IAPP Global Legislative Predictions 2025

Argentina 🇦🇷

Contributor: Mariano Peruzzotti

Argentina is poised for continued legislative data protection and artificial intelligence developments throughout 2025.

Data protection is currently regulated under the Personal Data Protection Law, which dates to 2000. Since then, several legislative initiatives have sought to modernize this framework to keep pace with rapid technological developments and legislative trends around the world, especially as neighboring countries in the region enacted new data protection laws — like Brazil and Ecuador — or updated regulatory frameworks — Uruguay.

Argentina's Agency of Access to Public Information, which oversees enforcement of the Personal Data Protection Law, has proposed various bills aimed at replacing the existing data protection regime in recent years. While none of these bills were ever debated in Congress, discussions toward a new data protection regime could continue in 2025.

In 2023, Argentina officially joined the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108+ under the Council of Europe. Although Convention 108+ has been open for signatures since 2018, it has not yet entered into force. It requires ratification by at least 38 countries. The necessary threshold may be reached in 2025, enabling Convention 108+ to take effect. If so, Argentina and other signatories will likely prioritize aligning their national frameworks with the provisions set forth in the convention, driving reform efforts forward.

On the AI regulation front, various bills aiming to govern AI have been introduced in Argentina's Congress. Some are tailored to specific areas while others seek broader regulation, akin to the EU AI Act. Throughout 2024, the House of Representatives engaged stakeholders and experts in discussions to outline a regulatory framework for AI. This dialogue is expected to continue into 2025, with discussions and negotiations likely intensifying. Meanwhile, public agencies are anticipated to issue additional guidelines for AI use, building on the trend from recent years.

Back to Top ↑

Australia 🇦🇺

Contributor: Olga Ganopolsky

It should come as no surprise that the privacy landscape in Australia is predicted to continue to evolve in 2025. A series of incremental developments and trends, rather than one radical or deliberate overhaul of the privacy regime, are anticipated to drive this evolution. These primarily include reforms to the Privacy Act 1988, adoption of a proactive approach and enforcement posture by the Office of the Australian Information Commissioner, and emerging case law that impacts the scope of the right to privacy, a concept developed by Australian courts.

These drivers will be underpinned by consumer expectations and a growing recognition by individuals that privacy is a right, indeed a human right, that is worth protecting.

It is also important to note most Australian states have a state-based data protection regulator overseeing sizable sectors of the Australian economy, including state-run transport, health and education departments. State regulators will continue to be a source of important reforms, guidance and enforcement of privacy rights in their respective remits.

The same is true of the freedom of information regimes that will continue to inform many of the open data and government-led information sharing arrangements. For example, recent changes introduced under the Privacy and Responsible Information Sharing Bill in Western Australia have introduced updated definitions of personal information and deidentification, as well as a new obligation of "fair and reasonable" collection practices.

Privacy Act reforms

Reforms to the Privacy Act will proceed in tranches and in parallel to reforms in adjacent areas, such as creating cybersecurity legislation, reforming the Security of Critical Infrastructure Act 2018 and developing AI-related standards and industry-related codes.

The first tranche of reforms, introduced under the Privacy and Other Legislation Amendment Act 2024, as enacted 10 Dec. 2024, creates a new statutory tort for serious invasions of privacy. The tort-related provision will come into effect within six months of enactment, by June 2025. The new statutory tort is intended to cover egregious violations of privacy when the plaintiff has a "reasonable expectation of privacy in all of the circumstances" and the invasion by the defendant was intentional or reckless and serious. The statutory tort will be actionable without proof of damage.

The first tranche also introduces a new requirement to address automated decision-making in privacy notices. The automated decision-making requirement has a 24-month implementation or grace period and comes into effect 11 Dec. 2026.

This first tranche of reforms is effective immediately. These changes clarify organizations are to take "technical and organisational measures" and align language to requirements under the EU General Data Protection Regulation. They expand the powers of the OAIC to conduct inquiries, enter and inspect, and issue civil penalties to enforce breaches of the act, such as the power to issue compliance and infringement notices for acts and practices that amount to contraventions of notice requirements, the direct marketing provisions or privacy notice requirements.

These changes are in addition to measures that seek to simplify cross-border data transfers and measures introducing criminal offenses for doxxing.

The second tranche of reforms is anticipated to clarify the definition of personal information to address the Federal Court of Australia's finding addressing the meaning of "about" an individual. This will potentially expand the definition of personal information to cover types of technical information that may relate to the individual without identifying them.

These reforms are also likely to introduce a new obligation on regulated entities to handle personal information in a manner that is "fair and reasonable." The new standard will focus on a holistic approach by organizations in all stages of the data life cycle and will require organizations to be proactive about protecting privacy as part of broader data management frameworks.

The combination of these reforms will mean the Privacy Act will gain some of the features that are common to many comparable overseas data protection regimes and will remain largely technology neutral and principles based. In most privacy matters, the emphasis will be on transparency, notice and agency of individuals, rather than consent.

The obvious exceptions will be rights of more vulnerable individuals, such as children — the bill requires the OAIC to develop and register a Children's Online Privacy Code — and the handling of sensitive personal information, such as health-related information or forms of biometric data and biometric templates.

We are also likely to see further testing and challenges to the existing exemptions to the Privacy Act such as the employee records and small business exemptions with further targeted consultations on this aspect of the law and its operations.

Proactive OAIC

The OAIC is expected to take a more proactive approach focused on minimizing privacy harms by making more enforcement actions and issuing guidance. This approach will be enabled and further enhanced by the additional enforcement powers under the act's reform.

The OAIC will continue to play an active part in regulating data breaches and has stated its intent to take a "risk-based and harm-focused approach" and to take regulatory action in response to issues that create a risk of "substantial harm especially to vulnerable people and groups and that concern systemic harms or contraventions." Enforcement will be prioritized for matters with "educative or deterrent effect" and matters that clarify aspects of policy or law.

Several OAIC investigations and proceedings are currently before the Federal Court of Australia under the act's civil penalty provisions in response to sizable data breaches. Noting human error remains the second biggest source of serious data breaches, after cyberattacks and ransom demands, we anticipate that, in addition to security-related matters, enforcement will extend to a broad range of privacy-related organizational matters, such as policies, procedures and data management initiatives, including collection, minimization and deletion practices.

In October 2024, the OAIC issued guidance articulating how Australian privacy law applies to AI and set out its expectations. The guidance focuses on governance and promotes privacy in the context of emerging technologies and digital initiatives. Privacy Commissioner Carly Kind said, "Addressing privacy risks arising from AI, including the effects of powerful generative AI capabilities being increasingly accessible across the economy, is high among our priorities."

In November 2024, the OAIC issued guidance on using third-party tracking pixels on websites and use of biometrics. The emphasis on addressing privacy risks as part of new technologies and systemic matters is consistent with the OAIC's broader enforcement and regulatory action strategy.

The enforcement position taken by the OAIC will be informed and enhanced by an increased penalty regime introduced in 2022, which increased penalties for serious or repeated contravention to a maximum of AUD50 million, three times the value of any benefit obtained through the misuse of information, or 30% of a company's adjusted turnover in the relevant period.

We anticipate matters under investigation and potential settlement or agreed forms of resolution will command higher amounts, referencing the higher fines legislated under the 2022 reforms. For example, the OAIC settlement with Meta Platforms involves an AUD50 million payment program as part of an enforceable undertaking to settle the civil penalty proceedings brought by the OAIC against Meta. The program enables individuals to seek redress for harms suffered due to the This is Your Digital Life app.

Private litigation and case law

In October 2024, the County Court of Victoria awarded a plaintiff AUD30,000 in damages for invasion of privacy and AUD10,000 in damages for breach of confidence. Building on precedents, the court concluded "an action for invasion of privacy forms part of the common law of Australia. Although historically this action has been housed under the overarching doctrine of breach of confidence, it is better viewed as separate and distinct from the action."

Similar types of litigation are expected to follow by litigants aggrieved by publication or dissemination of information that is private for various reasons. As the court reiterated, this reinforces the current norms and expectations of a right to privacy as a distinct right.

As always, the common law will continue to evolve and develop and will gradually build a body of precedent and consistent practices on core issues, such as an expectation of privacy and the types of intrusions that constitute a breach.

Conclusion

Perhaps the key prediction for 2025 is that individuals will see privacy not only as an expectation but as a right — and one that deserves protection.

For privacy practitioners in Australia, this means some change but also continuity. While new rights and obligations must be addressed, practitioners will remain focused on governance and key practices like data minimization and deletion, building privacy by design and by default, and working with colleagues in cybersecurity and incident response teams to minimize data breaches and their impacts on individuals.

Back to Top ↑

Austria 🇦🇹

Contributor: Andreas Zavadil

In 2025, Austria will experience significant developments.

The Parliamentary Data Protection Committee will commence its activities at the beginning of the new year, marking the first time Austria will have two supervisory authorities instead of one.

The Parliamentary Data Protection Committee, established as a result of the Court of Justice of the European Union's ruling in Case C-33/22, will be responsible for the legislative domain and the processing of personal data within that context.

Additionally, in the fall of 2025, the new Freedom of Information Act will come into force, ensuring a constitutional right to access information from public institutions. This will have implications for data protection law, as the requested information may include personal data, which often requires a delicate balancing of interests.

Finally, the intersection between data protection and AI will become increasingly relevant at the national level, particularly since both the EU GDPR and the AI Act will be applicable in parallel. A pressing issue is the need to designate competent authorities for the AI Act, which has not yet been addressed.

Back to Top ↑

Belgium 🇧🇪

Contributor: Charles Helleputte

Before jumping into 2025, Belgium deserves praise for being the first to implement — with guidance from authorities and freely available assessment tools — the NIS2 Directive framework into national law.

Increased cyber resilience through improved accountability can only bring good vibes — even more when, for once, the country was the good student in the class. The same cannot necessarily be predicted regarding the identification of relevant authorities charged with enforcing the EU AI Act, as it seems this is as complicated and unsettled as forming the future Belgian federal government.

The Brussels bubble will spark in 2025, which could create many changes and uncertainties, starting with brand new European Commissioners in the digital field. The last Commission delivered a lot in the digital spaces, and those who are expecting the regulatory agenda to be put on hold — if only to give time to digest — might be disappointed. There are signs of new initiatives to come, whether in the enforcement space — who said there will never be central enforcement of the GDPR — or through further nonprivacy-specific regulations impacting privacy. Yes, consumer protection seems high on that agenda.

The futures of two adequacy decisions are uncertain. Will the EU-U.S. Data Privacy Framework survive the possible overhaul of the U.S. surveillance system that might come with the new administration? And what about changes to the U.K. privacy regime that seem to be on the horizon?

If business is about taking risks and managing uncertainties and turbulence, then 2025 promises to be very successful.

Back to Top ↑

Bermuda 🇧🇲

Contributor: Nancy Volesky

"Bring in the new" was never more true than it was 1 Jan. 2025, when Bermuda's privacy regime with the complete Personal Information Protection Act 2016 fully came into force. Certain 2024 initiatives to support the objective of a privacy regime that meets best practice will carry on.

The government of Bermuda proceeded with its legislative harmonization efforts in 2024. These included regulations for transitional provisions related to personal information requests under the 2010 Public Access to Information Act, in progress prior to the act's implementation. Preparations were also made for transitional provisions for the Electronic Transactions Act 1999, while its amendments to continue to be dealt with.

Cybersecurity remains a priority for Bermuda's government. The Computer Misuse Act and the Cybersecurity Act both passed in 2024, and the government plans to update its cybercrime legislation to align with the Budapest Convention on Cybercrime.

AI has been readily adopted within certain sectors, but there are no regulatory initiatives on the horizon yet. An election will take place this year, which may bring in new priorities and measures.

The Office of the Privacy Commissioner for Bermuda now turns to enforcement and corrective action. Promoting privacy rights will be a mainstay, as will issuing further guidance such as for overseas transfers. AI and developments in privacy risk are also being monitored.

Although PrivCom previously recognized the APEC Cross-Border Privacy Rules as one certification mechanism for transfers, Bermuda joined the Global Cross-Border Privacy Rules Forum, which replaced the APEC CBPRs, as an associate member with PrivCom as the country's designated privacy enforcement authority to facilitate cross-border enforcement of data protection and privacy laws. Full membership would grant Bermuda mutual recognition as a trusted jurisdiction for privacy.

Back to Top ↑

Bolivia 🇧🇴

Contributor: Ana Valeria Escobar

Bolivia is still in the process of developing a comprehensive data protection framework, which will be essential for enhancing the country's data privacy and protection standards.

At least two legislative proposals are currently aimed at addressing this issue. Over the past year, these proposals have been actively discussed and promoted. The Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación's draft regulation is likely to shape the future of privacy regulations in Bolivia. There is also a possibility some components of the draft may be implemented through an executive decree, rather than through traditional legislative processes.

The AGETIC's proposal aligns with the EU GDPR. It includes a requirement for data controllers or processors not based in Bolivia to establish a legal representative within the country, extraterritorial application, personal data protection authority, and a mandate to register data databases. These provisions are expected to remain in effect regardless of whether the final regulation is enacted as a law or a decree.

Given the increasing regional and global pressure for enhanced privacy protections, it is likely Bolivia will introduce some form of regulation soon. However, with national elections approaching next year, substantial developments may not occur until 2026.

Back to Top ↑

Brazil

Contributor: Guilherme Peretti

In Congress, Bill 2338/23, which seeks to regulate AI in Brazil, will take center stage in 2025. During 2024, the bill saw 14 public audiences promoted by the Senate's Temporary Committee on AI and was approved by the Senate Plenary 10 Dec.

In 2025, it will be analyzed by the House of Representatives and, if the House makes changes to the text, will go back to the Senate for analysis before it can become law.

The version of the bill as approved by the Senate establishes a national system for AI regulation and governance, coordinated by Brazil's DPA, the Autoridade Nacional de Proteção de Dados. It defines AI systems similarly to the EU AI Act and adopts a risk-based approach: AI systems deemed to pose excessive risk would be prohibited, while high-risk systems would be subject to specific obligations for providers and deployers.

Also under congressional review, though with less attention, is Bill 522/22, which aims to amend Brazil's General Data Protection Law to define neural data and regulate its protection.

The ANPD's message to the Ministry of Justice and Public Security — detailing 2024 activities and 2025 projections — along with statements from board members at an event celebrating its four-year operational anniversary, offers insights into expected regulatory activities.

The ANPD's regulatory agenda for 2025-26, which takes a phased approach, prioritizes 10 unresolved themes from the previous cycle, including data subject rights, data protection impact assessments and AI, and incorporates new themes, such as personal data aggregators, sensitive and health data, and lawful bases for processing and consent. It also includes guidelines for the LGPD. For the guidelines, the ANPD will draw on the resources provided by its advisory body, the National Data Protection and Privacy Council, whose working groups are expected to complete their deliverables in early 2025.

Finally, following the 2024 release of its regulation on international data transfers, the ANPD is anticipated to begin identifying adequate countries for data transfers, with a focus on reciprocal recognition with the European Commission.

Back to Top ↑

Bulgaria

Contributor: Irena Koleva

In recent years, Bulgaria's Commission for Personal Data Protection has outlined the requirements for accreditation of certification bodies and bodies monitoring codes of conduct as an area of focus. The requirements are expected to be adopted in 2025 to finalize the national legal framework on accreditation.

