IAPP Global Legislative Predictions 2024

Argentina

Contributors: Pablo Palazzi

Argentina and other countries in the region, including Chile and Colombia, are discussing bills to amend and update data protection laws. Discussions are expected to take place across the region in 2024 and in the international fora as well.

On 30 June 2023, Argentina's executive branch sent the proposed Personal Data Protection Bill to the National Congress for consideration. Drafted by Argentina's data protection authority, the Agency of Access to Public Information, the bill seeks to amend the current Personal Data Protection Act.

The Personal Data Protection Bill is based on international and regional standards, recommendations and principles, including the EU General Data Protection Regulation, Convention 108+, the Standards for Personal Data Protection for Ibero-American States, and other Latin American countries' regulations on personal data protection and privacy. While the bill was drafted in open consultation with academia, international experts, nongovernmental organizations, companies and several government agencies, it has faced some objections and debate will take place in the National Congress in 2024.

The bill introduces definitions, principles and rights often seen in modern data privacy legislation, including privacy by design and by default, privacy impact assessments, accountability obligations, the obligation to appoint a data protection officer and legal representative for foreign companies, extraterritoriality provisions, data breach notifications, detailed regulation of international transfers of personal data, and portability rules. There are also specific regulations for credit reporting, automated decision-making and marketing, and rules for habeas data actions. The bill also grants the AAIP new powers, including the ability to halt personal data processing or activities that may affect users' privacy.

The PDPB introduces a new fine system based on units — a unit is 10,000 pesos — the value of which will be updated by the AAIP annually. If approved, the bill allows the AAIP to sanction companies five to 1 million units, or 2-4% of the company's global annual turnover. This has faced criticism since the use of global annual turnover may affect global companies and increase fines. An Argentine company with branches in Brazil, Colombia and Mexico could be fined based on regional global income, for example.

Other areas of concern include the bill's set age of 16 years old for children's consent and a provision stating the local representative of foreign companies can be liable in case the company it represents does not answer a data subject access request.

Argentina was the first Latin American country to have an adequacy determination from the European Commission and it appears this bill seeks to preserve this status as most of its provisions follow GDPR standards.

Once approved, the PDPB would be effective six months after publication in the Official Gazette. However, the new fines would be applicable immediately upon publication of the law.

Australia

Contributors: Anne Petterd

The start of 2024 will likely see the release of at least some proposed amendments to the Australian

Privacy Act 1988, following the long-running review of the legislation. The federal government's 2023 response to the Privacy Act Review Report stated it agreed with 38 amendments and "agreed-in-principle" with another 68 proposals subject to further consultation.

Agreed upon amendments included regulating information used in automated decision-making, facilitating cross-border transfers, and clarifying and enhancing information security requirements.

The precise details of the amendments and their impact on current practices will no doubt be the subject of much debate. Many interested parties will also be awaiting the government's roadmap for amending the legislation. For instance, how long will further consultations take and how will amendments be staged? Another critical implementation question on people's minds will be the length of any transition period to implement changes to systems and processes.

Regardless of the extent and pace of any amendments to the Privacy Act, in 2024 we will almost certainly see a continued focus by the Office of the Australian Information Commissioner and other interested government regulators on some of the hot topics from the past two years. This will likely include continued focus on data breaches, their causes and whether businesses are doing all that is expected of them to protect personal information — in particular, are they applying adequate security measures and appropriate data retention practices? Another key area of regulator focus will likely be responsible and transparent processing of personal information, especially for vulnerable groups such as children.

For the public sector, new and imminent public sector data breach notification schemes in New South Wales and Queensland will also keep privacy considerations at the forefront for state government agencies.

Austria 🇦🇹

Contributors: Andreas Zavadil

Landmark decisions from the European Court of Justice can be expected in 2024 that will be relevant for the practice of companies and data protection authorities.

One decision revolves around the imposition of fines on legal persons, which could fundamentally change the procedure of administrative fines in Austria. Another involves the question of whether the Austrian Data Protection Authority is competent to supervise legislative bodies. This decision will also have a major impact on data subjects and their data protection rights in Austria.

Finally, the upcoming year will continue to be dominated by new legal acts in the EU. On a national level, the accompanying law to the Digital Services Act recently went into public consultation. All new regulations have implications for data protection law, especially since the GDPR will have to be applied in parallel.

Belgium 🇧🇪

Contributors: Charles Helleputte

Asked in November 2023 whether there were more chances for the EU AI Act to be adopted by the end of the year than for Belgium to finally have a functioning Belgian Data Protection Authority, a large language model provided an interesting response. It stated we will see both the EU AI Act adopted and the Belgian Data Protection Authority "continue to operate independently to protect the rights of citizens."

Let's hope the capital of Europe will not be known anymore for its misfunctioning authority, but rather for its — still to be done — pioneering efforts to create a regulator that will tackle both privacy and AI responsibly.

What is for sure, though, is that the Belgian legislative landscape in 2024 will be heavily influenced by what the EU agreed to, or will be able to agree upon and pass, in the last round of its digital strategy. After a very productive period of EU secondary laws in the digital space, time to digest and implement has come.

No doubt that Belgium, like many EU member states, will play catch-up in 2024. One hope? That implementation of the Network and Information Security Directive (NIS2), which has so many overlaps with privacy, will run smoother than what we saw for NIS1.

But in 2024, even with EU institutions on pause due to upcoming elections, eyes will still be on the Brussels EU-bubble. What for? Think of the new European Data Protection Board strategy, which will set the tone of activities across the EU, and upcoming reform of the GDPR that comes under assessment, again. Privacy is a Sisyphus task.

Bermuda 🇧🇲

Contributors: Nancy Volesky

No longer the subject of speculation, entities in Bermuda now have only one year to become privacy compliant. In 2023, Bermuda's government announced all remaining provisions of the Personal Information Protection Act will come into effect 1 Jan. 2025. The PIPA applies to all organizations using personal information in Bermuda. Full implementation was contrary to an anticipated phased approach, so 2024 will entail a mad dash to the compliance finish line for many.

Bermuda's legislative framework around personal information protection will continue to see activity. Having passed the Personal Information Protection Amendment Act 2023, which aligns the PIPA with the 2010 Public Access to Information Act, the government is set to further its work by harmonizing the PIPA and the Electronic Transactions Act. The Legislature of Bermuda will also consider a cybersecurity bill and the Digital Identity Service Provider Act.

This year, the Office of the Privacy Commissioner for Bermuda will augment its existing guidance, training, tools and resources, providing additional certainty and clarity for the public and organizations ahead of PIPA's January 2025 deadline. PrivCom's compliance and enforcement staff will also be deep in preparations. As a member of the Global Privacy Enforcement Network, and the Global Privacy Assembly's Global Cross Border Enforcement Cooperation Arrangement, PrivCom may partner in joint investigations with global regulators, and individuals and organizations should do well to take note. Emerging technologies, including AI, are also on PrivCom's radar and more information on this topic is expected.

Bolivia 🇧🇴

Contributors: Ana Valeria Escobar

Bolivia continues to wait for a specific data protection framework that materializes much-needed changes in data privacy and protection.

While two draft regulations have been proposed, it is highly likely the draft promoted by the Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación will be the one that frames privacy regulations in Bolivia.

AGETIC's proposal follows GDPR guidelines, notably establishing an obligation for personal data controllers or processors not domiciled in Bolivia to appoint a legal representative in the country, extraterritorial scope, the Personal Data Protection Authority, and an obligation to register databases.

Considering the increasing importance of data privacy and protection, Bolivia stands at a critical juncture in shaping its regulatory framework. The government should prioritize the development and enactment of comprehensive data privacy legislation to safeguard the rights and personal information of its citizens while fostering trust in the digital economy. We expect to see advances within the year.

Brazil

Contributors: Angela Fonseca

As privacy breaches unfortunately become commonplace, Brazilian legislators have been catching up with constituents' demand for increased disclosure of security incidents. Brazil's General Data Protection Law currently states breaches that "may cause risk or relevant damage to data subjects" must be reported to the National Data Protection Authority. The proposed House of Representatives Bill 1876, which is expected to mature into law by the end of 2024, aims to extend that disclosure obligation to "mass circulation media outlets, their webpages and online profiles."

Also in progress on the legislative front, and expected to mature into law in 2024, are tax incentives for companies to implement LGPD into internal processes, Senate Bill 4 of 2022, and regulation of AI, SB 2338.

