for the creation of the work.

After attracting over 11,000 responses to the consultation, including criticism from both AI developers and those in the creative industries, and failing to lead to any form of consensus, the UK government announced in July 2025 that it was adopting a 'fresh start' by establishing a number of expert working groups comprised of representatives from both the creative industries and the AI sector to drive forward practical and workable solutions to the use of copyrighted material by AI developers.

Private Member's Bills (PMBs)

The Public Authority Algorithmic and Automated Decision-Making Systems Bill (a PMB introduced to the House of Lords in September 2024) aims to regulate the use of automated and algorithmic tools in decision-making processes in the public sector. If enacted, it would require public authorities to complete an impact assessment of automated and algorithmic decision-making systems while ensuring the adoption of transparency standards for such systems. Its proposals include a potential prohibition on the use of these systems where their effective assessment or monitoring cannot, for practical reasons, be guaranteed. The PMB has undergone its third reading in the Lords but has yet to be scheduled for its first reading in the House of Commons.

Meanwhile, another PMB, the Artificial Intelligence (Regulations) Bill (originally tabled in the Lords during the 2023-2024 parliamentary session), was reintroduced to the House of Lords in March 2025. This PMB, which includes proposals for the establishment of an overarching regulatory body with wide-ranging powers to oversee the other sector-specific regulators in their approach to AI regulation, is now awaiting its second reading in the House of Lords.

While both PMBs are in their early stages, alongside repeated attempts by the Lords to table amendments to the Data (Use and Access) Act (as it made its way through the UK legislative process) to provide greater protection for copyright owners against AI developers, these PMBs underscore the continued lack of consensus between the two Houses of Parliament regarding the UK's current AI regulatory framework.

Regulatory guidance

Following a request by the government to do so, various UK regulators published their own AI strategic updates and guidance in 2024 (e.g., the Civil Aviation Authority's Artificial Intelligence Guidance).

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

What are the most relevant AI updates?

The AI Opportunities Action Plan

The "AI Opportunities Action Plan for the British Government" was launched in January 2025. It contains several high-level proposals to facilitate the government's aims of strengthening AI infrastructure across the UK, driving the cross-economy adoption of AI throughout the public and private sectors, and positioning the government as the best state partner for those building frontier AI. The plan specifically addresses the regulation of AI in the UK, stating that well designed and implemented regulation, alongside effective assurance tools, will drive the fast, widespread and safe development of AI. However, the plan also states that the UK's current 'pro-innovation approach' to regulation is a source of strength compared to that of other more regulated jurisdictions, and that the UK should be careful to preserve this. Following its launch the government has rolled out numerous additional AI-related policy initiatives, including:

- The AI Playbook: In February 2025, the previous public sector framework 'Generative AI Framework for HM Government' was replaced by the 'Artificial Intelligence (AI) Playbook,' which is intended to serve as an introduction to the use AI, covering its capabilities and limitations, how to use it safely, and how to buy and deploy AI solutions in government. It is aimed at a range of civil servants and public sector organizations, and builds upon ten common principles guiding the safe, responsible and effective use of AI.
- Memorandum of Understanding (MoU): Throughout 2025 the UK government entered into numerous MoUs to establish strategic partnerships with various AI actors, such as OpenAI (to collaborate on identifying opportunities for how advanced AI models can be deployed throughout the government and private sector) and with Anthropic (to explore the potential of advanced AI tools in improving how UK citizens access government information and services online). In September 2025, the UK and US also agreed an MoU regarding the "Technology Prosperity Deal," an initiative to promote greater collaboration in science and technology matters between the two countries. The first stated area of cooperation is 'Accelerating AI Innovation,' which aims to create transformational change across the economy. The focus areas for accelerating AI include:
    - Establishing joint flagship research initiatives between the US and UK;
    - Advancing innovation research and development approaches to accelerate the application of AI for science;
    - Catalyzing an AI for space partnership between US and UK space agencies;
    - Advancing pro-innovation AI policy framework;
    - Promoting US and UK AI exports (chips, data centers and models);
    - Developing the workforce and ensuring US and UK citizens benefit from AI opportunities across the supply chain; and
    - Advancing the partnership between the US for AI Standards and Innovation and the UK AI Security Institute towards a shared mission to promote secure AI innovation.
- AI blueprint (regulatory sandboxes): Following the launch in Spring 2024 of the Medicines and Healthcare products Regulatory Agency (MHRA) AI Airlock, a regulatory sandbox for AI as a Medical Device, the government unveiled in October 2025 its new blueprint for AI regulation, which includes plans to further explore how companies and innovators can test new AI products in regulatory sandboxes (essentially safe, controlled environments where individual regulations are temporarily 'switched off' or 'tweaked' for a limited period, to accelerate the responsible development and deployment of AI products). The initial intention is to set these up in key sectors such as healthcare, professional services and transport.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