A new CPDP strategy is also expected through 2029. It should identify priorities for development in the areas of the protection of personal data and the protection of whistleblowers.

The Bulgarian law transposing the EU Whistleblowing Directive was adopted in 2023 and has already been amended several times. New amendments are yet to come; they were submitted to Parliament in mid-2024 and are still pending.

Cybersecurity is another area in which changes are expected. A new draft law on cybersecurity, transposing the NIS2 Directive, is in the legislative process. The Digital Operational Resilience Act will also influence organizations' cybersecurity strategies, requiring financial services entities to comply by 17 Jan. 2025.

Bulgaria is currently in the process of transposing the EU Representative Actions Directive, which establishes requirements with respect to collective actions on various topics, including data protection. Also, progress is anticipated around the implementation of national measures for the EU Digital Services Act and AI Act.

Last but not least, we will continue to see decisions from the CJEU, issued on preliminary ruling requests from Bulgarian courts.

Back to Top ↑

Canada

Contributor: Shaun Brown

Canada's federal privacy law reform will probably be pushed down the road in 2025. Bill C-27, which would replace Part 1 of the federal Personal Information Protection and Electronic Documents Act with the Consumer Privacy Protection Act and create the AI and Data Act, was introduced in June 2022.

While the bill has made some movement through the legislative process — it is currently before the Standing Committee on Industry and Technology for review — its passage is doubtful with a federal election coming in 2025. And regardless of which government is formed, as a new government is expected, privacy legislation is unlikely to be an immediate priority.

The government of Alberta recently announced plans to overhaul its public sector privacy and access regimes. The Protection of Privacy Act, Bill 33, and the Access to Information Act, Bill 34, would replace the Freedom of Information and Protection of Privacy Act, which has been in effect since 1995. Bill 33 would introduce several notable changes for public bodies, including requirements to implement privacy management programs, conduct privacy impact assessments and report privacy breaches. The bill also provides for penalties of up to CAD1 million. With a majority government, these bills seem likely to pass in 2025.

Between sweeping amendments to the Act respecting Access to documents held by public bodies and the Protection of personal information and the Act respecting the protection of personal information in the private sector, in addition to the Act respecting health and social services information coming into force, Quebec's privacy landscape has undergone a significant transformation in recent years. It will now be important to watch for the first enforcement actions resulting from these changes, with a newly announced president in charge of the Commission d'accès à l'information.

Back to Top ↑

Chile

Contributors: Annalena Fuchs, Javiera Sepulveda

Following approval of the Personal Data Protection Bill by the National Congress and the Constitutional Court of Chile's ruling declaring the provisions under review to be constitutional, Chile should enter 2025 with a new legal framework that completely modifies the current local data protection regulations, closely following the EU GPDR. However, despite this important step, we must remain patient, as its promulgation and publication are still pending, after which there will be a two-year legal vacancy.

The situation is similar regarding cybersecurity. With the new Cybersecurity Framework Law approved and published, the necessary regulations defining, among other aspects, the law's effective date — which will be no less than six months from the publication of the regulation — are still pending.

Regarding AI, the government introduced a bill to regulate the use of AI and create a Technical Advisory Council for AI, using the EU AI Act and UNESCO's recommendations on AI ethics as references. The project is currently in the first of three constitutional procedures.

In the financial technology industry regulation area, the Financial Market Commission issued specific regulations in 2024 regarding the open finance system, and technical groups are currently being formed for its implementation, which is scheduled for mid-2026.

Also set to come into force in 2026 is Law No. 21.680, which establishes a consolidated debt registry. Among other things, the law seeks to strengthen the protection of debt data, establish the right to be forgotten in financial matters and introduce certain information security obligations.

Thus, 2025 is anticipated to be marked by intense preparatory activity for the implementation of these laws.

Back to Top ↑

China 🇨🇳

Contributor: Barbara Li

2025 promises to be another dynamic year for data protection, privacy, AI, cybersecurity and digitalization in China. Several important laws, regulations and local rules will be issued or become effective in 2025.

The Regulations on Network Data Security Management, set to be enforced 1 Jan., are a pivotal set of rules for implementing China's Cybersecurity, Data Security and Personal Information Protection Laws. These regulations not only outline detailed and comprehensive compliance requirements for businesses but also serve as a crucial reference for regulators in enforcement actions.

In 2024, the Cyberspace Administration of China, the key regulator in charge of data and cybersecurity matters, passed an important rule to ease China's cross-border data transfer requirements, which is hugely welcome by businesses. Besides, the local authorities in China's multiple free trade zones, especially in Beijing, Shanghai, Tianjin and Hainan, are authorized to explore further relaxed schemes for outward data flows by passing local rules. More regulatory sandboxes are anticipated to be issued by the free trade zones in 2025.

The Great Bay Area in China consists of Hong Kong, Macau and Shenzhen, Guangzhou, and seven other cities in the Guangdong province. These cities have been authorized to pilot schemes aimed at promoting data flows within the GBA. In November 2024, data regulators in mainland China, Hong Kong and Macau issued industry guidelines and best practices on standard contractual clauses and certification schemes. Regulatory developments in the GBA are expected to be a key focus in 2025, with detailed measures to streamline data transfers across the region anticipated.

How to determine important data and critical information infrastructure has been a challenging issue for international and Chinese businesses, given the lack of detailed guidelines. Starting in the second half of 2024, Chinese data regulators at national, local and industry levels have made significant efforts in drafting rules, catalogues and guidelines on important data and CII. More guidance and clarity on these issues is expected in 2025 because some of those rules, catalogues and guidelines are close to finalization.

Since 2023, China has adopted several regulations on generative AI, deepfakes and algorithms, and in 2024, regulators started enforcement against noncompliant AI activities. Drafting a comprehensive AI law has been included in the work plan of China's top legislature, and we expect the first draft of China's AI law may be issued for public consultation in 2025.

In addition, China's courts have been spearheading tackling cutting-edge AI legal issues by passing landmark court rulings about hot AI topics such as copyrightability of AI-generated content, how to protect personal data in AI training datasets and internet platforms' watchdog responsibility for AI products. The Beijing and Guangzhou Internet Courts are not shy about ruling on emerging AI issues, and we expect more AI court rulings will come out to shape China's AI judicial landscape.

With data being identified as a "new productive force" by the government, China is actively promoting the digital economy and unlocking the value of data assets. Established in 2023, the National Data Bureau is a key player in this initiative, issuing regulations and policies that encourage better use of public and enterprise data. This proactive approach is expected to continue, with more regulations and policies aimed at promoting and leveraging the use of data assets, presenting potential opportunities for businesses.

According to the China Academy of Information and Communications Technology, China will become one of the largest data powerhouses in the world by 2025. Data security, cybersecurity and the protection of personal information are high on the priority list of Chinese regulators. In 2024, Chinese regulators including the CAC, the Ministry of Information Technology and Industry, the Ministry of Public Security, the State Administration of Market Regulation and industry authorities conducted multiple rounds of large-scale investigations and imposed high penalties on violators.

It is anticipated that in 2025, regulators will continue to stay active in enforcement, and mobile apps, consumer goods, hospitality, financial, health care and transportation industries will be key areas of focus for regulatory enforcement.

Back to Top ↑

Colombia 🇨🇴

Contributor: Luis Alberto Montezuma

In 2024, Colombia's DPA, the Superintendencia de Industria y Comercio, issued two circulars.

Circular 002/2024 sets instructions on the processing of personal data in AI tools in line with Colombia's Law 1581 of 2012, the country's data protection law, and Law 1266 of 2008, its credit reporting law. In the circular, the SIC suggests organizations and boards of directors should carefully consider the principles of proportionality, necessity, reasonableness and suitability when processing personal data through AI tools. As a matter of safeguards, the SIC recommends implementing accountability measures like PIAs and applying the principles of privacy by design and by default. If risks cannot be mitigated, the SIC suggests refraining from processing personal data.

In addition to emphasizing that personal data must be as accurate, complete and up to date as is necessary for purposes for which it is to be used, and that privacy rights must be ensured by organizations when using personal data through AI technologies, the SIC stresses that Law 1581 does not generally allow organizations to use publicly available data just because it is public.

Circular 003/2024 held that boards of directors are considered joint controllers with respect to the processing of personal data by their organizations, meaning they can be held personally liable, in addition to the organization itself, for breaching Law 1581. The SIC also clarifies that board members remain accountable for implementing and assessing the effectiveness of the organization's privacy program.

Although Circular 003 is still to be read only as soft law, industry representatives and stakeholders have raised concerns about the interpretation of joint controllers, as this definition is not contemplated in the law.

The SIC announced it would introduce a bill to modify the current Law 1581, inspired by the EU's Data

Protection Directive. Congresswoman Maria Fernanda Carrascal reintroduced Bill 152/2024C to enact a personal data protection regime. The bill would impose new requirements, including instituting the legitimate interest assessments and DPIAs. It would also update requirements around tracking technologies, AI and automated decision-making. The bill was referred for further consideration to the Standing Committee on Constitution of the Chamber of Representatives, which published its report 29 Nov. 2024. The report has not yet been tabled for debate and discussion by the committee.

Finally, the SIC opened an investigation into Worldcoin to determine if its collection of biometric data complies with Law 1581.

Back to Top ↑

Costa Rica

Contributor: Daniel Rodriguez Maffioli

The legislative landscape for data regulation in Costa Rica appears particularly promising for 2025, especially regarding data protection reform.

The Personal Data Protection Law, Bill No. 23097, is now positioned for its first plenary debate and shows strong potential for approval in the first quarter of 2025. With apparent consensus among legislative factions, this GDPR-aligned legislation would modernize Costa Rica's data protection framework, with implementation expected in 2026.

This development coincides with increased enforcement activity and involvement by the Costa Rica's DPA, the Agencia de Protección de Datos de los Habitantes. Notably, PRODHAB has been participating in health record interoperability projects that would establish specific obligations for health data management if implemented.

The Cybersecurity Law of Costa Rica, Bill No. 23292, which was initially prompted by the 2022 government cyberattacks, continues its evolution through expert consultation. While progress was measured in 2024, the bill's scope may expand beyond public sector governance to include critical infrastructure providers from both private and public sectors. New provisions could establish incident reporting requirements and enhanced data protection obligations for these entities.

The AI regulatory landscape has become more complex with multiple competing initiatives. While the Law for the Regulation of Artificial Intelligence, Bill 23771, progressed with a revised text under Technology Committee review, 2024 saw the introduction of the draft Law for the Implementation of Artificial Intelligence Systems, file No. 24484, focusing on copyright protection in AI training and data protection requirements for AI systems. However, given the technical complexity and overlapping proposals, the approval of any AI-specific legislation in 2025 appears unlikely.

The year 2025 is expected to be transformative for Costa Rica's digital regulatory framework, particularly in data protection and cybersecurity, while AI regulation continues to mature through legislative deliberation.

Back to Top ↑

Croatia

Contributor: Krunoslav Smolcic

In 2025, Croatia's data privacy framework is set for transformative changes as new regulations impose stricter controls on employee data handling and introduce EU-wide standards on industrial data access. These developments will require Croatian organizations to implement more robust data management practices, particularly within human resources and compliance departments, to meet rising privacy expectations.

As of 1 Oct. 2024, the Regulation on the Content and Method of Keeping Records of Workers Employed by the Employer implements stricter data storage limitations for employee records. The ordinance establishes clear retention timelines, requiring records to be kept only as long as necessary with a maximum retention period of six years after employment termination, unless specific legislation dictates otherwise. Unlike previous regulations, this ordinance specifies retention periods to eliminate inconsistencies and enforce uniform practices across employee data management, including for temporary workers, interns and contractors.

The new ordinance mandates stricter data protection measures, requiring employers to establish robust access controls for sensitive personal information. Noncompliance will result in significantly higher fines than those imposed by previous ordinances, highlighting a new approach that encourages proactive adherence to regulations. Additionally, the ordinance stresses the importance of securely deleting or archiving records once they are no longer needed, thus protecting employees from potential data misuse.

The EU Data Act, effective January 2024 and applicable beginning September 2025, establishes EU-wide standards for accessing and processing industrial data. Aimed at boosting competitiveness, it sets clear rules for data use across industries, including AI, enhancing user control and transparency.

In light of these regulations, Croatia's Personal Data Protection Agency is expected to increase inspections, particularly for organizations using innovative technologies or processing large amounts of data. Compliance with the new employee data ordinance will be crucial to avoid fines and maintain trust.

These changes present an important opportunity for Croatian organizations to adapt their data practices, strengthen governance and improve compliance.

Back to Top ↑

Cyprus

Contributor: Christos Makedonas

As Cyprus enters 2025, the regulatory landscape for data protection and cybersecurity is becoming increasingly complex, with significant changes on the horizon.

Organizations across various sectors are ramping up efforts to ensure compliance, driven by new and overlapping regulations. An emerging key trend is the growing number of organizations appointing data protection officers as the importance of managing personal data continues to expand across industries.

The EU DORA, which entered into force in January 2023 and applies as of 17 Jan. 2025, will profoundly impact financial services in Cyprus. Banks, investment firms, insurance companies and payment institutions will need to adhere to stringent new cybersecurity and resilience requirements. The DORA aims to ensure financial institutions can withstand, recover from and adapt to cyberthreats and disruptions. The regulation mandates robust governance frameworks, comprehensive incident reporting and operational resilience testing. Failure to comply with the DORA will not only expose organizations to penalties but also erode trust in the financial system.

Beyond the financial sector, the NIS2 Directive will extend its influence to other industries that are critical to national infrastructure, including energy, health care, transportation, telecommunications and water supply. The directive significantly broadens the scope of the previous NIS Directive, placing higher security and risk management obligations on operators of essential services and digital service providers. Organizations in these industries will need to adopt stronger cybersecurity measures, improve incident response capabilities and ensure third-party risk management. This expanded scope creates a new layer of complexity as industries beyond finance face more intense regulatory scrutiny.

The overlap between the DORA and NIS2 presents a major challenge for professionals in the fields of compliance, cybersecurity, risk management and data protection. Compliance teams, chief information security officers and DPOs are now faced with navigating a web of regulations, each with its own requirements and deadlines. Both frameworks demand a high level of vigilance in protecting data and systems, but the intricacies of implementing and managing compliance for multiple overlapping regulations can be overwhelming. Organizations must find ways to streamline their efforts without sacrificing security or compliance integrity.

This is where the need for compliance digitization becomes critical. As regulations evolve, it is becoming increasingly clear that manual processes and outdated systems are no longer sufficient to meet the stringent and often overlapping demands of the DORA, NIS2 and other frameworks like the EU AI Act. Automated compliance solutions will allow organizations to track regulatory changes in real time, perform continuous risk assessments, manage third-party risks and generate reports more efficiently. The shift towards digitization in compliance is not only a strategic advantage but also a necessity for organizations to avoid hefty penalties and reputational damage.

Moreover, the regulatory complexity is leading to a greater need for interdepartmental collaboration. Compliance teams, CISOs, DPOs and risk management professionals must work closely together to ensure a unified approach to cybersecurity and data protection. The convergence of these roles highlights the increasing integration between data protection, cybersecurity and operational resilience, with professionals now expected to manage risks holistically rather than in isolated silos.