The tax incentives include a deduction of direct and indirect costs associated with privacy consultants, software and more in the calculation bases of certain social contributions, to encourage companies to implement good privacy governance.

The AI bill focuses on protecting individuals from the negative impacts of automated decision-making. More specifically, it foresees the right of information of the AI system rationale, nondiscrimination and correction of indirect discriminatory biases, and the right to demand human intervention — which shall be easily accessible. The bill also features the creation of an AI authority and administrative sanctions.

On the ANPD front, the regulatory schedule for 2023-24 may suffer some understandable delays in the context of an authority "under construction." Some topics on the 2023 roadmap, such as international data transfers and data protection impact assessments, are yet to be seen in 2024.

Finally, the ANPD released a regulatory sandbox report, including a thorough benchmark with local and international authorities. Though it's not yet a specific sandbox program, it's a steppingstone for the progressive engagement of ANPD in future regulatory experiments.

Canada

Contributors: Shaun Brown

The biggest potential development to follow in Canada in 2024 is Bill C-27, introduced in June 2022, which would replace the federal Personal Information Protection and Electronic Documents Act with the Consumer Privacy Protection Act and create the Artificial Intelligence and Data Act.

This is important for several reasons, including the fact that federal privacy legislation would include penalties for the first time. The parliamentary committee reviewing the bill began its work in September, so it is conceivable the bill will be passed in 2024. The CPPA would likely not come into force for at least a year after passage, and the fate of AIDA is less clear, given the extreme challenges in regulating AI. It is possible the AIDA is passed without ever coming into force.

In Quebec, most of the significant changes under Law 25, including GDPR-like penalties, came into force in September 2022. It will be important to watch for guidance or enforcement activities from Quebec's Commission d'accès à l'information as there is a lot of uncertainty around how the new requirements apply in practice.

Although there are no other major legislative developments on the horizon, the Ontario government is in the process of finalizing the administrative monetary penalty regime under the Personal Health Information Protection Act through regulations, and it would not be surprising to see more proposals for penalties under provincial private and health sectors.

Chile 🇨🇱

Contributors: María José Díaz, Javiera Sepúlveda

Changes in the data protection and cybersecurity fields are expected to continue to be discussed in Chile throughout 2024. Last year, we were hoping for approval of the data protection bill that would completely modify the current local data protection regulation, closely following the GDPR. Unfortunately, its debate did not move as fast as expected.

However, it's been announced the parliamentary debate will soon be reactivated and projections suggest 2024 will finally mark the completion of this long-anticipated legislation. Once approved, the bill will become legally enforceable two years after its publication.

Additionally, a crucial debate has and will continue to take place in the National Congress of Chile concerning the bill to establish a framework law on cybersecurity and critical information infrastructure. The bill would create new public institutions and set forth a comprehensive regulatory framework for the development of cybersecurity, which is inexistent to this day except for regulation applicable to specific industries, such as those governing banks and financial institutions. Last April, the bill advanced to the second of three phases of the legislative process.

Also, an important law passed at the beginning of 2023 regarding the financial technology industry: Law 21.521, which promotes competition and financial inclusion through innovation and technology in the provision of financial services and creates an open finance system in Chile. The law contains a robust regulation for the protection of financial consumers' data, particularly regarding the open finance system, the first specific regulation of which is expected to be issued by the financial authority during the first half of 2024.

Lastly, we expect discussion to continue in Congress around other important but smaller bills, including legislation to create a consolidated debt register that, among other things, seeks to strengthen the protection of debt data, establishes the right to be forgotten in financial matters, and introduces some information security obligations.

China 🇨🇳

Contributors: Barbara Li

China's data protection and privacy legislative regime has been evolving extremely fast. 2024 will continue to be a year with active legislative and enforcement developments.

China's central government identified the digital economy as a priority industry for economic development in 2024. As an important national governmental agency in China, the National Data Bureau formally started operation in October 2023. It will work closely with the Cyberspace Administration of China, but with a different focus. The NDB is charged with formulating and implementing strategic national policies to promote the investment and development of the digital economy and facilitating the leverage and utilization of data assets. At the same time, the CAC will continue to regulate data protection, privacy and cybersecurity.

We expect new laws and regulations will be issued and implemented to reflect such a balanced approach.

At the end of September 2023, the CAC issued draft regulations on Regulating and Promoting Cross-Border Data Flows for public consultation. Compared with the existing Chinese Standard Contract Clauses regime, the draft regulations will remove or relax certain restrictions for outward data transfers from China, if finalized and implemented. The consultation ended and we expect the final version of the regulations to be issued and adopted in 2024.

Regional rules for the relaxation of cross-border data transfers are also expected. In December 2023, the CAC and the Innovation, Technology and Industry Bureau of Hong Kong issued the guidelines to launch a pilot program, streamlining the arrangements on cross-border data transfers within the Guangdong-Hong Kong-Macao Greater Bay Area.

China has set up 24 free trade zones where local authorities are empowered to adopt certain flexibilities for business organizations registered in the zones. Some major free trade zones in Shanghai, Beijing, Hainan and Zhejiang, among others, are likely to pass local rules to promote orderly and efficient data flows. Other important data regulations on the horizon include the rules on important data, critical information infrastructure, personal information compliance audits, and data breach reporting. The regulators have issued the consultation draft of those rules in past months, and we expect that those important rules will be finalized in 2024.

1 Jan. 2024 will be the effective date of two important data regulations: Regulations on the Internet Protection of Minors, which impose enhanced compliance requirements for the protection of minors' personal information; and the Interim Provisions on Accounting Treatment of Enterprise Data Resources, which provide that qualified data resources can be reflected in balance sheets of enterprises, thus creating new value for enterprises.

On the enforcement front, Chinese regulators have taken multiple rounds of investigations in 2023 and business entities, across industries and of varying size, were caught and penalized. It is anticipated regulators will remain active in enforcement actions in 2024, so it is enormously important for business organizations to keep close watch on data legislative and enforcement developments in China and strategize compliance steps aligned with business priorities.

Colombia 🇨🇴

Contributors: Luis Alberto Montezuma

2023 ended with the entry into force of Law 2300 of 2023, embedding strong measures prohibiting debt collectors from contacting individuals through email, telephone, mobile or SMS outside the hours of 7 a.m. and 7 p.m., Monday through Friday.

The superintendent delegate for the protection of personal data of the Superintendence of Industry and Commerce of Colombia actively participated in the Ibero-American Data Protection Network. In a coordinated action, the data protection authorities launched a dedicated task force to foster cooperation and exchange information on possible enforcement actions conducted against ChatGPT. The RIPD also adopted declarations on the impact of neurotechnology and neurodata on privacy, and digital violence toward women and girls.

Although Colombia's Ministry of Commerce, Industry and Tourism has shown no interest in modifying the current Law 1581 of 2012, inspired by the EU Data Protection Directive, Congresswoman Maria Fernanda Carrascal introduced Bill 156/2023C to enact a personal data protection regime. The bill would maintain, modernize and extend existing rules and impose new requirements on public entities and organizations for the protection of personal data, including instituting the principle of technology neutrality contract and legitimate interest as legal bases and data protection impact assessments. It would also update requirements around processing of personal data in the employment and business-to-business context, use of CCTV systems, whistleblowing channels, tracking technologies, and AI and automated decision-making for the digital era. The bill would continue and enhance the role of the Superintendence of Industry and Commerce in overseeing organizations' compliance with the new requirements.

Unlike the GDPR and other modern privacy laws in China and the U.S., Bill 156/2023C seeks to address challenges of automated processing of neurodata. Industry representatives and stakeholders have raised concerns about the potential regulatory impact and the need for further consideration of such a proposal to strike an appropriate balance and understanding by individuals and organizations.

Another matter that may concern stakeholders is that organizations and people using personal data for journalism would be required to comply with the principles of data minimization and accuracy, and to ensure the right to correction could limit the right to freedom of expression and information under Article 20 of the Constitution of Colombia.

The bill was referred to the Standing Committee on Constitution of the Chamber of Representatives for further consideration. To pass, it requires majority approval from members of both chambers, which must be completed within a single legislative year. This procedure also includes prior revision by the Constitutional Court.

Costa Rica

Contributors: Daniel Rodriguez Maffioli

2022 and 2023 marked significant progress in the proposal of digital and tech-related bills in Costa Rica, setting the stage for potentially fruitful outcomes in 2024. Among these is Bill No. 23097, the Data Protection Law, introduced in 2022. The bill proposes a comprehensive overhaul of data protection legislation, aligning with global standards such as the GDPR. Despite some delays due to last-minute concerns raised by certain political parties, its advanced stage in the legislative process suggests a strong possibility of being passed in the coming year.