The Data (Use and Access) Act 2025

Most of the provisions of the Data (Use and Access) Act 2025 (DUAA) will come into force by June 2026. This provides companies with sufficient time to update their policies and training to align with the Act before its full commencement. The UK government has released a four-stage roadmap for commencement.

Stage 1 and Stage 2 have already commenced. Stage 1 encompassed technical provisions, new statutory objectives for the ICO, and a government requirement to prepare a progress update and a report on AI systems and copyright works. Stage 2 focused on measures concerning digital verification services and included amendments to the Online Safety Act 2023. It also introduced requirements for Ofcom regarding the issuance of notices limiting the retention of information by social media providers in connection with the death of a child.

Stage 3 should commence in December 2025 and will include changes to data protection legislation. Stage 4 is anticipated in early 2026 and will involve work on the National Underground Register, the electronic system for registering births and deaths, changes to the ICO's governance structure, and measures requiring controllers to establish a process for handling complaints from data subjects.

AI and copyright reform

While it was making its way through the UK legislative process, DUAA was subject to repeated attempts by the House of Lords to table amendments to it to enhance protection for copyrighted works used by AI developers. While the government managed to resist the more substantive amendments proposed, the Act now compels the government to take concrete steps towards reforming UK copyright laws with respect to AI.

As a result, within nine months of DUAA coming into force, the government must prepare, publish, and lay before Parliament an assessment of the economic impact in the UK of the four policy options put forward in its Copyright and AI Consultation Paper of 2024. The document may also include an assessment of additional, alternative policy options to those proposed in the Consultation Paper but must include an assessment of the economic impact of each option on copyright owners, AI developers, and AI users.

Upcoming Cyber Security and Resilience Bill

Also on the horizon for 2026 is the Cyber Security and Resilience Bill, which is intended to enable the UK to keep pace with technological changes and reduce the number of cyberattacks in the UK. Recent attacks on the NHS, universities and local authorities have highlighted a weakness in the UK's cyber-defense infrastructure. Many UK companies can expect to be affected by the new cybersecurity framework, as the government plans to address cybersecurity vulnerabilities.

The Bill proposes mandatory incident reporting to give the government better insight into cyberattacks and expanding the resources available to regulators and the government, to enable them to better adapt to emerging threats. This includes a two-stage reporting system that requires companies and public sector organizations to inform their regulator and the National Cyber Security of any significant incidents within 24 hours of becoming aware of them. A second report should then be sent within 72 hours. These notifications should act as an early warning, bringing cybersecurity incidents to regulators much sooner than is current practice.

Additionally, as part of the Bill, the government is contemplating bringing data centers within scope of the NIS Regulations and providing additional powers for the Secretary of State. These new powers would allow the Secretary of State to issue directions to in-scope entities and regulators and publish a Statement of Strategic Priorities.

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Contributors

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Contributors

European Union	Ida Palombella | Pietro Boccaccini | Alessandro Amoroso | Valentina Forin | Fatima Dattena
Australia	Rachel Sciascia | Celeste Bennett
Austria	Sascha Jung | Christian Kern
Belgium	Matthias Vierstraete | Julie Van Com | Michaël Dours | Hind Salloum
Bulgaria	Miglena Micheva | Irena Koleva | Kristian Nemtsov
Chile	Ruby Soteras | Oliver Ortiz | Catalina Salas | Hernán Rodríguez
Colombia	Jose Luis Jerez | Andrés Felipe Salazar | Laura Nataly Forero
Costa Rica	Ricardo Güell | Estefanía Ramírez | Karla Chévez
Croatia	Zrinka Vrtarić | Ana Romić
Czechia	Jaroslava Kračúnová | Edita Bolková
Denmark	Jeanette Vallat | Simone Mai Flindt | Mia Holm Dietrich | Elvira Wolff-Sneedorff
El Salvador	Estuardo Paganini | Rita Camila Vega