In addition to the pressures from the DORA and NIS2, the AI Act will further reshape the regulatory environment. As AI becomes a more central component of business processes across industries, the act has introduced new compliance obligations aimed at ensuring transparency, accountability and ethical use of AI systems. Organizations in sectors like finance, health care and manufacturing will need to audit their AI tools and processes to ensure they comply with these emerging standards. This adds yet another layer of complexity to an already burdened compliance landscape.

Finally, the Digital Security Authority in Cyprus is expected to play a crucial role in 2025 by continuing its awareness campaigns, training programs and collaborative efforts to bolster national cybersecurity. These activities are particularly timely given the rapid pace of regulatory changes and the increasing threat landscape.

A pivotal year for Cyprus, 2025 will contend with a wave of new regulations that significantly overlap, creating both challenges and opportunities. The need for compliance digitization and the integration of cybersecurity, data protection and risk management efforts will be paramount. Organizations that can successfully adapt to these changes will not only strengthen their resilience but also gain a competitive advantage in an increasingly regulated digital environment.

Back to Top ↑

Czech Republic 🇨🇿

Contributor: František Nonnemann

Cybersecurity, new data regulation and critical infrastructure will be key legislative topics in the Czech Republic next year.

Two key EU directives, the NIS2 Directive on measures for a high common level of cybersecurity across the EU and the Critical Entities Resilience Directive, should be transposed in the Czech Republic by 2025 at the latest. These directives broaden the scope of entities obliged to systematically address cybersecurity, operational resilience, and availability of critical and important services, including public administrative, financial industry, health care, energy, telecommunications, food distribution, information and communications technology services.

In this context, new rules for supply chain management are also a big issue, including the ability of the public sector, either the cybersecurity authority or the government, to ban the use of a particular risky supplier by regulated entities.

Implementation of the new EU data regulations — the Data Act, Data Governance Act and others — is another important topic. It will be necessary to specify the role of individual regulators and supervisory authorities and the link to other regulations at the level of Czech legislation, including the EU GDPR and national laws regulating personal data processing.

There are also several proposals in the national legislative process that specify or tighten the rules for certain types of direct marketing. In 2022, an opt-in consent requirement for marketing cookies and telemarketing was explicitly introduced into Czech law. A proposal to increase fines for unsolicited commercial communications or spam from the current CZK10 million, approximately 400,000 euros, to 20 million euros or 4% of the annual turnover of a group of companies is now under discussion.

In 2024, the Czech Republic's DPA, Úřad pro ochranu osobních údajů, issued several methodological guidelines mainly on the use of closed-circuit television systems from the GDPR perspective, and on the position of DPOs. Unfortunately, the DPA does not publish a working plan for the upcoming period, so it is not possible to indicate whether and what other soft law documents it will publish in 2025.

Back to Top ↑

Denmark 🇩🇰

Contributor: Niels Torm

There is a growing focus on privacy both in the private and the public sector in Denmark. Denmark's DPA, Datatilsynet, issued several different rulings in 2024 around the topic of data minimization. In a few situations more data than necessary was collected and stored by apps or via online accounts, leading to the Datatilsynet's rulings to stop the unnecessary data collection.

Throughout 2024 there was a growing focus on online media and shopping platforms — especially those originating in China and the U.S. Authorities are expected to focus even more on the data that is collected and processed. And with the emerging use of AI and AI-like technologies, the challenges around protecting the privacy of especially online users seems to be getting even more in focus for authorities.

With a raise in fraud and online scams, the importance of protecting personal information from being spread uncontrolled has become even more relevant. Throughout Danish society there is a growing realization that emerging technologies not only provide new and interesting opportunities, but also bring a higher risk to personal safety and integrity.

Based on developments in 2024, I expect there will be an even higher focus on the protection of personal information in 2025 than Denmark has seen before, mainly driven by the emergence of AI-driven apps and opportunities. I do not expect new and updated legislation; however, authorities will likely be more proactive in their approaches to upholding current regulations.

In general, more people have realized the importance of keeping their personal information safeguarded, and this development will continue in 2025.

Back to Top ↑

Ecuador 🇪🇨

Contributor: Pedro Cordova

As Ecuador's DPA, the Superintendency of Data Protection, took office, significant normative and regulatory progress was seen. This is expected to continue in 2025.

Strengthening of the DPAs functions, increasing audits and actions toward data controllers and processors, as well as a bigger scope for the concepts and procedures established in current legislation, and regulating data handling through emerging technologies is anticipated.

By the end of 2024, the DPA initiated its first administrative investigations against companies for alleged data security breaches. For 2025, these actions, audits and controls will intensify. Therefore, domestic and foreign companies that process personal data of Ecuadorians must evaluate the legal, technical and physical measures they have implemented to avoid sanctions.

The DPA is also expected to issue the first resolutions declaring which countries, organizations and companies have adequate levels of protection for the international transfer of personal data. It will also establish standard clauses and legal instruments and approve contractual clauses that offer sufficient guarantees approved by the DPA.

Several pieces of legislation regarding AI are currently on the National Assembly's agenda, aiming to ensure greater protection of citizens' data privacy.

At least one piece of AI-related legislation is expected to be issued in 2025. It likely refers to the applicable technologies and limitations of their use, as well as the handling of data, especially by international companies, and reinforcing security measure requirements.

Back to Top ↑

El Salvador

Contributor: Laura Hernandez

El Salvador's Data Protection Law, approved in November 2024 by Decree No. 144, regulates the processing of personal data in El Salvador for individuals and public or private legal entities.

It establishes basic rights such as data access, rectification, cancellation, opposition, portability, erasure and limitation, which protect privacy and guarantee control over personal information. Companies are required to implement effective mechanisms so data owners can exercise these rights. In addition, the law imposes obligations such as obtaining informed consent, appointing data protection delegates, notifying security breaches within 72 hours and implementing internal procedures for international data transfers through appropriate legal mechanisms.

The deadline to comply with legal requirements ends in May 2025, pointing to the need to review internal policies, train staff, update technological systems and be transparent with users about the treatment of their data.

The State Cybersecurity Agency was created to monitor compliance with the law. Failure to comply with legal measures entails significant sanctions, including fines, corrective measures and even notification of the competent authority in the event of a violation related to the handling of personal data.

Concerns have been raised about possible abuses in application of the law, particularly concerning the exercise of the right to be forgotten or the deletion of data, which could become a tool for censorship or restriction of freedom of expression, freedom of the press and access to information if the rights and interests at stake are not adequately assessed.

In short, this legislation represents a significant advancement in the protection of privacy and personal data but poses challenges in its effective implementation and respect of other fundamental rights.

Back to Top ↑

European Union

Contributor: Isabelle Roccia

The new EU term kicked off last fall. The new European Commission structure may create coordination challenges across policy initiatives and implementation. A more right-leaning European Parliament may influence policy shaping regarding sovereignty, industrial policy and fundamental rights.

More initiatives impacting digital responsibility are coming, adding to the existing thick "blue wall" of regulation. The Digital Fairness Act will focus on strengthening consumer rights and addressing newer areas such as dark patterns and addictive design. Cybersecurity will remain a priority through initiatives on cyberbullying, software resilience and specific sectors, such as health care.

The Commission will further build the EU AI Act framework by addressing intersections with copyright, liability and possibly AI in the employment context, amid plans to boost infrastructure and investment. It will also seek to finalize legacy proposals across data sharing, law enforcement and GDPR enforcement.

International data transfers will remain high on the Commission's strategic agenda as it discusses adequacy arrangements with several jurisdictions, including Brazil, and monitors developments in the U.K. and the U.S.

Pressure may also mount on the EU to address data transfers to jurisdictions that do not share the same democratic values. The upcoming decision by Ireland's Data Protection Commission regarding TikTok's data transfers to China may trigger a broader EU response.

Many transformative texts for digital governance were adopted during the previous mandate — the Data Governance Act, the AI Act, the NIS2 Directive, the DORA and the Data Act — and have yet to be implemented by organizations.

The main challenge for professionals and regulators alike will be to make sense of it all. Organizing the patchwork of regulatory agencies involved in digital governance — over 270 already across Europe — will take time and may mean haphazard guidance as organizations face a increasingly complex framework.

Will the Brussels effect remain? The EU has successfully exported its regulatory model for years. A lot of big players that weren't visible at the time of the EU GDPR are now proposing alternative models. It will be interesting to watch how that plays out, where global conversations are happening and how the EU project continues to resonate — or not.

Back to Top ↑

Finland

Contributor: Eija Warma-Lehtinen

Finland's DPA, the Office of the Data Protection Ombudsman, has an interesting and busy year ahead. Complaints have increased during recent years and the DPA has renewed the organization to better respond to such volume.

The EU's digital package and its national implementation is very much a focus for the DPA and the need to ensure consistent enforcement not only with the AI Act but also with cybersecurity regulation is pivotal. Hopefully the DPA's budget will be increased.

The importance of children has been another focus area for the DPA. Along with the TIEKE Finnish Information Society Development Centre, it recently published the outcome of an EU-funded project GDPR4CHLDRN. The two-year-project aimed to facilitate protection of children's data. Finland's DPA will continue to keep children in focus in the coming year.

Finland's government is reviewing national data protection laws to enhance the mobility of personal data and appropriate use of cloud services among other things. One extremely interesting area is the need for administrative fines of public sector organizations. It is a widely discussed topic, and the DPA considers it would be important to advance this possibility.

Back to Top ↑

France 🇫🇷

Contributor: Cécile Martin

Each year, France's DPA, the Commission nationale de l'informatique et des libertés, defines topics of high public interest and its priority investigations.

As expected, the CNIL plans to focus mainly on two major concerns in 2025, one being the hot topic of minors' data being collected online through applications such as social networks, dating sites and online gaming platforms. This is given the high risks potentially raised by the massive collection of data related to minors' identities, preferences and lifestyles.

To ensure data controllers are complying with obligations, the CNIL is checking use of age control mechanisms, implementation of security measures and respect of the data minimization principle.

The CNIL's second area of focus is data subjects' right of access, the European Data Protection Board's 2024 Coordinated Enforcement Framework action. The CNIL is joining other DPAs in investigating compliance with this right by data controllers.

According to the CNIL, the goal is to harmonize effective application of the EU GDPR and coordination between supervisory authorities to enable a better understanding of this right.

AI is, of course, another point of attention after the 12 July 2024 publication of the EU AI Act — the first general AI legislation in the world. The CNIL published a booklet on the topic, based mainly on the development of privacy-friendly AI, the support of innovative players and the audit of the existing systems to protect data subjects.

Companies' application of the AI Act, especially regarding human resources and recruitment or evaluation of candidates and employees, will undoubtedly be one of the major issues in years to come.

Back to Top ↑

Germany 🇩🇪

Contributor: Ulrich Baumgartner

In 2025, Germany is expected to see notable developments in data protection law, both through national updates and the implementation of new European frameworks.

Key anticipated changes include a new dedicated Employee Data Protection Act, for which a draft bill was provided for interministerial coordination in October. Based on the broad opening clause in Article 88(1) of the EU GDPR, the law aims to clarify the GDPR's application in employment settings, providing clearer rules and legal certainty for employers while enhancing data protection for employees.

It specifies data processing in the context of employment relationships, for example by establishing that the dependency of the employee is a key factor when determining the necessity of data processing or whether consent by employees is provided voluntarily. The draft further specifies requirements for consent and conditions in which voluntary consent can be presumed to exist.

Additionally, it foresees shorter deletion periods for applicants' data, the participation of a works council when appointing a DPO, and specific rules and restrictions on surveillance of employees. The current draft bill initially had a mixed reception among practitioners. It remains to be seen whether it will actually pass in 2025, as it is not the first attempt to pass such bill.

With the EU Data Governance Act, Data Act and now AI Act in force, Germany will need to designate a national supervisory authority or authorities responsible for overseeing and enforcing these new regulations. To the surprise — and perhaps frustration — of the authorities that strongly campaigned to be made supervisory authorities under the AI Act, it seems the Federal Network Agency is likely to be appointed as the primary supervisory authority for the purposes of the AI Act, the Data Governance Act and, it appears, the Data Act.

The FNA was already appointed as the primary supervisory authority for the DSA in March 2024. Corresponding legislation can be expected to progress through Parliament throughout 2025 for each of the other acts.

As mentioned in predictions for 2024, the German Federal Data Protection Act is due to be overhauled. A draft bill for amending the BDSG was published in February 2024, but the bill has yet to proceed through Parliament.

An important change foreseen in the draft amendments is the formalization of the Datenschutzkonferenz, the body representing the collective data protection supervisory authorities of each German federal state. Until now, the body has been informally organized, but under draft amendments it would be directly docked in the BDSG, which should increase its importance and legal certainty regarding recommendations.

The draft amendments also clarify the right of access under GDPR Article 15 may be limited when trade secrets of the controller or a third party would be exposed in complying with the request. Finally, the amendments regulate the competences of the German data protection supervisory authorities in case of joint control of multiple controllers located in different German federal states.

Finally, the German Consent Management Regulation was officially adopted in September 2024, as foreseen by Section 26 of the German Telecommunications Digital Services Data Protection Act, which transposes the EU ePrivacy Directive into German national law. It serves to create a legal basis for the use of central consent management platforms, which, at least in theory, should reduce requests for consent in cookie banners.

The Consent Management Regulation provides, inter alia, for specific rules on the interoperability of the CMPs and sets minimum requirements for transparency and information obligations. It remains to be seen how widely such CMPs will be used in practice, partly because they must first be approved by the Federal Commissioner for Data Protection and Freedom of Information prior to their deployment and partly because the regulation only applies in Germany and is not EU-wide. The number of CMPs officially approved over the course of 2025 should be monitored, but cookie banners will likely persist for the foreseeable future.

Back to Top ↑

Greece

Contributor: Alexandra Athanasiou

In 2025-26, Greece is expected to implement a plethora of legislative acts, such as the incorporation of the NIS2 Directive, which is currently submitted for voting in Greek Parliament, into Greek law. The Greek law is not expected to differ from the NIS2 Directive.

Other legislative developments regarding data protection will mainly concern the ratification of the Council of Europe's Convention 108+ on the processing of personal data in Parliament. Signed by Greece in 2019, Convention 108+ aims to modernize Convention 108 by addressing the challenges arising from the use of new information and communication technologies and enhancing effective implementation.

At the same time, the Greek law for the incorporation of the Data Governance Act is expected to be passed. In combination with the Data Act, which comes into force in 2025, it will form the basis for equality and value creation for businesses from accessing data, contributing to innovation and the developing data-based technologies.

Finally, the Ministry of Digital Governance is already systematically coordinating efforts to adapt the country to the provisions of the EU AI Act, which it will continue in the near future with some of provisions coming into effect in 2025.

Regarding supervision, the head of the Hellenic DPA is expected to be replaced at the end of his term. For this reason, the HDPA has not defined its strategy or action plan for the year and, therefore, is unlikely to undertake major initiatives for market regulation or supervision.

On the other hand, following Article 77(2) of the AI Act, the Ministry of Digital Governance recently published the list of all competent supervisory authorities regarding its implementation in the context of high-risk AI systems, such as the DPA, the ombudsman, the Hellenic Authority for Communication Security and Privacy, and the Greek National Commission for Human Rights, which will take over their powers by August 2026.