Another key bill, No. 23292, titled "Cybersecurity Law of Costa Rica," was also introduced in 2022 in response to severe cyberattacks that affected the country and government institutions earlier that year. It focuses on the protection of critical information infrastructures, stipulating obligations for their providers, creating a cybersecurity agency, and setting minimum information security standards for the public sector. While its prospects for approval in the next year are moderate, the bill has undergone several revisions. Lawmakers are meticulously reviewing the text to ensure the final version is both technically robust and enjoys consensus, which is a promising sign of its thoughtful and thorough consideration.

In other matters, as 2023 marked an important year globally for AI, for Costa Rica it meant the introduction of two bills on the subject. The first among these, Bill 23.771, is notable for having been drafted by AI itself, specifically Open AI's ChatGPT software after being given a prompt by the proponent deputies. However, there are low expectations for the bill's progress due to this particularity.

The second proposal, Bill 23.919, represents a more comprehensive legislative effort, covering ethical principles, specific rules for high-risk uses of AI, transparency rules and sanctions against the use of AI in false content. While 2024 is anticipated to be a crucial year for advancing discussion around the bill, influenced by feedback from various sectors, it may not necessarily culminate in its approval. However, the possibility of its future passage remains open, signaling a growing recognition of the importance of AI regulation in the country's legislative agenda.

Cyprus

Contributors: Christos Makedonas

Entering 2024, the Republic of Cyprus is at a pivotal moment in its journey toward enhancing data protection and cybersecurity. The past year marked a series of significant regulatory and collaborative efforts, particularly in the wake of cybersecurity incidents that impacted key institutions, including universities and the republic's land registry.

The Office of the Commissioner for Personal Data Protection intensified GDPR enforcement, not only conducting random audits across various organizations to ensure compliance but also organizing comprehensive training sessions. These initiatives aim to elevate awareness and understanding of data protection regulations, thereby fostering a culture of data security and compliance.

The commissioner also signed a memorandum of collaboration with the Office of Commissioner of Communications, particularly pertinent in the context of recent cybersecurity breaches and highlighting the need for coordinated data protection strategies. The agreement is significant in its focus on two crucial areas: the mandatory disclosure of personal data breaches by providers of publicly available electronic communication services and addressing breaches involving entities operating essential services, critical infrastructure, and digital service providers.

Adding to the regulatory landscape are several impending compliance deadlines that are shaping organizations' cybersecurity strategies. The Digital Operations Resilience Act, which mandates compliance from financial services entities by 17 Jan. 2025, is a key framework aimed at enhancing the operational resilience of the financial sector against cyber threats. Additionally, the Cyprus Securities and Exchange Commission has directed entities under its authority to align with the European Banking Authority's Information and Communication Technology guidelines by June 2024. Furthermore, the NIS2 Directive, expanding the scope and strengthening the security requirements of the Network and Information Systems Directive, plays a crucial role in the evolving cybersecurity environment.

On top of these regulatory measures, the commissioner is also actively engaged in reviewing the cookie policies and practices of various entities, including scrutinizing websites' policies to ensure they comply with data protection standards and respect user privacy. This initiative is a vital component of broader efforts to safeguard personal data in the digital realm.

As Cyprus navigates through these developments, there is an anticipated increase in demand and investment in cybersecurity and data protection across multiple sectors. Organizations are expected to enhance their cybersecurity infrastructures, invest in state-of-the-art technologies, and embed cybersecurity awareness into their operational ethos.

2024 is set to be a transformative year for data protection and cybersecurity in Cyprus. The combination of rigorous regulatory measures, proactive enforcement actions, and the response to recent cyber incidents is steering the nation towards a more secure and resilient digital future. Cyprus' approach, characterized by stringent compliance, collaboration and capacity building, not only addresses immediate challenges but also sets a commendable example in managing cyber risks and safeguarding personal data on a global scale.

Czech Republic 🇨🇿

Contributors: František Nonnemann

In 2024, we do not expect significant changes to the general rules on personal data protection in the Czech Republic.

However, several legal acts should be adopted to update and specify rules for data processing, use and protection. This is in two main areas: better use of data, following new data regulation in the EU, and in the information security area.

A draft implementing act of the EU Data Governance Act has been submitted. The proposal aims, among other things, to ensure that data held in public administration registers, records or other evidence becomes a stand-alone artifact with its own life cycle and value that can be used by other users of the data, including members of the public.

Another important piece of legislation is the draft amendment to the Freedom of Information Act, specifying the range of entities obliged to provide information, including personal data under some circumstances. The draft clarifies the concept of a public institution, which are also obliged to publish information about their activities.

Cybersecurity is another area in which legislative changes are expected. The Czech Republic has begun transposition of the NIS2 Directive. A new draft law on cybersecurity and six implementing decrees are in the legislative process. The new legislation will impose obligations — administrative, organizational and technical measures — on a number of new organizations and sectors. Subjects regulated by cybersecurity legislation in the Czech Republic are expected to increase to more than 6,000, from a few hundred under current legislation, under the NIS2 Directive and the proposed cybersecurity legislation.

The Czech Republic is also expected to pass its first comprehensive class action law in 2024, transposing the EU directive on representative actions for the protection of the collective interests of consumers. Consumers, or data subjects in the data privacy jargon, should be able to exercise their rights collectively if they are affected by, among other things, unlawful processing of personal data or a data breach affecting their rights. This new legislation will both strengthen the position of data subjects and the GDPR risk appetite of personal data controllers.

European Union 🇪🇺

Contributors: Isabelle Roccia

Legislative activity in the EU will be split before and after the June 2024 European elections. The first trimester will be devoted to closing as many of the 150 or so pending legislative files across policy areas, while the third and fourth trimesters will focus on establishing the incoming EU leadership and its priorities for the next five years. The makeup of the new European Parliament in June will determine the appointment of the president of the European Council and the political composition of the European Commission — expected to take office in the fall.

Among others, the EU's Data Act entered into force in January while the Artificial Intelligence Act should be finalized by April. The European Commission will kick off its voluntary Cookie Pledge in the spring as well as release its second GDPR evaluation report. However, several privacy-relevant proposals may not be finalized before the elections, including the GDPR enforcement and harmonization proposal, data space legislative proposals for health and financial services, and the draft AI liability directive among many others. Negotiations of these proposals will continue after the elections.

In parallel, we expect European regulators to increase the level of activity and enforcement we saw in 2023 across priority areas such as ad tech, cookies, children's privacy, and legal basis for processing. The new EDPB chair, elected in May 2023, will unveil her strategy early 2024. It may address the evolving roles and responsibilities of regulators in light of new EU laws developed under this finishing legislative term. The EDPB will also address the findings of its report on the appointment and role of data protection officers published in January. This should lead to further enforcement as we expect data protection authorities will find GDPR requirements are not met by all the 700,000 organizations with a registered a DPO in Europe.

Last but not least, we will continue to see impactful rulings from the Court of Justice of the European Union, as demonstrated through the past year.

Finland 🇫🇮

Contributors: Eija Warma-Lehtinen

Head of the Finnish Data Protection Authority Anu Talus was elected chair of the European Data Protection Board on 25 May 2023. Talus has said the EDPB will shift focus from guidance to enforcement in the coming years.

In May 2023, the Nordic Data Protection Authorities from Denmark, the Faroe Islands, Finland, Iceland, Norway, Sweden and Åland held the annual Nordic Data Protection Meeting in Reykjavik, Iceland, where they agreed to strengthen cooperation.

The Finnish DPA emphasized the importance of consistent and clear implementation of the new data regulation package. The Finnish DPA should be the local supervising authority for all data protection-related regulations. Any other solution could lead to inconsistencies in supervision. It will be interesting to observe the outcome regarding these local supervisory powers.

A new government of Finland was appointed in June 2023. The government program states the need for administrative fines to public sector organizations will be evaluated as administrative fines for public sector organizations are currently not imposable. The Finnish DPA supports this and sees the evaluation as important.

France 🇫🇷

Contributors: Cécile Martin

France's data protection authority, the Commission nationale de l'informatique et des libertés, outlined three areas of focus within its 2022-24 strategic plan, given new challenges presented by the increasing digitization of our society.