France	Benjamin Balensi | Tony Baudot | Morgane Bourmault | Farah Agrebi | Laura Mallard
Germany	Nikola Werry | Jan Rudolph | Alina Scheja
Greece	Arianna Sekeri | Maria-Alexandra Papoutsi | Alexandra Sidiropoulou | Maria Lydakaki
Guatemala	Estuardo Paganini | Johana García Perdomo | Melissa Guerra Donis | Daniela Sánchez Pontaza
Hong Kong	Ven Tan | Kenneth Lee
Indonesia	Stefanus Brian Audyanto | Derryan Rahmat Putra | Nirmala Adisti Karunia | Ananda Rahma Olii
Italy	Ida Palombella | Pietro Boccaccini | Alessandro Amoroso | Valentina Forin | Fatima Dattena
Ivory Coast	Ursula Dutauziet | Audrey Allo-Ello | Nanga Balla Ouattara | Corine Anelone
Japan	Hiroshi Suga | Yosuke Araki | Ryo Hasegawa | Yusuke Tanahashi | Mizuho Inada
Luxembourg	Thomas Held | Sophie Brisson | Telma Da Palma
Malaysia	Ho Wei Lih | Rebecca Chong | Ong Xin Yi
Malta	Gianluca Busuttil | Michael Agius | Levente Bodi | Mireille Mangion

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

Contributors

Mexico	Mauricio Oropeza | Melissa Franco
Morocco	Grégoire Chaste | Amal Barhon | Juldrel Dudelvie Moudilou | Celmar Odcel Koubemba Nkoussou
Nigeria	Asiata Agboluaje | Inepaimi Ayah | Kemjika Igwe | Testimony Oluwadare
Norway	Bjørn Ofstad | Hanne Pernille Gulbrandsen | Eirin Helen Hauvik | Steinar Østmoe | Anniken Meuche Henriksen | Veronika Lundqvist
Peru	Jose Francisco Iturrizaga | Mariana Cordero
Poland	Monika Skocz | Kamila Mróz | Grzegorz Olszewski | Karol Juraszczyk | Marta Andrzejczyk-Karwicka | Paulina Szymańska
Portugal	Jacinto Moniz de Bettencourt | Joana Diniz Figueiredo | Madalena Pestana de Almeida | Mariana Teixeira Correia
Romania	Georgiana Singurel | Silvia Axinescu | Andreea Zaharia | Corina Damaschin | Denisa Pîrvu | Sebastian Maxiniuc
Serbia	Mirjana Mladenović | Igor Denčić | Luka Trifunović
Singapore	Joanna Yap | Gretchen Su
Slovenia	Ana Kastelec | Gregor Strojin | Klemen Kos | Nina Strmljan | Ema Burazer | Tjaša Mučič
Spain	Rodrigo González Ruiz | Carlos de Jorge | Nieves Fonseca de la Serna
Sweden	Michelle Smed | Julia Bergman
Switzerland	Paul de Blasi | Audrey Soutter | Elisabeth Zoe Everson | Aurélien Rocher | Nancy Nghemkap
Taiwan	Henry Tsai
Thailand	Niorn Yukolthong | Sutthika Ruchupan | Chanond Saicheua
The Netherlands	Sebastiaan ter Wee | Marlieke Bakker | Julie van Vliet | Rakeem Strijk
Turkey	Ceren Savaşçı | Mustafa İriboz
Ukraine	Dmytro Pavlenko | Anton Bychkov | Mykhailo Koliadintsev | Oleksii Voichyshyn | Anastasiia Kopylchak | Vasyl Chop
United Kingdom	Paul O'Hare | Luke Golding | Elizabeth Lumb | Jess Bridgewater
Deloitte Legal Center Of Excellence (CoE)	Ioana Niculae | Alexandra Biliuți | Julia-Maria Nedelcuț | Mihail Octavian Suciu

© 2025. For information, contact Deloitte Touche Tohmatsu Limited.

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

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

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our 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.

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.

© 2025. For information, contact Deloitte Global.