However, by August 2025, the competent authority for the implementation of the regulation in the Greek territory must be announced. Overall, no significant developments are expected in the national legislation or supervision level during 2025, but in terms of compliance and shaping the Greek ecosystem, the implementation of the relevant legislations in the private and public sectors will be an indicator of how ready Greece is to absorb all the legislative changes in the real market.

Back to Top ↑

Hong Kong

Contributors: Kieran Donovan, Timothy Ma

2024 has been a busy year in Hong Kong. The Office of the Privacy Commissioner for Personal Data has issued various guidelines related to data breach handling and notification and the use of AI.

With respect to cross-border data transfers, even though the relevant provisions of the Personal Data (Privacy) Ordinance are not operational, the PCPD published nonbinding guidelines on cross-border data transfers and issued guidance to assist companies in understanding how they can benefit from the voluntary Standard Contract for the Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area, which was issued by the Cyberspace Administration of China in December 2023.

Since that year, the PCPD reviewed the PDPO and proposed changes that include implementing a mandatory mechanism for notifying data breaches, obligating data users to create a policy regarding data retention periods, granting the privacy commissioner the authority to impose administrative fines, directly regulating data processors and providing a clearer definition of personal data.

However, despite the PCPD's efforts and due to the government's concerns that the new changes to the PDPO could cause significant financial pressure on small businesses, we expect Hong Kong's data privacy landscape will remain largely unchanged in 2025.

Nevertheless, we expect the PCPD will continue to actively enforce the anti-doxxing provisions in the PDPO and require companies to comply with the principles as set out in the regulation.

Back to Top ↑

Hungary 🇭🇺

Contributors: Tamas Bereczki, Ádám Liber

Digital Citizenship Program implementation

Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services introduced digital citizenship in Hungary through the DÁP mobile app. It offers innovations like e-identification and digital contract signing that are compliant with the EU eIDAS Regulation, which created a content-wide digital identity framework. This qualified electronic signature will replace Hungary's Identification Based Document Authentication service, discontinued in January 2025. A legislative amendment set for June 2025 will mandate certain organizations, like waste management public service providers and universal postal service providers, to provide digital identification services.

New national cybersecurity act

Bill No. T/9716 on Cybersecurity in Hungary, which was open for public consultation through October 2024, will repeal the 2013 Information Security Act. It introduces a national cybersecurity strategy, establishes cybersecurity authorities and forms computer security incident response teams to strengthen Hungary's cybersecurity infrastructure.

Digital land registry

Hungary's Land Registry has continuously improved its online services since 2003. The new Act C of 2021 on the Land Registry, effective January 2025, introduces an electronic land registry system called E-ING to replace the current paper-based system. This platform will provide more secure, efficient digital property management through fully electronic administrative procedures.

Implementing the AI Act

The government adopted Resolution 1301/2024 (IX. 30.), addressing implementation of the EU AI Act in Hungary. Implementation will be managed by a dedicated organization established by law, under the supervision of the Minister of National Economy, rather than the National Authority for Data Protection and Freedom of Information. The organization will provide a one-stop-shop service, conduct market surveillance tasks and operate a regulatory sandbox to enable preliminary testing of AI developments.

Additionally, the Hungarian Artificial Intelligence Council will be established, with members delegated not only by the NAIH but also by the National Media and Infocommunications Authority, Central Bank of Hungary, the Competition Authority, the Supervisory Authority for Regulatory Affairs, and Digital Hungary Agency. The council will be authorized to issue guidelines and opinions regarding implementation of the regulation.

Developing cybersecurity legislation

With the introduction of the NIS2 Directive and its national implementation through Hungary's Cybersecurity Act No. XXIII of 2023, which took effect 1 Jan. 2024, we expect lower-level legislation, such as regulations on auditors and a unified audit methodology, to come into effect by 2025. Organizations subject to the Cybersecurity Act will be impacted, as the first audits must be conducted and reported to the supervisory authority by the end of 2025.

We expect the same for the financial industry, as entities subject to the EU DORA will need to implement the finalized technical regulatory standards. Consequently, both legal and cybersecurity teams will likely be occupied throughout 2025, conducting information and communication technology risk assessments and updating agreements with ICT service providers.

Back to Top ↑

India 🇮🇳

Contributor: Pranav Rai

India's legislative privacy landscape is set for significant changes in 2025. Following the 2023 enactment of the Digital Personal Data Protection Act, the focus now shifts to its implementation and the anticipated introduction of complementary laws.

The DPDPA, India's first comprehensive data protection law, is expected to be fully operational in 2025. Despite a relatively quiet 2024, the groundwork laid in 2023, including the Bharatiya Nyaya Sanhita, the Indian Justice Code, which addresses cybercrime, sets the stage for significant developments. The government has urged organizations to begin compliance preparations even before the rules are fully notified. This proactive stance is crucial, given that a significant portion of consumers remain unaware of their data rights, and many find privacy notices difficult to understand.

The Ministry of Electronics and Information Technology, perhaps responding to pressure from the IT Standing Committee, published for public consultation the draft Digital Personal Data Protection Rules. These draft rules, embodying a "digital by design" philosophy, aim to enhance ease of living and ease of doing business by making consent mechanisms, grievance redressal, and the Data Protection Board inherently digital. For instance, the board will operate as a digital office, enabling citizens to file complaints and have them adjudicated without the need for physical presence, thereby optimizing workflows for speed and transparency.

Another significant development anticipated in 2025 is the introduction of the Digital India Act, which aims to replace the outdated Information Technology Act of 2000. The DIA is expected to provide a robust legal framework for India's digital economy, addressing contemporary challenges such as online safety and algorithmic transparency, as well as regulating emerging technologies like AI and blockchain. However, the delay in its release has raised concerns about the government's ability to keep pace with technological advancements.

The political climate in 2025, particularly with a coalition government at the helm of the country, could impact the prioritization of these legislative efforts. While there is strong momentum for advancing digital and data protection laws, political dynamics may shift focus to more immediate political issues.

In summary, 2025 is set to be a transformative year for India's privacy legislation with the full implementation of the DPDPA and the anticipated introduction of the DIA. These developments will significantly shape the future of data protection and digital rights in India. However, the government's delays and lack of clarity have raised valid concerns about its commitment to keeping pace with the rapidly evolving digital landscape.

Back to Top ↑

Indonesia 🇮🇩

Contributor: Glenn Wijaya

In October 2024, Indonesia's Personal Data Protection Law came into force. The Ministry of Communications and Informatics — which nomenclature has changed to the Ministry of Communications and Digital, pursuant to Presidential Regulation No. 139 of 2024 regarding the Organization of Duties and Functions of State Ministries of the Red and White Cabinet for the Period of 2024-29 — aims to finalize the government regulation implementing the PDPL as quickly as possible.

Once issued, Indonesia's DPA is expected to be established within two months. Until then, the ministry will handle any data breach incidents.

By 2025, with both the government regulation and the DPA in place, businesses in Indonesia will need to align operations with the new regulatory landscape. This will likely require updating privacy notices, strengthening data security protocols, and conducting regular audits to ensure compliance and prevent data breaches.

One key area that is still awaiting clarification is the certification process for DPOs, a role that will be critical in both businesses and government organizations. While many informal courses are expected to emerge, the focus will remain on the formal certification process, which will play a pivotal role in establishing qualified DPOs across sectors.

Back to Top ↑

Ireland

Contributors: Poojan Bulani, Kate Colleary

Ireland's DPC welcomed two new commissioners in 2024. There may also be a third commissioner appointed in 2025 to meet the Data Protection Act's maximum of three commissioners.

In 2024, the DPC continued to issue headline-grabbing administrative fines and sanctions, often engaging with the EDPB. One of the biggest fines, 310 million euros, was imposed on LinkedIn Ireland in October 2024 following an inquiry into LinkedIn's behavioral analysis and targeted advertising of its members. The decision concerned the lawfulness, fairness and transparency of processing.

It also focused on LinkedIn's reliance on legitimate interest as its lawful basis for processing. The DPC found LinkedIn could not demonstrate that its members' rights did not outweigh its own interests. The decision included a reprimand, an order for LinkedIn to bring its processing into compliance and administrative fines.

In September 2024, Meta was hit with a fine of 91 million euros for inadvertent storage of social media users' passwords in plaintext on its internal systems — that is, without cryptographic protection or encryption.

The DPC also took issue with the social platform X's AI model, Grok, and brought an emergency application before the High Court of Ireland to compel X to suspend, restrict or prohibit the processing of personal data and to restructure Grok's processing framework in line with the EU GDPR. This was the first time the DPC used this power, under Section 134 of the Data Protection Act 2018.

In 2025, the DPC is expected to continue to engage with organizations and enforce, using the full panoply of its powers, working closely with the EDPB and colleagues in supervisory authorities across Europe. At the IAPP Europe Data Protection Congress 2024 in Brussels, the new commissioners discussed their strategic focuses and changes to the DPC's published five-year strategy, confirming it will undergo a midcycle review in 2025.

The EDPB opinion on the EU AI Act notes DPAs should have a strong role in regulating AI. The Department of Enterprise, Trade and Employment ran a public consultation on how the regulatory bodies should be structured. While nine bodies with responsibilities for fundamental rights have been listed per Article 77, the national competent authorities for Ireland per Article 70, will likely be announced in 2025.

Back to Top ↑

Israel

Contributor: Dan Or-Hof

Israel will transition to a new data protection and data governance regime in 2025.

For years, privacy enforcement in Israel was limited, but on 5 Aug. 2024, Israel underwent a major transformation in its data protection and governance framework with the passage of Amendment No. 13 to the Protection of Privacy Protection Law, 5741-1981. Amendment No. 13 will take effect in August 2025.

The reform makes drastic changes and requires greater attention to the processing of personal data, as regulatory, civil and criminal risks become higher.

The main topics requiring attention following the reform include: very high administrative fines of up to 5% of annual turnover, statutory and exemplary damages in civil actions, redefinition of the scope of data processors, enhanced notice requirements, mandatory appointments of CISOs and DPOs, new duties of submissions to the Privacy Protection Authority, new rules for data brokers, and severe criminal penalties. For example, processing personal data without the controller's approval will be a criminal offense with up to three years' imprisonment.

Israel's privacy protection laws put a significant emphasis on data security with detailed obligations under the 2018 Data Security Regulations, which govern the entire private market and all public authorities. The current reform introduces substantial fines for violations of these regulations, thereby increasing once more the level of attention required for securing personal data properly.

With the enactment of the current reform, the PPA is granted immense administrative and criminal powers, establishing it as one of the most formidable regulators in the country. Over the past five years, even with limited enforcement capabilities, the PPA has conducted extensive supervision campaigns and released numerous guidelines, opinions, recommendations and market compliance reports.

The PPA is now poised to utilize its expanded powers to enforce its interpretation of the law, as outlined in its published guidelines and directives. Specifically, the PPA recently put a special focus on the role of the board of directors in overseeing privacy protection and cybersecurity with new guidelines that draw another target for enforcement.

There is no doubt that sensitive and mass-scale processing and use of personal data with advanced technologies, including AI systems, will be the top priorities for supervision, enforcement and litigation by the third quarter of 2025.

Companies doing business in Israel should check their alignment with the new and updated requirements of the country's laws before August 2025.

Back to Top ↑

Italy 🇮🇹

Contributor: Rocco Panetta

The year 2024 was a busy one full of developments in Italy, and 2025 will be no different.

This year, Italy's DPA, the Garante, will be increasingly involved in the processing of personal data by companies offering AI services. If, as it seems, the Garante will not be the authority directly charged with enforcing the EU AI Act, its role will remain prominent, given the massive use of personal data in both the training and output phases.

Therefore, a major challenge will be coordinating and collaborating at the international level, between DPAs, and at the national level with others such as the Italian Competition Authority, the National Cybersecurity Agency and the Agency for Digital Italy. The latter two are in charge of enforcing the AI Act.

The search for a practical solution to protect minors and their access to various online services is another major unresolved issue that has been debated in recent years and that, in light of the recent entry into force of the EU DSA and the potential invasive uses of AI, will require shared solutions, including at the international level.

Finally, in light of recent cases concerning the illegal consultation and exfiltration of personal data from databases by disloyal employees, it is clear 2025 will focus on awareness operations, which have long been at the heart of the Garante's agenda. These cases highlight not so much a cybersecurity problem as a lack of data protection culture, both in the public and private sector. This could be avoided with adequate technical and organizational measures, such as internal controls that highlight suspicious accesses.

I am certain the year ahead will, therefore, be dedicated to awakening the consciences of those who think privacy is just bureaucracy and will force several Italian institutions, both public and private, to review their internal controls.

Also, on the enforcement side, I see a growing trend in quality over quantity of inspections and enacted administrative sanctions. In 2024, for instance, the Garante issued a maximum fine equal to 80 million euros to a large energy company for alleged unlawful processing of personal data for telemarketing purposes in violation of the EU GDPR.

In short, focusing on children, improving coordination between national and international AI authorities and DPAs, and promoting dedicated awareness-raising and training initiatives, while keeping attention on enforcement and inspection high, will be at the heart of the Italian agenda.

Back to Top ↑

Japan

Contributor: Hiroyuki Tanaka

According to a supplementary provision of Japan's Act on the Protection of Personal Information, a review of whether to amend the APPI is conducted every three years. Based on this provision, the Personal Information Protection Commission published the "Interim Summary" 27 June 2024, outlining its current thinking based on discussions and examinations to date.

The PIPC published the results of a public consultation on the "Interim Summary" 4 Sept. 2024; however, it remains unclear whether legislation based on the summary will be submitted before the next regular Diet session, which runs from January to June. If the amended law is enacted, its implementation is expected to begin in either 2026 or 2027.

The main topics covered in the "Interim Summary" include new regulations on biometric data; specifying and categorizing the regulations on improper use and unauthorized acquisition; aggravating obligations on the opt-out scheme for provision of personal data to third parties; regulations regarding children's personal information; strengthening APPI enforcement, including implementation of an administrative fine system and establishment of a new system of injunctive relief and restoration of damages; streamlining the scope and details of data breach reports and data subject notifications; exempting certain data processing from data subject consent that is currently required by law; and PIAs and those in charge of handling personal data.

On 31 July 2024, an expert panel was established to discuss issues regarding strengthening APPI enforcement. The panel published a report 25 Dec. 2024.

Additionally, the PIPC published "Perspectives for Enhancing the Triennial Review of the Personal Information Protection Act" 21 Oct 2024. These perspectives could possibly be interpreted as suggesting a shift toward GDPR-style legislation to some extent, but such fundamental institutional changes may not be realistic in the short term, particularly as passage in the next regular Diet session would face significant hurdles. The PIPC conducted hearings with various stakeholders regarding these perspectives, and the results were published 17 Dec. 2024.

Back to Top ↑

Kenya 🇰🇪

Contributor: Mugambi Laibuta

The upcoming year will potentially determine the constitutionality of Kenya's Data Protection Act, 2019.

A constitutional petition filed a few weeks after the act's November 2019 enactment is likely to conclude in 2025. The petition questions the act's constitutionality due to a lack of sufficient public participation and its passing through Parliament without due regard for constitutional procedures.