The CNIL will focus on promoting better control and respect for people's rights in the privacy field. It intends to act on several fronts in France, but also at the European level. While the CNIL plans to locally increase its communication efforts and publish tools to facilitate this exercise, it also seeks to reinforce the effectiveness of individuals' rights and organizations' compliance with the GDPR by implementing a dissuasive and proportionate repressive policy within tighter deadlines. To this end, the CNIL is adapting its control, formal notice and sanction procedures. In addition, the regulator intends to increase the effectiveness of the "one-stop shop" mechanism and pushes for concerted actions within the EDPB.

Promoting the GDPR as an asset of trust for companies will be the CNIL's second area of focus. One of the tools the CNIL underlines to reinforce the efficiency of the GDPR is the certification and code of conduct process. According to the CNIL, these tools are powerful given they enable controllers to take charge of compliance in a way that is adapted to their specificities. Furthermore, being conscious that cybersecurity is at the heart of digital confidence and cybercrime is on the rise, the CNIL will strengthen its role in the public authorities' response to cyber risk.

Lastly, the CNIL will prioritize targeted regulatory actions on subjects with high stakes for privacy. The CNIL selected three priority themes: augmented cameras and their uses, the cloud, and smartphone applications. With the accelerated development of AI, the CNIL aims to extend its work in generative AI to large language models and derived applications, notably chatbots. Its AI action plan will focus on understanding how AI systems work and their impact on people, enabling and overseeing the development of AI that respects privacy, federating and supporting innovative players in the AI ecosystem in France and Europe, and audit and control of AI systems and protecting individuals.

Germany 🇩🇪

Contributors: Ulrich Baumgartner

The biggest changes to the German data protection landscape in 2024 shall primarily come at the European level, with passage of the Data Act and its framework for sharing personal and nonpersonal data. Additionally, obligations on the first wave of designated "gatekeepers" under the Digital Markets Act will begin to take effect from the first quarter of 2024, six months after the date of designation by the European Commission.

On a national level, Germany will likely adopt its new regulation on consent management services, as foreseen by Section 26 of the Telecommunications and Telemedia Data Protection Act, which is Germany's still rather fresh ePrivacy law. Section 26 of the TTDSG foresees the introduction of consent management services, which can collect consent preferences for the purposes of the act's Section 25 TTDSG, transposing Article 5(3) of the ePrivacy Directive into German law. The legislature aims to reduce or eliminate the need for cookie banners by allowing users to provide their consent preferences to consent management services in advance, which would then submit them to websites as the user browses the internet. The draft regulation was published in June 2023 and will likely be adopted in 2024, which could lead to a significant reduction in cookie banners if widely adopted in practice.

From mid-December 2023 the provisions of the new Whistleblower Protection Act will also apply to small and medium-size enterprises with 50 to 250 employees, which were initially given an implementation period. The act has several data protection implications in practice, particularly regarding record of processing activities, privacy by default and design and data protection impact assessments.

The German Federal Data Protection Act is due for an overhaul in 2024. An important change foreseen in 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 that the right of access under the GDPR's Article 15 may be limited where trade secrets of the controller or a third party would be exposed in complying with the request. Finally, it regulates the competences of the German data protection supervisory authorities in case of joint control.

Lastly, the EDPB's 2024 coordinated enforcement action regarding Article 15 of the GDPR will be of particular importance in Germany, especially given the wealth of claims for damages currently before courts due to non-compliance with the article's provisions.

Greece

Contributors: Antonios Broumas

This year, Greece is expected to amend its national data protection Law 4624/2019, which enacts supplemental measures for the GDPR. Currently in force, the act has previously been amended once following a formal infringement notification by the European Commission against Greece for failure to adequately transpose the Law Enforcement Directive. The new law is expected to radically reform the current regulation and upgrade the benefits of national data protection legislation for public bodies, businesses and data subjects.

Other legislative developments related to data protection will mainly concern the incorporation of the NIS2 Directive into Greek law and the enactment of supplementary national legislation for major EU Acts, such as the Digital Services Act and the Digital Markets Act. Furthermore, the government will begin deploying its national AI policy under the supervision of the newly established national committee for the development of AI.

In terms of supervision, the head of Greece's Hellenic Data Protection Authority is bound to be replaced by the newly elected Parliament due to the expiration of his tenure. For this reason, the DPA has not presented its strategy or action plan for the year and is, therefore, not likely to take major horizontal or sectoral initiatives for the regulation or supervision of the market.

On the other hand, the Greek government plans to introduce a new law for the transformation of the national cybersecurity authority into an independent administrative authority with enhanced enforcement powers on par with the transposition of the NIS2 Directive into Greek law.

Overall, significant developments are expected to take place in the year ahead, revolving around both national legislation and the supervisory level, reiterating the need for public and private entities in the country to keep data protection compliance frameworks constantly up to date.

Hong Kong

Contributors: Timothy Ma, Kieran Donovan

In 2024, Hong Kong's Personal Data (Privacy) Ordinance is set to undergo a comprehensive review and amendment process. Enacted in 1996, the PDPO has remained largely unchanged over the past two decades. However, due to the increasing prevalence of cross-border data transfers and the need to align its data protection laws with international standards, Hong Kong is likely to introduce new provisions to the PDPO. There is also an indirect impact on processing of personal data in Hong Kong as a result of guidance and recommendations issued in respect of cross-border data transfers, particularly mainland China.

Amendments to the PDPO may include mandatory data breach notifications, which would require organizations to promptly inform the Privacy Commissioner for Personal Data and affected individuals in the event of a data breach. This would enable both the regulator and the public to take appropriate measures to mitigate potential harm arising from such breaches.

Another amendment could be the introduction of a requirement for organizations to formulate data retention policies. This places more accountability on organizations regarding the responsible use of data.

Furthermore, the PCPD may be granted stronger enforcement powers, allowing for more effective action against noncompliant organizations. This could include increased fines and sanctions to deter organizations from violating data privacy regulations.

As Hong Kong continues to embrace digital transformation, the role of technology in data privacy is another key area to watch. To address the privacy implications of new technologies, such as AI, big data analytics and facial recognition, the PCPD may issue new guidance on privacy impact assessments and best practices for implementing privacy-by-design principles in technology development.

Hungary 🇭🇺

Contributors: Ádám Liber, Tamás Bereczki

2023 was a somewhat hectic year for Hungarian data protection professionals, as Hungary transposed the EU's NIS2 Directive and Whistleblowing Directive into its national law.

We expect 2024 to be less hectic, with most of the work going into preparing for the NIS2 requirements, although the detailed requirements will be set out in a ministerial decree and the decree of the president of the cybersecurity supervisory authority.

We also expect Hungarian Parliament to adopt an amendment to the Criminal Records Act allowing employers to directly request data from criminal records where the law allows for verification of employees' criminal records.

In addition, Parliament amended the Civil Code and the Civil Procedure Code and introduced new legislation on the definition of "written form" and the use of digital signatures by natural persons provided by the Hungarian administration's online Identification Based Document Authentication service, which entered into force on 1 Jan. 2024.

The Hungarian government submitted the draft Law on the Digital State and Certain Rules for the Provision of Digital Services, which intends to establish the foundational principles of the Digital Citizenship Program. In 2026, Hungarian citizens can expect the practical realization of a digital mobile application, which will include identity verification, secure electronic signatures and the ability to carry out administrative tasks, including life-event-based matters such as birth registration.

The Hungarian Parliament adopted Act XXV of 2023 on complaints, disclosures in public interest and rules for reporting abuse. Known as the Whistleblower Protection Act, the act transposes the EU Directive 2019/1937 on the protection of persons who report breaches of union law. The initial compliance deadline for organizations employing more than 249 employees was 24 July 2023. We expect many organizations will only have adopted the relevant compliance measures by 17 Dec. 2023, which was the implementation deadline for employers with at least 50 but no more than 249 employees.

Act XXIII of 2023 on Cybersecurity Certification and Supervision implements the provisions of the NIS2 Directive. The act defined a very broad range of sectors in which companies will be subject to the new legislation and set several deadlines for organizations to prepare for compliance, with a final deadline of 18 Oct. 2024 for implementing relevant measures.

The government also submitted the Legislative Proposal on the System of Utilization of National Data Assets and on Certain Services in November 2023, to ensure a coherent regulatory framework and fulfil the legal obligations imposed by EU Regulation 2022/868 on European data governance. The proposal aims to establish a state service system supporting the utilizations of national data assets.

India 🇮🇳

Contributors: Pranav Rai

2024 is set to be a landmark year for India's privacy legislation. The Digital Personal Data Protection Act, 2023, passed in Parliament in August, is anticipated to be fully operational in 2024. Six years in the making, the DPDPA supersedes the outdated and confusing data protection rules of 2011, effectively shedding the "Confusion Raj" label, a term borrowed from a chapter title in Graham Greenleaf's "Asian Data Privacy Laws: Trade & Human Rights Perspectives," that was previously associated with India's legislative privacy landscape.

The DPDPA, India's first comprehensive data protection law, imposes penalties of up to approximately USD30 million for noncompliance. It was crucial for India to protect the constitutionally guaranteed fundamental right to life and personal liberty of its residents, and also for trade reasons. The law is designed to minimize disruption, enhance ease of living and doing business, and bolster India's digital economy and innovation ecosystem.

The Ministry of Electronics and IT has noted the act is "concise," "simple, accessible, rational and actionable." However, despite its merits, the DPDPA has faced criticism for its broad delegation of power to the Union government, its potential to weaken the Right to Information Act, and its perceived lack of clarity and specificity.

Critics contend these issues could result in arbitrary and unaccountable decision-making, impede transparency and accountability, and create uncertainty for businesses and individuals. Regrettably, one might observe the DPDPA may have fallen short of carving out a unique "fourth way to privacy, autonomy and empowerment" — a path distinct from China, the EU and the U.S. — an ambitious goal proposed by the Justice B.N. Srikrishna committee. Notably, the Srikrishna Committee's 2018 report was instrumental in recognizing data protection as a fundamental right and proposing a comprehensive data protection law, thereby influencing India's data protection landscape.

On another front, the upcoming companion legislation, the Digital India Act, currently in draft form, is poised to replace the 22-year-old IT Act. The DIA aims to encompass the entire ecosystem of technology, providing a more comprehensive and future-ready legal framework for India's digital economy. It also includes provisions for regulating social media companies, online intermediaries, and e-commerce platforms. An intriguing interplay may emerge between the DPDPA and the forthcoming DIA, as both laws will significantly shape the future of data protection and digital rights in India.

While the DPDPA may not be flawless, it represents a substantial advancement over previous data protection rules. It is anticipated that any existing issues will be resolved over time. Despite the challenges, the government's dedication to establishing a comprehensive data protection framework is evident. As the implementation processes progress, including the establishment of the Data Protection Board and the development of rulemaking, we can look forward to the emergence of a more robust data protection framework in India.

Indonesia

Contributors: Glenn Wijaya

On 17 Oct. 2024, Indonesia's Personal Data Protection Law is set to come into full force. The PDPL stipulates the necessity of implementing regulations, which are outlined as follows:

- Presidential Regulation: It is anticipated this regulation will be enacted to establish the Personal Data Protection Authority.
- Government Regulation: Public input was sought through a dedicated website until 25 Sept. 2023. This regulation was expected to be put into effect by the end of 2023, providing further details on provisions of the law.

Regardless of the expected months of enactment, it is likely that both regulations will be enacted before 17 Oct. 2024.

Once established, the Personal Data Protection Authority will issue regulations addressing these key issues: verification of personal data; automatic data processing; suspension and limitation of personal data processing; operational technical measures and determination of data security levels; competence and appointment of personal data protection officers; international data transfers; compliance monitoring and legal actions; and mediation.

Additionally, Indonesia is in the process of developing regulations pertaining to AI. As an initial step, Deputy Minister of Communication and Informatics Nezar Patria stated the ministry is drafting a circular letter offering guidance on AI ethics. Currently, Indonesia has only formulated a national strategy for AI spanning the years 2020 to 2045.

It is also essential to note that this year's election may exert influence on the drafting and enactment of all these regulations.

Ireland

Contributors: Kate Colleary, Demilade Adeniran

In September 2023, Ireland's Data Protection Commission completed its inquiry into TikTok, finding the platform failed in its obligations as a controller of children's data under the GDPR. TikTok was issued a reprimand, an order to bring processing into compliance within three months, and a 345 million euro fine, the largest TikTok has received from regulators.

TikTok has commenced an appeal and a judicial review challenge. We await further developments on this in 2024 and on other statutory appeals against decisions of the DPC following DPC/EDPB decisions.

The Courts and Civil Law (Miscellaneous Provisions) Act 2023 was recently enacted, allowing the DPC to bar publication of information relating to its proceedings.

Specifically, the DPC can issue notice to a person requiring they not disclose information it provided to them. These confidentiality obligations are limited under Section 26A(1) which states the DPC may issue a written notice to a "relevant person" where it is or will be providing them with confidential information, directing the person not to disclose the information unless required by law or authorized by the commission. We are likely to see notices issued in 2024, particularly where there are large scale inquiries being carried out. These notices may be subject to legal challenge by those impacted.

Also in 2023, the DPC successfully prosecuted several organizations for breaching e-Privacy Regulations related to electronic marketing. The violations included sending unsolicited marketing communications, including phone calls, emails and messages, without consent or valid opt-out options.

The DPC has warned organizations should remain cognizant of these regulations as it will continue to prosecute those that fail to comply, so this is likely to be an area of further enforcement in 2024.

Israel

Contributors: Dan Or-Hof

On 15. Jan. 2024, following a long review process, the European Commission determined Israel continues to maintain an adequate level of protection of personal data transferred from the European Union. As a result, data transfers from the EU to Israel can continue to take place without additional requirements. The

Commission's adequacy first review report follows recognition of Israel's privacy laws in 2011 and extensive discussions between the EU and Israel over the past three years. During that time, Israel has made considerable efforts to maintain the recognition by, among other things, strengthening the independent position of the Privacy Protection Authority and enacting the Privacy Protection Regulations, granting enhanced rights to personal data transferred from the EU to Israel. The EU Commission report includes a recommendation on enshrining in legislation the protections that have been developed at sub-legislative level and by case law. This is particularly important given the ongoing legislative reforms in Israel's Protection of Privacy Law.

As a result of frequent elections in Israel, substantial amendments to Israel's Protection of Privacy Law are still pending. It is yet to be seen if the current government will move forward with enacting the amendments, which include, providing the PPA with substantial enforcement powers, updating terms and definitions, forming a privacy compliance function in national security agencies and considerably reducing the mandatory database registration obligation. Deliberations on the amendment known as Bill No. 14 by the Constitutional Committee in Israel's Parliament, the Knesset, continue. Concurrently, the justice department is anticipated to introduce Bill No. 15 to the Protection of Privacy Law, which will likely add substantial EU General Data Protection Regulation-like provisions, including the need for data protection impact assessments, appointment a data protection officer, and enhanced data subjects rights and lawful grounds of processing.

The PPA continued to be active during 2023 with guidelines, policies and supervision activities, including in relation to the use of biometric and location data in a workplace environment, the privacy protection status in pension funds, limitations on the use and copying of government issued IDs, a prohibition on the use of leaked medical data for artificial intelligence modeling and guidance on privacy aspects of smart homes. The PPA will likely continue to be active during 2024 in filling-in gaps made by the outdated law with guidelines addressing modern challenges and privacy practices.

The war waged by Israel against the Hamas has sparked a wave of cyberattacks on Israeli companies and public authorities. The Israeli government enacted regulations on handling severe cyberattacks, applying obligations on suppliers of digital, IT, cloud and other data-related services, to cooperate with the National Cyber Directorate and other cyber-related government agencies. The regulations will sunset when the Israeli government publishes a decision that ends the emergency situation in Israel as a result of the war.

The PPA followed with a supervision campaign, demanding data hosting and data management services to produce evidence of their privacy law compliance, particularly with data security regulations enacted under the Protection of Privacy Law.

Class-action lawsuits associated with privacy violations involving claims related to unlawful data sharing, processing without consent, insufficient privacy notices and insufficient information security controls, continue to be on the rise and are a dominant privacy-related risk.

Italy

Contributors: Rocco Panetta

As expected, 2023 proved to be a busy year for Italy's data protection authority, the Garante, a year that heralds an equally exciting 2024.

It is undeniable 2023 was a year in which the Garante made itself known far beyond national borders. The open proceedings against two global AI players Replika and OpenAI (which I had the pleasure of assisting) were enlightening to remind everyone — companies, data protection officers and regulators, alike — that data protection rules have not been retired and, on the contrary, are a fundamental guide for those who want to develop AI systems.