The High Court of Kenya may render several decisions on the allegations: It may dismiss the petition, declare the act unconstitutional and cease its operation or request Parliament establish the process for enactment of the act. Options two and three could fundamentally disrupt data protection compliance practice in Kenya.

Another High Court decision expected in 2025 regards the court case challenging Worldcoin's operations in Kenya. The decision may redefine how foreign data handlers operate in Kenya.

In 2024, the Ministry of Information, Communications and the Digital Economy Sectoral Working Group published a report proposing reforms that will impact Kenya's privacy landscape. Some of the proposed reforms are anticipated to see implementation in 2025.

These include enacting a national data policy and national data act to regulate governance of nonpersonal data in the public and private sectors. They also propose forming and enacting national and public sector data strategies to provide guidance on data handling between the public and private sectors.

The report proposes amending the act to enhance the independence and governance structure of the Office of the Data Protection Commissioner by creating a board of directors consisting of three commissioners vetted by Parliament.

Regarding AI, the report recommends developing a national AI and emerging technology policy, implementing a soft regulatory framework for AI, and developing an AI and emerging technology act as well as future regulations. Stakeholders have been holding discussions on whether Kenya needs an AI act, strategy or policy for close to 18 months. Perhaps this question will find answers in 2025.

The report also recommends enacting a bill to regulate blockchain technologies and virtual assets, including cryptocurrencies, and developing a national cybersecurity policy.

In 2024, the ODPC was active in auditing data handlers, handling complaints by data subjects, and issuing administrative and penalty notices to noncompliant data handlers. It is therefore expected to ramp up operations to ensure greater data protection compliance for data handlers and access to remedies for aggrieved data subjects.

However, the potential for outcomes of many appeals challenging ODPC decisions before the High Court in 2025 may redefine the ODPC's operations and actions.

Back to Top ↑

Lithuania 🇱🇹

Contributor: Gabriele Kaveckyte

In 2025, Lithuania is expected to see some developments in the field of personal data protection as amendments to the Law on Legal Protection of Personal Data come into effect.

Starting January 2025, the Lithuanian State Data Protection Inspectorate will be required to publish its decisions on data protection infringements publicly, and the information will remain available for a period of 10 years. This move toward transparency aims to help organizations better understand the enforcement landscape, which previously lacked transparency.

The VDAI's 2024-26 strategic plan highlights a proactive agenda, including a focus on strengthening oversight and ensuring transparent data protection practices for 2025. Key initiatives include advancing cross-border cooperation with other supervisory authorities, preparing for the EU AI Act and DSA, and increasing public trust through educational outreach and resources for both public and private sectors.

Back to Top ↑

Luxembourg

Contributors: Yoann E. A. Le Bihan, Vincent Wellens

In 2025, data protection in Luxembourg will face significant shifts, notably with the gradual implementation of the EU AI Act. Since phased enforcement of the act began in August 2024, questions remain about which local agency — or agencies — will oversee its enforcement.

However, as its provisions gradually take effect over the next three years, the AI Act is likely to become a central focus, addressing the complexities of AI regulation and balancing innovation with privacy and data protection standards.

In the unlikely event Luxembourg's National Commission for Data Protection does become an enforcement agency in this field, we expect it will fully use its powers under the EU GDPR to tackle AI-related problems. It has become quite visible in the field and, more generally, follows all innovative trends, including implementation of the European Health Data Space. In the same vein, it has developed a GDPR-related regulatory sandbox, through which organizations can test innovative ideas while striving for GDPR compliance.

The notable increase in cyberattacks, such as distributed denials of service and advanced phishing campaigns specifically targeting the region in recent months, may well fuel greater public awareness of privacy and the need to protect against increasingly sophisticated threats, such as CEO frauds supported by deepfake technologies or high-quality phishing emails generated by AI-powered large language models.

Consequently, there has been a rise in data subject requests, data breach notifications from data controllers and complaints from data subjects. This, in turn, could drive a more robust CNPD enforcement response to ensure compliance with relevant legal frameworks, including the GDPR and potentially the AI Act, if the CNPD becomes involved in its enforcement as anticipated.

The CNPD published only one decision in 2024, but many more likely remain unpublished due to appeal deadlines or pending appeal procedures. Several investigations are ongoing, though, and they may lead to decisions in 2025, providing valuable insights into the CNPD's stance on GDPR enforcement.

Back to Top ↑

Malaysia

Contributor: Pavla Jonette Vydrzelova

In 2025, Malaysia is expected to witness significant changes in its privacy and cybersecurity landscape, driven by the rapid digital transformation and rising cyberthreats.

The government already signaled plans for reform, including an overhaul of the Personal Data Protection Act 2010, which governs how businesses handle personal data. Once adopted, the amendments will likely further strengthen data breach notification requirements, increase penalties for noncompliance, and broaden the scope of data protection to include newer technologies like AI and Internet of Things devices.

To accompany the reform and help business adapt to the changes, enhanced support through guidelines, FAQs and further resources is anticipated in 2025.

Following the release of the Cyber Security Act 2024, which came into effect in August, the push for stronger cybersecurity measures will also intensify, as cyberattacks on businesses and government agencies are on the rise.

The National Cyber Security Agency is expected to take a more prominent role in defending critical infrastructure and enhancing public-private collaboration. This could involve introducing mandatory cybersecurity frameworks and certifications across industries, ensuring organizations comply with higher security standards.

In addition, as Malaysia aims to boost its digital economy, privacy concerns around AI and big data analytics will grow, likely prompting further regulation of how such technologies can ethically collect and use data. Public awareness of cyberthreats is also likely to increase, leading to stronger, more formal and more frequent consumer demands for privacy.

Overall, in 2025, Malaysia's evolving privacy and cyber landscape will involve a more stringent regulatory environment, greater focus on cyber resilience and heightened emphasis on protecting personal data in an increasingly connected digital society.

Back to Top ↑

Mexico 🇲🇽

Contributor: Gabriela Espinosa Cantu

Legislative activity is moving quickly in Mexico and most likely will continue to do so throughout the upcoming months.

Among the most relevant and impactful for privacy pros, before the end of his term in 2024, then-President Andres Manuel Lopez Obrador presented a bill to Congress that aimed to simplify government organization by eliminating several agencies, including Mexico's DPA, the National Institute for Transparency, Access to Information and Personal Data Protection. The INAI is an independent, specialized, impartial, autonomous entity, as established under Article 6 of the Constitution of Mexico — hence, dissolving it would require amending the Constitution.

At the time of this publication, the bill sits with the House of Representatives awaiting a vote. It proposes dissolving the INAI and transferring its functions, including granting access to public information and acting as DPA, to other existing government bodies dependent on the executive branch, which are under direct authority of the Mexican president. This would jeopardize the INAI's independent and autonomous nature, undermining its capacity to act as grantor for transparency and privacy. If passed in both houses of the federal Congress, the bill would need to pass a vote by the majority of the states' local congresses, which would not be a challenge given the current political landscape.

Many have raised concerns including, but not limited to, the INAI's commissioners, who have proposed alternatives to INAI's simplification and cost reduction. Nevertheless, current President Claudia Sheinbaum publicly stated her interest in completing the INIA's dissolvement by the end of 2024 with the support of her political party, which represents the majority in Congress. A shower of amendments to federal laws is anticipated to follow during 2025 to operate the Constitutional reform and transfer the oversight and regulatory functions to other government entities.

Back to Top ↑

Netherlands 🇳🇱

Contributor: Abraham Mouritz

Many developments throughout 2024 will further shape the Netherlands' legal data privacy landscape, including the outcomes of two recent court decisions.

The Royal Dutch Lawn Tennis Association was fined 525,000 euros by the Netherlands' DPA, Autoriteit Persoonsgegevens, which rather oddly insisted that purely commercial interests could not be considered legitimate interests under Article 6(1)(f) of the EU GDPR. In this case, the commercial interest entailed the sharing of members' personal data with the KNLTB's sponsors.

However, the CJEU ruled 4 Oct. 2024 that, depending on the circumstances, purely commercial interests can fall under the heading of legitimate interests and reversed the AP's earlier decision, including the imposed fine. It was not the first time the AP adopted this rather controversial approach, for example it was also used in the VoetbalTV decision from 2022.

The CJEU's KNLTB decision was welcomed. Had the AP's approach been upheld, it would have surely stifled commerce and innovation in the Netherlands. I anticipate further legal developments involving data privacy that will be more accommodating to commercial interests.

Class-action lawsuits

The Netherlands is home to many class-action lawsuits. The main reason being that its courts are, generally speaking, trade-focused, internationally oriented and very affordable compared to those in other countries, especially in the U.K. and the U.S. Since 2020, as a result of the Act on Collective Damages in Class Actions, victims of mass damages can also be adequately compensated.

This has led to an influx of data privacy class-action lawsuits. Examples include cases against TikTok, and Oracle and Salesforce, jointly. However, class-action lawsuits are very complex, and it will take many years to find out if claims are even admissible. From that point on, the next hurdle will be if, and to what extent, damages can be awarded.

One positive legal development in this respect occurred recently in the joint case against Oracle and Salesforce. On 24 Sept. 2024, the Amsterdam Court of Appeals ruled that, while it is yet to be decided by a court whether the data privacy claims are at all admissible, the court can already start to consider the merits of these claims. This will speed up the legal process and give more clarity on the chances of success at an earlier stage.

Now that the discussion on the viability of class-action lawsuits, that is, on damages, is being held at an earlier stage, I foresee more data privacy class-action lawsuits will likely be launched in the Netherlands.

Back to Top ↑

New Zealand 🇳🇿

Contributor: Daimhin Warner

2025 looks set to be a busy year for privacy in New Zealand, with several legislative and regulatory changes commencing or progressing.

Two bills that will make a host of amendments, with low-to-medium impact, to the Privacy Act 2020 are moving through Parliament.

The Privacy Amendment Bill will introduce new information privacy principle 3A, primarily to maintain New Zealand's hard fought EU adequacy status, and will implement a new and explicit notification obligation related to the indirect collection of personal information. Subject to the legislative process, IPP 3A is expected to take effect with respect to personal information collected from 1 June 2025.

The Statutes Amendment Bill will make a number of interesting adjustments to the Privacy Act. These include reinstating the ability for an organization to refuse a request for personal information on the basis that the information is not readily retrievable, clarifying that an organization acting solely as an agent of another organization, that is as a data processor, will not be liable for privacy breaches, and providing the Office of the Privacy Commissioner more discretion to take no action on complaints, when this would be inappropriate.

We should know early this year whether the OPC intends to implement the Biometrics Processing Privacy Code, a code of practice issued under the Privacy Act to regulate the processing of biometric information, including facial recognition information. A code seems likely, in view of the strong public support the OPC received on the draft. The OPC's decision will also be influenced by a review of the facial recognition technology trial by Foodstuffs North Island, which resulted in at least one case of harm.

2025 might also see some progress on the Customer and Product Data Bill, which has been back and forth on the legislative agenda for many years. The bill will introduce a sectoral data portability right and framework for New Zealand.

Finally, in 2025, the rubber will really hit the road regarding the Digital Identity Services Trust Framework Act 2023. Rules issued under the act will be in force, and the newly established Trust Framework Authority will commence consideration of applications for digital identity provider accreditation, including independent privacy evaluations.

Back to Top ↑

Nigeria

Contributors: Ridwan Oloyede, Dorcas Tsebee, Tojola Yusuf

The past year was another important one for data protection in Nigeria, marked by the first anniversary of the Nigeria Data Protection Act and significant court decisions that further solidified its impact. The NDPA's influence is becoming increasingly evident, and 2025 is anticipated to be a year of more implementation and enforcement.

Nigeria's Data Protection Commission is expected to finalize the much-anticipated General Application and Implementation Directive for the NDPA, following public consultations on the draft released earlier this year. This directive will provide crucial guidance on interpreting and applying the NDPA's provisions. Additionally, clarification is anticipated on the cross-border data transfer provisions under the NDPA. Likewise, the NDPC will likely issue further guidelines, guidance notes and regulations to address specific sectors and emerging challenges.

The NDPC is also poised to actively exercise its enforcement powers, issuing sanctions and penalties for noncompliance with the NDPA. Court judgments throughout the year are expected to offer further clarity on various aspects of the act, shaping its practical application and setting precedents for future cases.

Sector-specific regulations, both those directly related to data protection and those with implications for privacy, are expected to emerge from various regulatory bodies. These regulations will tailor data protection requirements to the unique needs and challenges of different sectors, such as finance, health care and telecommunications. This may also extend to children's online safety, with potential intervention addressing data protection concerns related to children's online activities.

Progress is anticipated on several pending bills, including the National Digital Economy and E-Governance Bill and the Control of Usage of Artificial Intelligence Technology Bill, among others. These bills, along with other proposed legislation like the Digital Rights and Freedom Bill, may be reintroduced or undergo further revisions.

AI governance will likely remain a key focus area. The long-touted National AI Strategy is finally expected to be published, setting the stage for its implementation. We expect to see more AI-specific regulatory interventions, potentially in the form of guidelines, advisories or regulations, as Nigeria seeks to balance innovation with ethical considerations and data protection principles.

Overall, 2025 promises to be a year of significant developments in Nigeria's data protection landscape. With the NDPA firmly in place, a shift toward greater accountability, enforcement and sector-specific guidance is anticipated.

Back to Top ↑

Norway

Contributor: Martha Ingves

Norway leaves behind an exciting fall for data protection, with a lot of activities on different fronts. Looking forward to 2025, there are no signs the focus on data privacy will slow down.

The new year kicks off with a new Electronic Communications Act, adopted in November 2024. With this new law, placement of cookies and other tracking technologies will require active consent, bringing the Norwegian legislation up to par with the rest of Europe. The new law is expected to be accompanied by an increased level of enforcement in the area.

In 2024, Norway's government announced it is looking into revising the Norwegian Data Protection Act. Among other things, empowering Norway's DPA, Datatilsynet, to issue coercive fines against foreign multinational companies is being considered. This is in light of the outcome of a recent case against Meta, which successfully argued the DPA does not have such power under existing rules. The findings of the review will likely be seen during 2025.

The Grindr saga will also continue into 2025. It started in 2021, when the dating app was fined NOK65 million for its lack of legal basis when sharing personal data for advertising purposes. It was the highest fine ever issued by Datatilsynet. Thus far, Grindr has not succeeded in having the fine repealed. However, the litigation will continue in the Court of Appeal in 2025.

Back to Top ↑

Panama

Contributor: Lia P. Hernandez Perez

In 2024, Panama's Personal Data Protection Law reached three years since it entered into force. Enforcement by organizations and regulatory authorities is not as efficient as expected. Likewise, with changes to the National Assembly of Panama, several initiatives have been presented that directly or indirectly impact the regulation of privacy in the country.

In August 2024, Congressman Manuel Cheng presented a draft bill to regulate and promote AI in Panama. This is not the first proposal on the matter to be presented in the National Assembly. In 2023, a draft bill on the regulation of AI was presented through the citizen participation procedure. And 1 Nov. 2023, former Congresswoman Marylin Vallarino presented a draft bill on the promotion and investment of AI to the Committee on Trade and Economic Affairs. Neither of the bills were approved or discussed before the committees of the National Assembly of Panama.

Likewise, Congressman Ernesto Cedeno presented another draft bill to modify Article 3 on the scope of application of the PDPL, excluding the practice of journalism due to fines imposed by the previous administration of Panama's National Authority of Transparency and Access to Information to several media outlets. On the other hand, Congressman José Pérez Barboni presented an initiative for the regulation of body surveillance cameras by the National Police of Panama.

In October, the Bill of Law on Cybercrime was approved, adapting Panama's criminal legislation to the Budapest Convention. However, President José Raúl Mulino partially vetoed the bill of law that seeks to fill a gap in Panamanian criminal legislation, establishing new criminal types for conduct that was previously unregulated.

Since 2023, Panama's government has been working to develop a national AI strategy with the support of a development bank. The initial draft of the strategy has not yet been released but is anticipated in 2025.

A group of experts are also working on a comprehensive modification of the current PDPL to be presented to the National Assembly in 2025.

Back to Top ↑

Paraguay 🇵🇾

Contributor: Cecilia Abente

Awareness of the importance of a comprehensive data protection law among both individuals and public authorities was brought to the fore many times over the past year in Paraguay.

Despite being on the parliamentary agenda several times in 2024, the proposed Personal Data Protection Bill was not discussed thoroughly in the Chamber of Deputies. Nevertheless, the bill was approved during the last legislative session, but the study of its details was delayed until the following session, which will take place after the summer break in 2025.

The bill follows the EU GDPR and creates an appropriate data protection framework that includes data protection principles, data subject's rights, controller's obligations, international transfers requisites and appointment of a new supervisory authority.

Though it is very likely amendments to the original bill will be proposed by private and public sector parties when the discussion arises, the current main subject areas are expected to remain in the text.

Moreover, there are other bills involving personal data, such as a bill "providing for mandatory retention of traffic data to combat child pornography and related punishable acts" that could be on the parliamentary agenda once the data protection bill is discussed.

Looking ahead, we remain hopeful to have good news in 2025 regarding data protection law in Paraguay.

Back to Top ↑

Peru 🇵🇪

Contributor: Catherine Escobedo

In 2025, Peru's legislative priorities will likely center around AI regulation and enhanced cybersecurity and cyberdefense measures.

Peru positioned itself as a Latin American pioneer in AI regulation with the 2023 enactment of Law No. 31814, promoting the use of AI for economic and social development of the country. In May 2024, the Secretariat of Government and Digital Transformation introduced draft regulations inspired by the EU AI Act. However, the draft regulations faced several challenges, including limited clarity, regulatory gaps and inconsistent application — such as being mandatory for the public sector but optional for private entities. The regulations' requirements for high-risk AI systems may also prove overly complex for smaller businesses. An amended version is expected to be approved in 2025.

Peru's Congress actively pursued AI-related legislation throughout 2023 and 2024. Notable among pending bills is No. 6524/2023-CR, which focuses on transparency by mandating digital labeling for AI systems. The bill requires disclosure of the AI's purpose, impact and potential for misleading users, particularly for content resembling real entities. As AI adoption accelerates, ensuring transparency and preventing deception will remain key priorities for lawmakers.

On the data protection front, after the 30 Nov. 2024 approval of the new regulations of the Personal Data Protection Law, Peru's DPA, the Autoridad Nacional de Protección de Datos Personales, is expected to publish additional guidelines and regulations, or modifications to the preexistent law, to clarify the new obligations imposed by these regulations. Additionally, Bills No. 2942/2022, 3131/2022 and 3541/2022, amending Article 58.1 of the Consumer Protection and Defense Code to prohibit unsolicited spam calls, are under review following executive branch observations and are expected to pass in 2025.

Regionally, the Andean Congress — representing Bolivia, Ecuador, Peru and Colombia — initiated discussions in April 2024 about establishing a unified right to be forgotten. While this initiative could establish cohesive cross-border privacy standards, varying national frameworks pose challenges to implementation. Though approval is unlikely by 2025, this collaboration signals growing regional commitment to data privacy rights.

Regarding cybersecurity, the February 2024 approval of Cyber Defense Law regulations prompted a review of existing laws to strengthen armed forces and police capabilities against digital threats. A major bank data breach in late 2024 highlighted the need for comprehensive breach notification regulations, which the new Data Protection Law regulations have just incorporated. Nevertheless, we should also remember Peru's Digital Trust Framework, Urgent Decree No. 007-2020, addresses security incidents in digital environments, which mandates specific reporting of breaches also to the National Digital Security Centre, but fails to provide clear guidelines. With draft regulations from 2023 still pending approval, establishing detailed breach notification requirements will likely be a legislative priority in 2025.

Back to Top ↑

Philippines 🇵🇭

Contributor: Irish Krystle Almeida

The Philippines' National Privacy Commission is set to release an advisory on child-oriented transparency that will provide guidelines on processing children's personal data, recognizing their best interests and evolving capacities. According to the NPC, as data subjects and rights holders, children are entitled to meaningful access to information and should be provided with opportunities to create and interact within a protective environment.

Additionally, the NPC is gathering use cases on privacy-enhancing technologies to gain a contextual understanding of PETs across various sectors in the country. Real-world and practical insights on the applications and benefits of PETs will allow the NPC to shape its policy and drive innovation.

On the cybersecurity front, the Department of Information and Communications Technology released a draft Department Circular Prescribing the Adoption of Relevant Information Security Standards and Certification for Public Telecommunications Entities. The DICT deems that the adoption of information security standards for all critical information infrastructure, which includes public telecommunication entities, is essential.

As in 2024, AI continues to be in the spotlight. Government agencies are organizing roundtable discussions, public consultations and regulatory sandboxes to ensure the creation of AI law and policy is tailored to the country's setting and is responsive to its specific needs.

Notably, the National Economic and Development Authority is crafting a policy note on AI to address the data privacy and cybersecurity risks of its integration into various aspects of life and industry, among other things. The policy note likewise seeks to address ethical considerations, particularly related to how AI applications may be misused as a tool for disinformation, manipulation and the commission of crimes.

Back to Top ↑

Poland 🇵🇱

Contributor: Piotr Lada

In the context of privacy and personal data, 2025 in Poland will be a time for facing new challenges in terms of the regulatory framework of the EU, as well as national legislation. As part of the national implementation of the EU AI Act, a draft law on AI systems was published 15 Oct. 2024 with a planned deadline for the Council of Ministers to adopt the draft by the end of 2024 for further legislative proceedings. Similarly, in the fall of 2024, a draft law on data governance was published in Poland for the proper application of the EU Data Governance Act.

With considerable delay, the EU Whistleblower Directive, EU Directive 2019/1937, on the protection of persons who report breaches of union law entered into force in Poland in September 2024. The application of these regulations will pose a number of challenges in terms of the protection of whistleblowers' personal data and the notification procedure, as well as compliance more broadly, especially in the initial period of its application, including the first half of 2025.

In 2024, there was also a change to the position of the president of Poland's DPA, the Urząd Ochrony Danych Osobowych, whose activities in 2024, as well as those planned for 2025, should be assessed in a positive light. A social committee of experts has been set up within the DPA to advise, give opinions, support and evaluate legislative processes in the field of personal data protection, as well as to promote good practices.

Consequently, in 2025, guidelines can be expected on the application of the EU GDPR in Poland. Authorities will likely pay attention to existing regulations and practices regarding new technologies, AI and the pay-or-consent model, as well as the areas of modern medicine and employment.

In 2025, Poland's data privacy landscape is likely to reflect both regulatory advances stemming from the EU and a growing national focus on data rights and compliance, signaling a year of alignment and strengthening of privacy practices in the country.

Back to Top ↑

Portugal 🇵🇹

Contributor: Maria Catarina Batista

While Portugal was anticipated to launch a Data Protection Portal in 2024 — included as a major element of the National Data Protection Commission's 2024-2026 Strategic Plan — reports indicate full operational functionality might not be achieved until 2025. The portal is designed to enhance public engagement and streamline communication with key stakeholders, including data subjects, controllers and processors.

The INCoDe.2030 program, managed by Secretary of State for Digitalisation and Administrative Modernisation Mário Campolargo, was originally planned to unveil the National Data Strategy in 2024. However, the release is now likely to be launched in 2025 following election-related adjustments.

Also in 2025, the CNPD will hopefully release guidelines on balancing data protection with emerging technologies, focusing on AI.

Back to Top ↑

Romania 🇷🇴

Contributor: Adriana Neagu

As in many countries around the world, elections were held in Romania in 2024, which may bring significant changes regarding major themes in the public sphere. While there is no local initiative to modify the applicable data protection rules in Romania, the annual plan for transposing EU directives in 2025 includes a point on the implementation of Directive (EU) 2023/2123, amending Council Decision 2005/671/JHA on the exchange of information and cooperation on terrorist offenses related to its alignment with EU rules on the protection of personal data. The deadline for transposition into national law is 1 Nov. 2025.

Additionally, Romania recently unveiled its National Action Plan committing to the digital objectives outlined in the European Digital Decade Policy Programme 2030. The plan provides a vision for Romania's digital ecosystem, aligning with European digital values and targets. Based on this plan, rules and measures to attain the outlined targets are expected in the coming years.

Significant targets within the plan include: achieving 100% online availability of digital public services by 2030; addressing the low adoption rates of advanced digital technologies among enterprises, currently standing at 11% for cloud services, 1% for AI and 5% for big data, all below EU averages; and focusing on closing the digital gap between urban and rural areas by modernizing infrastructure and increasing access to essential services.

This initiative represents a significant step toward integrating Romania into the broader European digital landscape. Understandably, the success of this plan will heavily depend on the strategy of the newly invested government.

Back to Top ↑

Serbia 🇷🇸

Contributor: Petar Mijatović

In March 2024, Serbia's DPA, the Commissioner for Information of Public Importance and Personal Data Protection, adopted its official yearly report. As in previous years, the report reaffirmed the commissioner's view that main impediments in exercising data subject rights under the Law on Personal Data Protection are the legislation's normative flaws.

Among other things, the LPDP lacks recitals that would establish criteria for further interpretation of the law. Noncompliance of other laws with the LPDP is also an impediment. Additionally, many aspects of the law are either inadequately regulated or not regulated at all, and there is an exceptionally high number of exemptions from the application of the LPDP. Therefore, Commissioner Milan Marinović concluded it is necessary to amend and supplement the LDPD.

According to a Data Protection Strategy for 2023-30, adopted in August 2023 by the government of the Republic of Serbia, steps should be taken to regulate the automated processing of genetic and biometric personal data and to regulate personal data processing using audio and video surveillance though adoption of the amendments and supplements to the LPDP and adoption of special regulations. Since these steps have not yet been substantively undertaken in 2024, 2025 is expected to bring more concrete actions in this direction.

Additionally, considering the commissioner's recent activities regarding changes to the privacy notices of Meta and the social platform X concerning the processing of personal data for AI development, it is notable that these companies do not follow the same approach in Serbia as they do in the EU, despite identical data protection requirements. Therefore, a more proactive approach by the commissioner can be expected in 2025, albeit with very limited authority, given the lower penalties stipulated under the LPDP.

Back to Top ↑

Singapore 🇸🇬

Contributor: Pranav Rai

As we move into 2025, Singapore is set to continue its proactive stance on data privacy, building on significant strides made in recent years.

The Personal Data Protection Act has undergone substantial changes to enhance consumer protection and align with technological and business trends. A key development is the introduction of data portability provisions, anticipated to take effect in 2025, which will grant individuals greater control over their personal data and encourage innovative data use by organizations. The right is expected to be broad, with exceptions and restrictions to address scenarios in which data transmission could compromise national interests.

As global data flows become more complex, Singapore will likely update its regulations on cross-border data transfers. New frameworks and agreements with international partners will likely be introduced in 2025 to facilitate secure and compliant data exchanges, reinforcing Singapore's position as a trusted data hub in the region.

On the AI and privacy interaction front, with voluntary AI governance frameworks in place, Singapore's Personal Data Protection Commission is focused on issuing comprehensive guidelines. The recently issued Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems emphasize transparency and obtaining consumer consent. In 2025, the PDPC is expected to continue developing guidelines to address the ethical use of AI in data processing, stressing transparency, accountability and minimizing bias in AI algorithms.

Singapore's hallmark of addressing privacy challenges through practical and innovative methods is set to continue. This includes promoting the adoption of PETs and building on previous initiatives like the Infocomm Media Development Authority's PET Sandbox, which provides a secure environment for organizations to experiment with and identify suitable PETs.

In summary, 2025 will be pivotal for data privacy in Singapore, with actions aimed at enhancing consumer protection, fostering innovation and maintaining high standards of data security. This will be achieved through guidelines, advisories — including those on AI initiatives — and a continued practical approach. These developments will solidify Singapore's reputation for effectively balancing privacy rights with technological advancement and business growth.

Back to Top ↑

Slovakia 🇸🇰

Contributors: Lukas Mrazik, Barbora Blahova

In Slovakia, the Office for Personal Data Protection, Úrad na ochranu osobných údajov, is anticipated to increase its activities with the appointment of a new president. An increased focus on cybersecurity is also expected due to the implementation of the NIS2 Directive.

Since April 2020, the ÚOOÚ lacked a permanent leader, resulting in reduced activities, with guidelines in particular. Zuzana Valková was appointed president in 2024, promising stability and improved operational effectiveness. This change is intended to reinvigorate the office's role in GDPR enforcement and align it more closely with evolving EU standards. Slovakia adopted the NIS2 Directive into the Cybersecurity Act, which takes effect in early 2025. The changes will significantly impact a high number of businesses across Slovakia and the number of in-scope companies is expected to significantly grow. In addition, Slovakia's National Security Authority is raising awareness and will likely continue to be active during the implementation and enforcement phase. Cybersecurity will also be an important topic for businesses linked to the financial sector, with the EU DORA taking effect. In practice, there is a strong impact not only on the financial sector but also the entire supply chain of IT services.

In mid-2024, Slovakia implemented new laws on consumer protection, which implement the European Commission's New Deal for Consumers and Representative Actions Directive, extending consumer protection to various digital elements and services and enabling collective consumer actions for monetary and nonmonetary claims. The impact of collective actions is yet to be seen, as it may enable class violation of the GDPR to be brought to courts, but it is not expected to be extensively used by data subjects in Slovakia.

Back to Top ↑

South Africa 🇿🇦

Contributor: Armand Swart

In 2024, South Africa's Information Regulator issued seven enforcement notices for noncompliance with the Protection of Personal Information Act, the country's equivalent of the EU GDPR, including for failure to comply with data breach notification obligations and for inadequate security safeguards. Between April and September 2024 alone, 980 data breaches were reported to the IR.

Further enforcement related to data breaches and security controls is likely in 2025, especially for financial institutions.

The most high-profile enforcement notice issued by the IR in 2024 was against WhatsApp for a subpar South African privacy notice in comparison to its EU counterpart. There may still be further developments on this enforcement process in 2025.

The IR intends to propose amendments to allow it to issue fines immediately without issuing an enforcement notice first. Draft amendments may be published in 2025.

The IR is set to issue guidelines regarding electronic direct marketing in 2025. It argues electronic direct marketing includes telephone calls by live voice and that strict consent requirements must be met to direct market. This has been met with criticism, and any published guidelines may be challenged in court.