Since then, other authorities, European and otherwise, have also started their own investigations, including the U.S.'s Biden administration, which convened an urgent meeting on generative AI in the spring. It seems the role of data protection officers and data protection authorities, whatever form the EU AI Act will take, will not be sidelined — far from it. On the other hand, the way in which proceedings against the two companies were closed showed how dialogue and confrontation between companies and authorities, especially in such uncertain terrain as AI, can only be fruitful for both sides.

For 2024, I therefore foresee more activity by the Garante on AI-related issues, but also the analysis of an old but still topical issue, that of data valorization and monetization. The recent choice of several social media platforms to switch to an (optional) business model based on paid subscriptions so as not to see advertising, could reopen a chapter that seemed to have been closed with the latest court rulings. It remains certain that, with the new European regulations in force — the DSA, DMA and DGA — as well as those on the way — the AI Act — there will be no lack of opportunities for confrontation.

Japan

Contributors: Hiroyuki Tanaka

According to supplementary provisions of the Act on the Protection of Personal Information, the review of whether to amend the APPI is conducted approximately every three years. According to the Personal Information Protection Commission's 15 Nov. 2023 document titled "APPI: Review Based on the So-called Triennial Review Provision," the PPC plans to issue an interim draft on the direction of APPI revision in the spring of 2024.

- Although the official timeframe has not yet been published, based on past experience, it can be estimated that a general outline of the proposed APPI revision will be published in the second half of 2024. It can also be estimated that the draft law of the amended APPI would be published in 2025 and could be expected to take effect in 2027. Each will be subject to public comment. At this stage, it is not easy to estimate what will be included in the possible amendments, however, according to the PPC's 2023 document, the following issues may be on the table:
- More substantive protection of the rights and interests of data subjects. This could include, for example, clarification of the principle of data minimization, expanded enforcement of innovative technologies using the inappropriate use clause, stricter requirements for data subjects' consents, protection of children, and expanded remedies for individuals, such as the introduction of class actions.
- Effective monitoring and supervision by the PPC, including the introduction of GDPR-like fines.
- Promoting the use of personal information, including establishing a system for the use of personal information in areas of high public interest, such as health and medical care, education, disaster prevention, and children, as well as designing a system to promote international data transfers and voluntary efforts by companies to protect personal information.

Kenya

Contributors: Mugambi Laibuta

2024 will set in motion a series of interesting and critical legislative changes that will impact Kenya's data privacy landscape, including the enactment of regulations under the Computer Misuse and Cybercrimes Act. The current draft regulations provide for cybersecurity operations centers, define critical information infrastructure and establish cyber threats reporting mechanisms.

In September 2023, the cabinet secretary in charge of information, communications and digital economy appointed a working group on policy and legislative reforms for the sector. The working group's term of reference includes reviewing existing policy, legislative frameworks, institutional structures, and administrative protocols regulating or underpinning Kenya's information, communications, technology, and digital economy sector and making recommendations for reform, which will be published in 2024.

A Parliamentary Ad Hoc Committee Report on Worldcoin's activities in Kenya, published in September 2023, is bound to have far-reaching data privacy effects. The committee's recommendations include the need to develop a legal framework on virtual assets in Kenya and to harmonize the Data Protection Act with the Companies Act. It called for amendments to the DPA to scale administrative fines and create a board to oversee Kenya's Office of the Data Protection Commissioner. The committee also called for co-option of the ODPC into the National Computer and Cybercrimes Coordination Committee. These legislative proposals are bound to be tabled and debated in 2024.

ODPC guidelines in the telecommunications, education and digital credit sectors are also expected to be in place within 2024 and with more litigation on privacy and data protection reaching the courts, formal legal announcements regarding the efficacy and constitutionality of current privacy and data protection legislation are anticipated.

On AI, the Media Council of Kenya appointed a task force to formulate data and AI guidelines for media, while President William Ruto announced the country will enact legislation to regulate AI. It is not yet clear what the proposed legislation will contain, but it will potentially provide an interesting regulatory shift in Kenya.

The above initiatives, where carried out to conclusion, will redefine data privacy regulation in Kenya.

Luxembourg 🇱🇺

Contributors: Vincent Wellens, Yoann Le Bihan

In its strategic plan for 2023-25, published in March 2023, Luxembourg's data protection authority, the National Commission for Data Protection, highlights the disruptive effects of innovative technologies — AI, blockchain, virtual reality, etc. — and the personal data protection questions they raise. It goes without saying this will be a focus of the CNPD and, hence, data protection in Luxembourg.

This challenge is further exacerbated by the constant evolution of EU legislations in the data and digital sector — Data Governance Act, Digital Markets Act and Digital Services Act — and the different attempts to regulate new technologies, such as those within the Data Act and AI Act. These new legislations will redefine rules governing the processing of personal data in several respects and may lead to a new set of competencies for the CNPD. More generally, the CNPD will need to find ways to ensure data protection while allowing innovative technologies to unlock potential benefits for society.

Some of the new EU legislations require national implementation on several points and we would not be surprised if the Data Governance Act triggers an amendment of the Luxembourg 2018 Personal Data Protection Act, which could be an occasion to revise other provisions of the act as well.

Finally, the call for efficient enforcement remains at the heart of the CNPD's preoccupations and it is not impossible that the commission will further streamline its complaint and enforcement procedures.

Mexico 🇲🇽

Contributors: Gabriela Espinosa

The privacy landscape will most likely resemble an arid desert during 2024 in Mexico. The lack of impulse and interest from the federal government for privacy and personal data protection has resulted in a barren environment for legislative developments and for Mexico's data protection authority, the National Institute of Transparency, Access to Information and Personal Data Protection, to fully operate.

As of the time of writing this, the Mexican Senate has neglected to appoint three INAI commissioners, leaving it lacking the necessary quorum to legally hold plenary sessions according to the Mexican Constitution and law. Since the end of August, a ruling from the Supreme Court of Justice in Mexico has served as a temporary suspension of the quorum requirement until the Senate completes the pending appointments and allows the INAI to function with its four seated commissioners.

While several initiatives were presented in Congress in 2023 to amend the Mexican Federal Data Protection Law Held by Private Parties, INAI's struggles have taken up most of the public agenda with activists, journalists and privacy professionals publicly stating support for the INAI and relentlessly challenging the Senate to fill its empty seats.

Amendment bills presented this year have separately intended to protect biometrics, children's privacy, increase penalties for crimes related to improper use of personal information, and include credit information bureaus within the law's scope. Nevertheless, none has had any significant legislative response. A cybersecurity law and several bills aiming to regulate AI have also been introduced in Congress but have not advanced.

With a big election — presidential and legislative — coming up in June 2024, it is safe to assume public focus will be on campaigns, and we will continue to see tumbleweeds in the privacy landscape.

New Zealand 🇳🇿

Contributors: Daimhin Warner

As with the rest of the world, AI and biometrics dominated New Zealand's regulatory landscape in 2023. The Office of the Privacy Commissioner consulted on the development of a biometrics code of practice, published a position statement on generative AI and issued guidance on applying the New Zealand Privacy Act to AI use.

In addition, several legislative developments progressed, including passage of the Digital Identity Services Trust Framework Act 2023, a draft Customer and Product Data Bill which will deliver a version of the data portability right, and release of a Privacy Amendment Bill that will apply the Privacy Act's transparency obligation to the indirect collection of personal information.

Many of these changes will really take effect in 2024, meaning it will be a year of significant legislative and regulatory upheaval for many organizations and privacy professionals. A new biometrics code of practice will create additional obligations for organizations looking to implement biometric solutions, such as facial recognition technologies. All organizations will need to consider how they will comply with expanded privacy transparency obligations, and will likely look to overseas practice. The banking sector will need to ensure it is ready to meet the requirements of the new consumer data right, which should come into force before the end of the year.

Finally, in addition to the above, the OPC will continue its broad review of children and young peoples' privacy, including how fit for purpose current laws and regulations are to protect this vulnerable group.

Nigeria 🇳🇬

Contributors: Dorcas Tsebee, Temitayo Ogunmokun, Ridwan Oloyede

2023 marked a significant milestone in Nigeria's data protection landscape as the long-anticipated Nigerian Data Protection Act was finally enacted in June 2023, putting Nigeria on the global list of countries with a comprehensive data protection law.

The law establishes the Nigeria Data Protection Commission to oversee its implementation. The NDPC inaugurated the Nigeria Data Protection Act General Application and Implementation Directive Drafting Committee with a mandate to develop an implementation framework. The commission is also expected to publish additional guidelines and regulations and launch its registration portal.