South African regulators have issued cybersecurity standards and directives that apply to financial institutions and payment institutions, including payments services providers. The directive for payment institutions came into effect in late 2024, while the standard for financial institutions will come into effect in June 2025.

A draft National Artificial Intelligence Policy Framework has been published for consultation and will inform the drafting of a national policy to guide AI regulation. The framework should be finalized in 2025.

An independent body, the South African AI Association, recently lodged a complaint to the IR against LinkedIn for using personal data to train AI models without users' consent. The IR's decision on this, expected in 2025, will inform future AI developments in the country.

Back to Top ↑

South Korea 🇰🇷

Contributor: Kyoungjin Choi

Since the 2023 comprehensive revision of the Personal Information Protection Act, South Korea has experienced many changes in personal information regulations, and these changes are still ongoing.

To minimize the PIPA revision's impact, the revised law is being implemented in three stages, with most revised provisions implemented in September 2023 and March 2024. The final stage concerning the right to request data transmission, which is the foundation of the MyData data-sharing initiative, is set to be implemented by March 2025. With the goal of introducing the MyData system across all sectors, subordinate statutes are being revised to specify details such as methods and procedures for transmitting personal information, designation and supervision of specialized personal information management organizations, information transmission standards and fees related to transmission requests.

However, social consensus surrounding the introduction of MyData in all areas is not yet fully aligned. Issues such as the scope of personal information to be transmitted by businesses, including those in the distribution sector, and the special characteristics of each sector are still under debate. In-depth discussions and efforts to reach a social consensus among stakeholders, including businesses, the government and data subjects, are expected to continue throughout 2025 to fully settle the MyData system.

South Korea's Personal Information Protection Commission plans to finalize the AI Privacy Risk Assessment and Management model and improve the Biometric Information Regulation System, following publication of the Guide on Processing Publicly Available Data for AI Development and Services.

Looking ahead to 2025, the global AI hegemony competition is anticipated to intensify. South Korea will continue its efforts to support autonomous privacy risk management of AI companies under the national strategy to secure global AI competitiveness, and the government will push to revise the PIPA to introduce a personal information regulation sandbox system to support AI innovation. Separate legislation will be promoted for systematic legal improvement of biometric and image information, which are highly utilized in the AI era.

The government will also seek to implement revisions enhancing the effectiveness of personal information protection for children and adolescents who require special protection.

Back to Top ↑

Spain 🇪🇸

Contributor: Joanna Rozanska

Throughout 2024, Spain's DPA, the Agencia Española de Protección de Datos, doubled down on the intersection of personal data protection and emerging technologies, highlighting just how seriously it takes these rapid advancements.

The AEPD released guidelines on everything from neurodata processing to Wi-Fi tracking technology and even internet addiction patterns. The agency's focus is set to continue — if not intensify — in 2025, as technologies with potential privacy impacts evolve faster than ever.

Cybersecurity will also be a key area of focus in 2025, as recent years have seen a significant rise in data breaches. In response, the AEPD intensified efforts to educate companies and individuals, releasing various guides and resources to raise cybersecurity awareness and encourage preventative measures.

In 2024, the appointment of a general director for the Spanish Agency for the Supervision of Artificial Intelligence — the first supervisory authority for AI in Europe — set the stage for momentum in the year ahead. The AESIA is expected to publish several guidelines in 2025, including one specifically addressing the interplay between AI and data protection.

Its guidance will provide businesses with essential direction on managing personal data responsibly within

AI applications, promoting transparency and clear expectations in a field that is increasingly shaping both business and everyday life. Similarly, guidelines related to the newly approved EU AI Act's scope of applicability, as well as the responsibilities of different stakeholders along the AI value chain, are anticipated.

Finally, while there is a growing emphasis on regulating digital products across Europe — extending beyond the AI Act with the recent revision of the EU Product Liability Directive for defective products, now covering software, and the proposed AI Liability Directive — these initiatives remain in early stages.

Although they may not lead to immediate changes in the national legislative framework, their influence is expected to unfold progressively over time.

Back to Top ↑

Sri Lanka 🇱🇰

Contributor: Ashwini Natesan

Sri Lanka's comprehensive Personal Data Protection Act, which passed in 2022, comes into operation 18 March 2025. The upcoming year will be a milestone one for Sri Lanka, since there was no previous comprehensive data protection legislation. In 2025, the provisions related to personal data processing, data subjects' rights, controllers and processors, and penalties will become enforceable.

This fall, Sri Lanka's DPA released several draft rules, regulations and guidelines for the PDPA for public consultation. The DPA also released rules on cross-border data flows, data breach notification and data protection management.

Draft regulations mandate the appointment of a DPO in entities with "regular and systematic monitoring of data subjects on a certain scale and magnitude or processing of special categories of personal data on a scale and magnitude," as well as under certain other conditions, like when data of over 25,000 individuals or of different types is processed.

Considering Sri Lanka did not previously have data protection legislation that applies across sectors, including government entities, it would be a significant step for these entities to have procedures and processes in place to comply with the PDPA.

The DPA also released guidelines for compliance by public authorities, stating they are anticipated to train officials on the PDPA and its compliance requirements. Thus far the DPA has not issued guidelines on use of personal data for public interest, including journalistic purposes. It remains to be seen if this will be addressed.

As organizations prepare themselves for compliance and with the enforcement date looming large, these rules, guidelines and regulations are of great importance.

Back to Top ↑

Sweden 🇸🇪

Contributor: Sofia Edvardsen

Sweden, like other member states, must adapt its national laws to align with the EU AI Act's requirements. Sweden's DPA, the Integritetsskyddsmyndigheten, is expected to play a key role in overseeing AI systems involving personal data, particularly when their decisions impact individual rights.

The act, which aims to regulate AI systems across the EU — focusing on high-risk applications in sectors like health care, public administration and justice — mandates transparency and human oversight in AI systems. Swedish organizations, both public and private, will need to revise technical and organizational processes to meet these standards, including data training and usage. The health care sector, where AI is already in use, will face significant changes, linking closely with existing patient data laws.

NIS2 Directive and CER Directive

Implementation of the NIS2 and CER Directives into Swedish law is delayed and expected by August 2025. The acts will be implemented into Swedish law by the Swedish Cybersecurity Act, which proposes reliefs for the public sector and exempts its management from personal liability. Cloud service providers and certain NIS1 actors, however, were obligated to apply the NIS2 Directive Article 21 requirements starting 7 Nov. 2024.

EU DORA

Sweden is on track to implement the EU DORA by 17 Jan. 2025. Sweden's Financial Supervisory Authority, Finansinspektionen, is leading efforts to align national regulations with the DORA's requirements. This involves updating existing frameworks and issuing new guidelines to ensure financial entities comply with the forthcoming standards.

Back to Top ↑

Switzerland

Contributor: Stéphane Droxler

As Switzerland welcomes 2025, several legislative developments are set to shape the country's data protection landscape.

In 2024, the European Commission confirmed Switzerland's data protection adequacy, affirming alignment with EU standards. This decision allows continued data transfers between Switzerland and the EU/European Economic Area without additional safeguards, benefiting Swiss businesses engaged in European data exchanges.

In September 2024, Switzerland also ratified the Swiss-U.S. Data Privacy Framework, which facilitates compliant transatlantic data flows between Swiss data controllers and American companies adhering to the framework.

Domestically, following the recent implementation of the revised Federal Act on Data Protection in early 2024, Switzerland's Data Protection and Information Commissioner continues to oversee its enforcement. Over 2,000 DPOs have registered on the new portal dedicated to DPOs, while the security breach notification system has recorded around 250 incidents in its first six months. This gradual increase in notifications reflects the growing compliance efforts of Swiss businesses, which are expected to continue into 2025.

The Federal Assembly of Switzerland is currently debating two laws with significant data protection impacts. First, following the rejection of a previous text by popular vote, discussions around a new e-ID law are ongoing, with implementation not anticipated before 2026. The law aims to introduce a state-issued electronic identity to bolster digital trust and simplify electronic interactions once approved.

Additionally, amendments to the Federal Act on the Electronic Patient Record are under review. The draft revision marks a paradigm shift, moving from the current opt-in model to an opt-out system. This change would require all Swiss residents with mandatory health insurance to have an electronic patient record unless they actively refuse it. In cases of refusal, an objection would be recorded in a centralized registry.

These legislative developments are anticipated to impact Swiss businesses, health care providers and citizens, all within an evolving data protection environment.

Back to Top ↑

Taiwan 🇹🇼

Contributor: Ken-Ying Tseng

Taiwan is poised for significant privacy developments in 2025 with the establishment of a new government agency, the Personal Data Protection Commission, slated for summer. This initiative follows an August 2022 decision by Taiwan's Constitutional Court, which mandated the creation of an independent monitoring mechanism to safeguard personal data.

A preparatory office of the PDPC has already been established to undertake necessary preparations, including issuing interpretation rulings as well as assessing potential amendments to the existing Personal Data Protection Act.

On 20 Dec. 2024, the preparatory office publicly released a draft bill proposing amendments to the PDPA, initiating a 21-day public consultation period, which was later extended to a 60-day period. The primary aim of the draft is to address the PDPC's establishment in 2025. It delineates the PDPC's role as the authority overseeing the PDPA, responsible for supervising other government agencies and coordinating with sectoral regulators at both central and local levels in regulating the private sector.

The draft also proposes certain significant changes affecting the private sector. Notably, it introduces major amendments regarding data breach incidents. Currently, the PDPA does not mandate data controllers to report data breaches to the regulator. The draft imposes a mandatory reporting obligation on data controllers to notify the regulator if a data breach poses a "potential significant risk of harm to the rights and interests of the data subjects."

Regarding notifications to affected data subjects, the existing PDPA requires data controllers to inform affected individuals of a data breach, regardless of the risk level or the number of individuals impacted. The amendment introduces a threshold for such notifications, aligning it with the threshold for reporting data breaches to the regulator. Additionally, the amendment establishes a new penalty scheme for noncompliance with the above reporting and notification requirements.

The amendment mandates designated privacy businesses to appoint a DPO to oversee personal data protection matters and assign personnel as data protection auditors to plan and conduct data protection audits. Furthermore, the draft amendment empowers the competent authority, in consultation with relevant agencies, to prioritize industries with higher risks of personal data breaches for administrative inspections.

There are also noteworthy developments concerning restrictions on cross-border data transfers. The sectoral regulator for the pharmaceutical industry is considering an order to prohibit pharmaceutical companies from transferring personal data from Taiwan to China and issued a new draft ruling for public comment in December 2024. According to the draft ruling, a pharmaceutical company may be allowed to transfer personal data to China if a data transfer agreement, akin to those in the EU, is established between the transferring and receiving parties.

With the PDPC's establishment on the horizon, it is expected the draft amendment will soon be forwarded to the Legislative Yuan, Taiwan's legislature, for enactment. Once operational, the PDPC will propose comprehensive amendments to the PDPA, potentially including significant changes such as the introduction of extraterritorial effects and restrictions on cross-border data transfers.

Back to Top ↑

Thailand 🇹🇭

Contributors: Athistha Chitranukroh, Gvavalin Mahakunkitchareon

Thailand's Personal Data Protection Act came into full effect 1 June 2022, and the Personal Data Protection Committee has since issued various subordinate regulations. These include regulations on security measures to be implemented by data controllers, data breach notification requirements, a mandatory obligation to appoint a DPO when the processing activity requires regular monitoring of personal data or a system due to the large scale of personal data, administrative measures, data processors' record of processing activities, data breach notifications, cross-border transfers of personal data including the criteria for the adoption of binding corporate rules and contractual clauses, and handling of data subject requests to exercise the right of erasure.

Some areas under the PDPA still require further clarification, and public consultations for the remaining draft subordinate regulations are anticipated in 2025. A potential area for further clarification is DPIAs, which are crucial for organizations and particularly for entities with establishments in other jurisdictions.

In July 2024, the PDPC announced the first decision of the expert committee —designated by virtue of the PDPA with the power to make determinations related to imposing administrative fines and other penalties — to impose an administrative fine of THB7 million against a data controller entity.

The entity allegedly committed three offenses related to the failure to implement appropriate security measures, failure to appoint a DPO as mandated and failure to comply with data breach notification obligations. The expert committee ordered the entity to rectify its noncompliance earlier in 2024, but it failed to do so, resulting in the administrative fine.

Enforcement in 2025 is expected to become more active and potentially more serious, which means organizations should pay closer attention to ensuring compliance with the PDPA.

Similar to the EU GDPR, the PDPA also has extraterritorial effect. The subordinate regulation on international cooperation to be issued by the PDPC should clarify how PDPA enforcement against organizations located outside of Thailand will be conducted by Thai regulators.

Silence surrounds the development of sector-specific data protection laws.

Back to Top ↑

Turkey

Contributor: Furkan Güven Taştan

Policy documents published by the Turkish presidency in recent years have outlined two legislative packages planned for reform. This year marked a milestone with the adoption of the first legislative package, which came into force in June 2024, addressing the processing of special categories of personal data, data transfers abroad and the competent court for monetary fines imposed by Turkey's DPA, Kişisel Verileri Koruma Kurumu.

Building on this momentum, the presidency published the Medium-Term Programme (2025-2027) and the Annual Programme for 2025. In these documents, the government outlined its intention to complete the harmonization process of Turkey's Personal Data Protection Law with EU regulations, primarily the GDPR. Accordingly, the second legislative package is being prepared and is scheduled for the fourth quarter of 2025.

Moreover, the documents also highlight the impact of the EU's digital economy rules on exporting goods and services. In other words, the regulations — namely the Data Act, Data Governance Act, Digital Markets Act and DSA — might soon become additional focuses for Turkey's government. For instance, the documents include initiatives to regulate the sharing of public data, with plans to launch a national open data portal.

In conclusion, Turkey's actions signal a commitment to full GDPR compliance. Despite these promising signs, it is important to note the country's ever-changing political climate can sometimes overshadow efforts to reform the data protection framework.

Back to Top ↑

Ukraine

Contributor: Natalia Kirichenko

In Ukraine, personal data protection is governed by the Law of Ukraine on Personal Data Protection, which is primarily based on the EU Directive 95/46 and Convention 108+. The existing law provides a foundational regulatory framework for data protection, covering essential aspects but lacking the comprehensive scope of the EU GDPR.

Although a new draft law that aligns with the GDPR is under consideration by the Parliament of Ukraine, its adoption is anticipated only after the martial law due to the ongoing war with Russia is lifted.

Ukraine is currently developing a regulatory framework for AI systems, including the protection of personal data. The Ministry of Digital Transformation developed a step-by-step introduction of regulation in the field of AI, which is described in its June 2024 white paper on the regulation of AI. The document establishes a regulatory strategy to integrate AI within existing data protection laws while aligning with future EU standards.

The proposed AI regulatory framework work consists of two main phases. The first phase of implementation is preparatory and involves the creation and implementation of nonlegislative tools to prepare for future mandatory regulation. This phase is expected to last two to three years.

In the absence of a legally binding and specific law on AI during the first stage, businesses and developers shall comply with relevant national laws that can apply to AI, such as constraints on automated decisions that affect individuals' rights.

The second phase envisions the adoption of mandatory AI regulations harmonized with EU legislation, covering areas such as personal data protection and the ethical use of AI.