We anticipate a more sector-driven approach in the coming year. In 2023, the Nigerian Communications Commission published draft data protection regulations and held a public consultation that is anticipated to be finalized in 2024. Other regulators — like the Central Bank of Nigeria, Securities and Exchange Commission, and Federal Competition and Consumer Protection Commission — may also publish related regulations or guidelines. The CBN attempted to introduce a sectoral data protection regulation for the banking industry in 2018. Conclusion of the amendment to the NCC Registration of Telecommunications Subscribers Regulation, which opened for public comment in 2022, is also anticipated in 2024.

Some past failed legislative proposals may also make a comeback. Notably, we anticipate the return of the National Electronic Health Record Bill, the Electronic Transactions Bill, the Cybercrimes Act, and the Digital Rights and Freedom Bill. In addition, an analogous legislative proposal with data protection implications, like the Lawful Interception of Communications Bill, may make a return.

Mirroring global trends, Nigeria is increasingly focusing on AI governance. In 2022, the National Information Technology Development Agency began drafting a national AI policy, anticipated to be published by 2024. The government underscored its commitment to this focus by recently publishing a National Strategic Blueprint, which includes the development of a National AI Strategy as an objective. The objective of developing a national AI strategy has been further emphasized by the minister of Communications, Innovation and Digital Economy in recent public comments. An AI and robotics bill is currently under review in the National Assembly, promising significant developments in the near future. Regional efforts, as highlighted by data protection legislative bills in Lagos and Ogun State, may make a return in 2024 with other states expected to join the trend.

Norway 🇳🇴

Contributors: Martha Ingves

Norway's data protection authority, the Datatilsynet, was involved in several high-profile cases in 2023 and we can expect some of these to spill over into 2024.

Most notably, in July 2023, the Datatilsynet issued an order against Meta banning its processing of personal data for behavioral advertising purposes in Norway. This led to litigation, which might continue in 2024. This case may also have important implications outside Norway — as the EDPB was called upon to order similar measures for the rest of Europe — and will be one to follow in 2024. It will be especially interesting to see whether Meta's pledge to switch to consent as a legal basis for behavioral advertising will be enough to settle the case.

On the topic of consent, Norway's Electronic Communications Act has been in the pipeline for several years and is expected to finally be adopted in 2024. With its adoption, Norway is likely to move beyond consent to cookies through browser settings, which has been considered acceptable in Norway, contrary to many other European countries.

Finally, AI has been on top of the legislative agenda across the world in recent years and Norway is no exception. The Norwegian government has been very active in this area with recent initiatives including earmarking NOK1 billion for AI research and creating a specific ministerial post for digitization and AI. The government is also in the process of assessing whether Norway should come up with its own AI regulation, which would complement the EU AI Act. We will likely start seeing the first results of these initiatives in 2024.

Paraguay 🇵🇾

Contributors: Cecilia Abente Stewart

In 2024 we can expect discussion of Paraguay's proposed comprehensive data protection bill. The bill takes the GDPR and Standards for Personal Data Protection for Iber-American States as reference, as well as other modern legislations. Data protection principles, data subject rights, controller obligations, and international transfers are included within the proposal, as well as the appointment of a new supervisory authority.

Amendments to the original bill are likely to be proposed by the Chamber of Deputies, for example, utilizing a functioning entity linked to information technologies or commerce as supervisory authority, instead of creating a new public entity.

Additional bills involving personal data are expected to be discussed in Parliament, such as the amendment and extension of Article 260 of Paraguay's Penal Code regarding identity theft, including virtual identity and mandatory storage of traffic data to combat child pornography and related punishable acts.

Toward the end of 2023, a public hearing was held on AI during which it was agreed that a solid privacy regulation is a necessary first step. Meanwhile, the evolution of this technology and possible regulation courses will be studied.

Hopefully 2024 will bring a breakthrough with the enactment of a comprehensive data protection law that will enable more legal certainty for future technological developments.

Peru 🇵🇪

Contributors: Catherine Escobedo

During 2023, the Peruvian government issued bills and legislation to improve current legislation and policies on data protection, digital government and digital transformation. However, a number of these bills are still awaiting discussion on the floor of Congress and will probably see the light in 2024.

For instance, the modification of the Data Protection Law, a bill proposed by the legislative branch earlier in 2023, is still in the works after receiving mixed advisory opinions from different sectors. Unfortunately, the first draft focused on an imprecise, and unnecessary, definition of the "right to be forgotten," which should be either deleted or improved. The long-awaited modification of the Regulations of the Data Protection Law, a bill proposed by the Executive Branch through the Ministry of Justice and Human Rights, is also a work in progress and has received comments, suggestions and recommendations from different private and public institutions. As expected, the bill includes stronger regulations on the treatment of personal data with emphasis on security and response to data breaches.

Also, a proposal for regulations of the Digital Trust Framework, issued by the Executive Branch, was published for comments. The proposed regulations cover digital security incidents, defining response protocols, communication channels, and deadlines for reporting such incidents.

A law promoting the use of AI in favor of the economic and social development of the country has been drafted. It emphasizes that AI should not transgress people's privacy and that AI use is expected to help the improvement of, among other things, digital security.

It is clear Peru is working toward strengthening regulations on cybersecurity and in 2024, and the years to follow, we will continue to see more proposals on this matter. The recently published "Peruvian National Digital Transformation Policy for 2030" has as one of its priority objectives "consolidating digital security and trust in society" and commits to ensuring proper functioning of the National Digital Transformation System, developing and articulating national strategies with emphasis on security and digital trust.

Finally, in 2024 we expect the publication of the National Cybersecurity Policy — which has been in the works for over a year — and advances in drafting the Cybersecurity Law and regulations of the Cyberdefense Law, both pending since 2019.

Philippines 🇵🇭

Contributors: Irish Salandanan-Almeida

With technological advancements and the rapidly evolving business landscape, the Philippines' DPA, the National Privacy Commission, released guidelines on consent, legitimate interest and deceptive design practices or "dark patterns." These are expected to aid personal information controllers and processors in complying with the Philippines' privacy law, the Data Privacy Act, especially as they navigate a complex business environment while accounting for the many novel uses of data in AI and the metaverse or virtual environments.

There continues to be increased government and private sector collaboration as the NPC signed a memorandum of understanding with the country's three largest telecommunications companies to raise awareness against spam, scams and other fraudulent schemes that capitalize on Filipinos' personal data, especially of those left jobless during the COVID-19 pandemic. This follows the full implementation of the Subscriber Identity Module Card Registration Act with the NPC providing guidance to telecommunications companies on how to secure subscribers' personal data while achieving the objectives of identification and prosecution of fraudulent actors and cybercriminals.

The NPC is also working closely with members of its Data Privacy Council — made up of data protection officers from various industries including health, education, banking, insurance, retail and outsourcing — in drafting sectoral codes to govern data use in their respective industries.

Digitalization and modernization are also top priorities as the NPC implemented its Data Breach Notification Management System and NPC Registration System, automated platforms intended to facilitate compliance by personal information controllers and processors.

Finally, the NPC reiterated its commitment to increasing knowledge and awareness through comprehensive advocacy programs to help individuals navigate the digital world. In connection, the NPC announced the release of circulars on a Data Privacy Competency Program as well as a Philippine Privacy Mark Certification Program.

Portugal 🇵🇹

Contributors: Sofia Calado

Portugal's National Data Protection Commission released its 2024-26 Strategic Plan. The CNPD will celebrate its 30th anniversary in 2024 and aims to launch a training national plan, as well as a Data

Protection Portal to foster communication with data subjects, controllers and processors.

The program InCoDe.2030, under the secretary of state for Digitalisation and Administrative Modernisation, was planning to disclose the Data National Strategy in 2024. However, the release of the strategy will likely be postponed as a new parliamentary election was called in the meantime.

In terms of legislative proposals, Law no. 58/2019, the implementing law of the GDPR, will likely be amended to allow medical students that provide treatments or diagnosis access to health data platforms and information systems. This follows the CNPD decision no. 262/2020, determining the lack of legal basis for such access under current Article 29 of Law no. 58/2019.

The Portuguese Parliament may try to approve new provisions applicable to metadata retention scope and periods by telecom operators and their transfer to criminal investigative authorities, amending Law no. 32/2008. In a ruling, the Constitutional Court considered the latest suggested retention period of three to six months, applicable to all traffic and location data stored under the law, to be unconstitutional.

New rules governing competent authorities on addressing the dissemination of terrorist content online, under Regulation (EU) 2021/784, will be ratified. The CNPD issued its opinion no. 2023/57 concerning this topic.