Back to Top ↑

United Arab Emirates

Contributor: Motunrayo Ope-Ogunseitan

The United Arab Emirates is unquestionably a country at the center of technology disruptions and innovations, as it constantly opens to global players, leverages technology and invests in its data infrastructure. The UAE continues to pioneer growth in the Middle East with strategic partnerships and policy developments. Also noteworthy, in 2017, the country developed its Strategy for Artificial Intelligence with the goal to become a world leader in AI by 2031.

Data is at the center of technological advancements. Technology leverages data to build, assess and evolve products and services. Personal data is a very significant element of this, as businesses seek to gain insights from customer profiles to curate advanced customer journeys and increase demand.

Several countries have released data protection laws and frameworks to regulate the use of personal data. These include the EU, U.K., China, Qatar, Oman and Saudi Arabia. The UAE released its Personal Data Protection Law in 2021, however, the law is to be operationalized by executive regulations that have yet to be issued.

Considering notable developments across the region, including Saudi Arabia's Personal Data Protection

Law fully coming into effect after the one-year grace period for companies to achieve compliance, it is likely the UAE will follow suit in operationalizing its data protection law in 2025.

When this occurs, significant data processing changes are likely to occur across industries, especially high-risk industries like telecommunications, health care, hospitality and real estate. These industries in the UAE process massive volumes of personal data, which will have stricter processing requirements. Consent requirements, purpose limitation, data transfer restrictions and marketing limitations will be focal points for compliance.

It is noteworthy that the Dubai International Financial Center and Abu Dhabi Global Market, both in the UAE, have operational data protection regulations that apply to the regions independently. As we anticipate the UAE PDPL executive regulations, we will continue to watch the space while proactively leading privacy compliance in line with global standards.

Back to Top ↑

United Kingdom 🇬🇧

Contributor: John Bowman

The U.K.'s political landscape recently experienced a notable transformation, with the Labour Party assuming power following the general election 4 July 2024. This shift opened new avenues for establishing a clear direction in terms of privacy and AI policy.

Despite the change in government, the Labour administration's approach to privacy and AI policy is not substantially different from its Conservative Party predecessor. Although the latter was unable to pass its proposed Data Protection and Digital Information Bill before the election, the new administration promptly initiated its own legislative process with the first reading of the Data (Use and Access) Bill in the House of Lords 24 Oct. 2024. Given the government's substantial parliamentary majority, legislative process is anticipated to progress throughout 2025.

The DUA Bill is considered to be a pivotal piece of legislation by the government, promising significant economic benefits and improved data protection standards. It includes amendments to the U.K. GDPR and Data Protection Act 2018 regarding consent for processing personal data for scientific purposes and law enforcement. It also provides more clarity on claiming legitimate interest as grounds for processing and broadens the legal basis for using solely automated decision-making in certain situations.

One significant development in the bill is the alignment of the enforcement powers of the U.K. Information Commissioner's Office under the Privacy and Electronic Communications Regulations with those of the U.K. GDPR. This amendment increases the potential maximum fine for infringements from 500,000 GBP to 17.5 million GBP.

In 2025, several factors are expected to influence the U.K.'s data protection landscape, including the potential establishment of the Information Commission to replace the Information Commissioner's Office if enacted under the DUA Bill, the U.K.'s ability to issue its own data partnership agreements or adequacy decisions with third countries, and the European Commission's review of its own U.K. adequacy decision.

In the impact assessment for the DUA Bill, it was noted the government's "position is that the proposals within the Bill are 'essentially equivalent' and have the ability to preserve EU adequate status" and that the loss of adequacy "is a scenario the Government considers highly unlikely." The Commission's own view will be closely watched as it emerges.

While no legislation that specifically addresses AI governance has been announced yet, AI is a high priority for the government. For instance, the government recently published a report examining the U.K. AI assurance market with a view to driving its future growth. It also launched a consultation on the design, content and use of a new AI Management Essentials tool. For the time being, U.K. regulators such as the

ICO will continue to apply cross-sectoral responsible AI principles under existing powers.

Back to Top ↑

United States 🇺🇸

Federal law

Contributor: Joe Duball

Potential U.S. comprehensive privacy legislation and broader AI guardrails could be a ways off heading into 2025. The recalibration of U.S. Congress and the White House after the 2024 election may render the illusion of opportunity, but the Republican trifecta may have loftier priorities on its policy agenda.

Congress quarreled over two comprehensive privacy proposals in consecutive years, with familiar disagreements over a private right of action, federal preemption and civil rights protections. Those disagreements leave a perceived gap that is proving to be too complex to close.

AI legislation garnered a similar lack of consensus among Congress. The additional wrinkle for 2025 is incoming President Donald Trump, who signaled a rollback of past AI governance initiatives under President Joe Biden with an eye toward more innovation.

Questions around chairs of the House and Senate committees handling any AI or privacy bills are additional reasons to believe both topics will be shelved.

The House Committee on Energy and Commerce is losing Chair Cathy McMorris Rodgers, R-Wash., a noted privacy torch carrier in the 118th Congress. Meanwhile, Sen. Ted Cruz, R-Texas, is expected to take the gavel in the Senate Committee on Commerce, Science, and Transportation, where he previously showed little appetite for meaningful AI and privacy bills that came about while he was ranking member.

If a Republican groundswell around privacy does occur in 2025, past debate shows any potential bill will likely focus on solid preemption paired with other business-friendly provisions taken from state-level initiatives, such as the right to cure, narrowed applicability and simplified definitions.

In the absence of federal action, state legislatures will continue to work diligently on comprehensive AI and privacy bills as they have in recent years.

States without a comprehensive privacy law on the books are likely to find an easier path to passage based on palatability alone with 19 enacted bills around the country to consider. Maine, Pennsylvania, Wisconsin and Vermont may look to revive and complete prior efforts on comprehensive bills.

Federal Trade Commission

Contributor: Cobun Zweifel-Keegan

After a contentious election, the U.S. is preparing for a new year distinguished by markedly different policy priorities in the federal executive branch.

Though the Federal Trade Commission is an independent agency, which inoculates it from direct interference by Congress or the president, the chairmanship of the agency — and thus its general policy direction — will be determined by incoming President Donald Trump.

This means Chair Lina Khan's controversial term at the head of America's de facto DPA will come to an end. The new era will likely signal a new approach to the FTC's competition enforcement. In contrast, overall consumer protection enforcement, including privacy matters, is likely to remain relatively stable. After all, data privacy remains a bipartisan priority. The two sitting Republican commissioners, Andrew Ferguson and Melissa Holyoak, have made their support for most of the FTC's recent privacy enforcements clear, with some marginal disagreement about tone and scope.

Nevertheless, there will be changes. For one, we are unlikely to see a continuation of the FTC's proposed Trade Regulation Rule on Commercial Surveillance and Data Security. The next step of the rulemaking process would be to release a draft rule narrowing the scope of the proposed regulation, but most Republicans have made clear they do not support this regulatory project and would prefer the FTC to focus on one-on-one enforcement in the privacy arena.

Another area seeing ongoing rulemaking is the update to the Children's Online Privacy Protection Act. This process was started during the first Trump administration and reopened for additional comments under Khan. Whether the FTC finalizes the update or again asks for additional comments, we are likely to see a continued emphasis on modernizing the COPPA, a process that has been a tad delayed compared to the usual 10-year updates. This might dovetail with the ongoing priority of the U.S. Congress to pass kids safety and privacy laws extending to teens, which may finally find purchase in 2025.

Though privacy enforcement will continue apace, we may see different priorities when it comes to AI enforcement. The type of settlement seen in the Rite Aid case, banning certain practices and mandating a detailed AI governance program, is less likely to be seen under the next FTC. But bipartisan support remains for continuing basic consumer protection enforcement related to AI systems, such as ensuring claims made in the marketplace about accuracy are not deceptive.

In short, 2025 will start out with a lot of uncertainty for the FTC but will likely settle into a new era with continued robust engagement from the top U.S. privacy enforcer.

Health care

Contributor: Kirk Nahra

The word for U.S. health care privacy in 2024 was chaos.

Lots of new laws impacted a broad range of overlapping activities, entities and information. These changes are leading to a growing web of complexity in what was once a relatively stable environment.

For 2025, we will be watching whether the fits and starts of new legislation from 2024 will carry over into the new year and whether these developments will, in fact, improve overall privacy issues and/or make the health care system increasingly challenging.

Most of the actual impact in 2024 stemmed from state laws, including the growing array of state "comprehensive" privacy laws, which fill in a range of gaps that exist in privacy protection for health care information, new consumer health laws such as Washington state's My Health My Data Act and the growing range of Dobbs-related laws.

While health care is not driving the broad range of comprehensive state privacy laws, we expect more in 2025, with the expectation that these laws will continue to exempt Health Insurance Portability and Accountability Act covered companies from their scope and likely continue a recent trend of adding additional consent requirements for the processing of health care data.

For consumer health data, 2024 led to passage of the first laws in this category, but the expected onslaught of additional laws and class action litigation has not yet materialized. We can expect the charged political climate for this area, which had its start in Dobbs-focused activities, will lead to more states passing laws, some rise in class-action lawsuits, which may impact whether new states add a PRA in this area, and perhaps initial enforcement activities.

At the federal level, separate from whether a federal privacy law will move at all, there continues to be a vacuum on leadership on health privacy issues. The health care industry wants to be carved out of the law, and has been successful so far, but that leaves few knowledgeable health privacy experts with any relevant vested interests involved in the discussion. So, if a federal law moves in 2025, it likely will make the overall state of health privacy worse rather than better.

Back to Top ↑

Uzbekistan

Contributors: Sarvarbek Olimjonov, Malika Murodova

Data protection regulations in Uzbekistan began to take shape in 2018-19 with the introduction Decree no. 707 of the Cabinet of Ministers on Measures for Improving Information Security in the Global Information Network Internet and the Law on Personal Data, both of which were later strengthened by regulatory developments in 2022 and 2023.

During this period, the Cabinet of Ministers and Ministry of Justice issued key resolutions establishing rules for personal data processing and clarifying the responsibilities and operational standards for data owners and operators. These reforms introduced various procedural and technical requirements for data protection, including defining protection levels, setting cross-border data transfer standards and addressing data protection in cyberspace.

However, enforcement mechanisms for addressing personal data breaches, particularly in cyberspace, remain problematic due to insufficient staffing within the Personalization Agency under the Ministry of Justice, overlapping regulatory mandates, and ambiguous provisions governing the allocation of responsibilities and corrective measures in data processing violations.

A major anticipated reform in Uzbekistan should aim to simplify the procedure for addressing breaches of personal data laws within cyberspace by consolidating the management of the data breach registry. Currently, both the State Inspection Agency, Uzkomnazorat, and the Personalization Agency under the Ministry of Justice share responsibilities; the Uzkomnazorat maintains the registry, while the Personalization Agency publishes it. This division creates redundancies and inefficiencies, requiring multiple compliance stages.

At present, the process involves three steps: the Center for Mass Communications reports data processing violations within 24 hours, the Personalization Agency reviews the report within the next 24 hours and the Uzkomnazorat issues directives to data operators, setting deadlines for corrective actions.

This multistage procedure complicates the registry's efficient operation and increases administrative burdens.

In addition, a lack of clear restrictions on the use and dissemination of personal images without consent remains. Although Uzbek law permits individuals to provide data processing consent in any form, the absence of specific guidelines for obtaining consent in cases involving video surveillance has led to unauthorized publication of personal images in media and online, suggesting this will be an area of regulatory focus moving forward.

Ultimately, by addressing staffing shortages, clarifying regulatory mandates and consolidating enforcement procedures, Uzbekistan can improve the effectiveness of its data protection regime.

Back to Top ↑

Vietnam

Contributors: Athistha Chitranukroh, Tram Ngoc Bich Nguyen, Quang Minh Vu

As promised, regulators in Vietnam have been active in continuing to strengthen the personal data protection framework with new regulations in the regulatory pipeline.

The Department of Cybersecurity and High-Tech Crime Prevention is currently developing a new Personal Data Protection Law. The first draft was released in September 2024 and retains most of the regulations of the Personal Data Protection Decree adopted in 2023 — notably the consent-centric approach, the broad definition of sensitive personal data, the data subject rights and timeline to respond, and stringent notification requirements in case of violation of personal data protection regulations.

The draft includes many new additions, including specific regulations applying to AI, big data, employment, biometrics and geolocation processing. The burdensome requirements to establish and submit impact assessment dossiers to the department are retained. The draft law also introduces a new requirement for entities processing sensitive personal data — still broadly defined to cover almost all processing entities — related to the "trust" rating, which is basically a note given to the enterprise from a trust rating service provider to attest to the seriousness of the internal data protection culture of an entity. Qualification requirements for DPOs are also more detailed.

In addition, the draft Digital Technology Industry Law is intended to be submitted to the vote of the National Assembly in May 2025. This law will continue to shape Vietnam's digital economy with specific regulations now addressing AI, big data and cloud computing, to name a few.

Adopted by the National Assembly 30 Nov. 2024, the Data Law imposes, among other things, the obligations to provide information to the Vietnamese authorities upon request in certain circumstances. The cross-border transfer of core and important data, both broadly and unclearly defined, will be elaborated in detail by the government in a future decree guiding the Data Law.

Although administrative enforcement action against data-related violations has yet to start in Vietnam, with the development of the sanction decree on hold, the DPA is expected to proactively monitor compliance with personal data protection regulations in the country in the future, with a special focus on illegal data trading. Legal reforms to impose criminal liability for illegal data trading are currently being contemplated. The DPA promises to remain active in 2025 and to keep compliance departments busier than ever.

Back to Top ↑

Zimbabwe

Contributor: Tsitsi Mariwo

Zimbabwe has adopted a proactive regulatory approach to the processing of personal data by approving and issuing five regulatory guidelines for individuals and entities on matters related to personal data protection.

In particular, the Postal and Telecommunications Regulatory Authority issued guidelines on cross-border transfer of personal information, data breach management, children's data processing, consent and DPO appointments.

In 2024, the authority made strides in deepening international cooperation and exchanging notes and ideas with other DPAs. After applying for membership in July 2024, Zimbabwe attended the Global Privacy Assembly for the first time. The country was admitted to the Global Privacy Assembly on 1 Nov. 2024, demonstrating the its commitment to collaborate with other authorities in advancing the right to privacy.

2024 also saw efforts directed toward the operationalization of the Cyber and Data Protection Act through various interventions. On 13 Sept. 2024, the government promulgated the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations under Statutory Instrument 155 of 2024. The regulations provide for data controller license categories and fees; the qualifications, functions and appointment of DPOs; the procedure for reporting data breaches; obligations of data controllers; capacity development; and certification. Training and capacity-building initiatives to create a critical mass of data privacy practitioners were also pursued with various industry players.

Going forward to 2025, the authority will consistently forge partnerships with other supervisory authorities to enhance capacity development and enforcement particularly from those that have made noteworthy progress in operationalizing data protection laws.

It will also assist new authorities with the necessary support required to get off the ground. In addition, the authority intends to develop more guidelines to assist organizations with compliance to the provisions of the act. Continuous capacity development through various partnerships, as well as stakeholder engagement to enhance the legal and regulatory framework, will also be high on the agenda.

Back to Top ↑