TEIn 2024, the CNPD will hopefully publish new guidelines on the interplay between data protection and disruptive technologies, with a special focus on AI.XT

Romania

Contributors: Adriana Neagu

As in previous years, there is no expectation 2024 will bring a new law focused on privacy and data protection, with Romania tending to rely on EU-wide applicable rules.

However, not surprisingly, AI made its way into the public agenda. In 2023, Romanian authorities established a consultative body of the Romanian government to create a uniform strategy toward AI governance. What this means is not entirely clear, as this body is not currently fully operational. There is an open invitation for experts in the area to participate.

Another interesting proposal is a draft law that would ban deepfake content. Progressing through the legislative process, the draft legislation targets the creation, dissemination and storage of content online or in mass media, such as images or audio-video recordings, that is designed using AI or virtual reality technology to create the appearance that an individual said or did things they did not. The draft law would require such content to include notice visible on at least 10% of the exhibition surface for the duration of its publicizing. It proposes fines and criminal penalties for those using deep fakes for defamation purposes.

Saudi Arabia

Contributors: Dale Waterman, Benjamin Crew

The amended Personal Data Protection Law was implemented by Royal Decree on 27 March 2023 and came into force on 14 Sept. 2023. Controlling entities have until 13 Sept. 2024 to become compliant.

The PDPL is the Kingdom of Saudi Arabia's first comprehensive data protection law. It has extraterritorial scope and applies to any processing of personal data that takes place in the Kingdom as well as any processing by an outside entity of personal data of individuals living in the Kingdom.

One of the most significant amendments is the removal of the strict data localization requirement governing cross-border transfers of personal data. The PDPL sets out circumstances under which personal data may be transferred lawfully outside national borders, provided the transfer or disclosure does not prejudice national security or the vital interests of the Kingdom and there is an adequate level of protection for personal data outside the Kingdom.

Organizations should, however, assess this development with reference to applicable data localization requirements under other national or industry-specific requirements, such as the National Cybersecurity Authority's Essential Cybersecurity Controls, the Communications, Space and Technology Commission's Cloud Computing Regulatory Framework and the Central Bank's Rules on Outsourcing.

The PDPL also introduced another recognizable legal basis in legitimate interest by permitting the processing of personal data without consent if it is necessary to achieve a lawful interest of the controller or any other party without prejudice to the rights and interests of the data owner, and provided the personal data is not sensitive in nature.

The Saudi Authority for Data and AI published the Implementing Regulation of the PDPL and the Regulation on Personal Data Transfer outside the Kingdom a week before the PDPL came into force. These new regulations offer additional details setting out how organizations should comply with the PDPL, including requirements for the adequacy regime for data transfers, new requirements for data subject rights, notification requirements for personal data breaches and when controllers must appoint a data protection officer.

Organizations should also consider the Data Management and Personal Data Protection Standards released by the National Data Management Office in January 2021, which incorporate 15 domains, including data protection. An updated version of these standards is expected to be published in early 2024.

Finally, in September 2023, SDAIA released a Version 2.0 of the AI Ethics Framework. This framework applies to all AI stakeholders designing, developing, deploying, implementing, using or affected by AI systems. It creates four risk classification levels, an AI system life cycle, seven AI ethics principles and dedicated roles and responsibilities.

Serbia 🇷🇸

Contributors: Petar Mijatović

In March 2023, Serbia's DPA, the Commissioner for Information of Public Importance and Personal Data Protection, adopted its official yearly report. As it did in 2022, the report reaffirmed the commissioner's view that main impediments in exercising data subject rights under the Law on Personal Data Protection are the normative flaws of the LPDP. Among other things, the LPDP lacks recitals that would establish criteria for further interpretation of the law. Additionally, provisions that echo the EU's Law Enforcement Directive are scattered throughout the LPDP. The noncompliance of other laws with the LPDP are also an impediment.

In August 2023, the Government of the Republic of Serbia adopted a new Data Protection Strategy for 2023-30.

According to the new strategy, the following steps are expected to be taken in 2024: regulation of automated processing of genetic and biometric personal data, and regulation of personal data processing using audio and video surveillance by adoption — or at least the initiation of procedures for adoption — of the amendments and supplements to the LPDP and adoption of special regulations.

Relatedly, the strategy reinforces the understanding that introduction of new technologies in the processing of personal data, digitization, video surveillance and use of AI must not be at the expense of human rights and equality. The Office for Information Technologies and eGovernment is responsible for regulating this area.

Singapore 🇸🇬

Contributors: Pranav Rai

2024 marks an important year for data privacy in Singapore, as data portability provisions are expected to take center stage. Singapore's Personal Data Protection Act underwent significant changes for enhanced consumer protection and to align with technological and business trends, with data portability provisions anticipated to be implemented in 2024 following the PDPA's comprehensive review in 2020. This right, already a fundamental element of the GDPR, is poised to offer individuals increased control over their personal data.

Singapore's data portability right not only aims to grant individuals more autonomy over their personal data, but also to stimulate innovative, intensive data use by organizations. This could bolster the development services provided by these organizations. Singapore's data portability right is expected to be broad, encompassing a list of exceptions and restrictions to address scenarios where data transmission could compromise national interests.

In a related but distinct development, Singapore's Personal Data Protection Commission is expected to release new advisory guidelines, following public consultations in 2023. These consultations revolved around the use of personal data in AI recommendation and decision systems, and the safeguarding of children's personal data. The forthcoming guidelines will offer clarity on these intricate issues, aiding organizations in ensuring compliance.

The increased penalties for PDPA violations, introduced in 2022, will continue to incentivize organizations to prioritize data protection. With the maximum penalties now at 10% or 5% of an organization's annual turnover in Singapore, depending on whether the turnover exceeds SGD10 million or SGD20 million, respectively, the financial stakes are higher than ever.

Looking forward, 2024 will see Singapore further strengthening its data protection framework, with a particular focus on data portability and the introduction of new advisory guidelines. These developments will enhance consumer protection, stimulate innovation and reinforce Singapore's standing as a significant player in data privacy legislation.

Slovakia 🇸🇰

Contributors: Lucia Semančínová

In 2024, Slovakia expects significant regulatory developments across several key areas.

DPA leadership: Since the departure of its previous chairwoman in April 2020, Slovakia's DPA, the Office for Personal Data protection, has been without a leader, which has led to decreased activity. With the September 2023 elections, a new leader is anticipated to be elected, promising to stabilize the office and enhance its operations.

Consumer interests: In July 2023, Slovakia implemented a law regulating collective consumer interests' protection, aligning with the EU's Representative Actions Directive 2020/1828. Slovakia's law introduces collective consumer actions for both monetary and nonmonetary claims and is expected to significantly empower data subjects seeking compensation under Article 82 of the GDPR.

Digital Markets Act implementation: Slovakia is in the process of implementing the DMA, with the Antimonopoly Office expected to play a pivotal role in enforcement. Legislative changes are currently under review and approval is expected in early 2024.

Cybersecurity legislation revision: 2024 will bring changes to Slovakia's cybersecurity legislation, influenced by the NIS2 directive. The revisions will focus on expanding the scope of entities covered and the National Security Authority is encouraging entities to prepare for these changes.

In summary, Slovakia anticipates a year of significant regulatory changes in 2024. These developments aim to strengthen data protection, consumer rights, digital market oversight, and cybersecurity, promoting enhanced protection, transparency and operational efficiency.

South Africa 🇿🇦

Contributors: Armand Swart

2023 marked the 10-year anniversary of South Africa's Protection of Personal Information Act and approximately two and a half years since it became fully effective. POPIA is enforced by the Information Regulator of South Africa. While 2022 saw the IR "finding its feet" and becoming operational, 2023 has seen it taking large strides in enforcement and protection of data subjects' rights. In April 2023, the IR reported it received 895 POPIA complaints within the previous year, 616 of which were resolved.

In 2023 the IR issued its first ever fine of ZAR5 million, approximately USD260,000, against the Department of Justice for its failure to comply with an enforcement notice related to a data breach. The DOJ indicated it will take the IR's decision on review. Any court decision on this in 2024 will be beneficial as South Africa has very few judgments dealing with the relatively new concepts of POPIA and the IR.

The IR issued several enforcement notices in 2023 and granted some organizations exemptions permitting noncompliance with parts of the POPIA. As the POPIA and the IR continue to gain traction, we are likely to see more enforcement notices, exemptions and industry codes of conduct in 2024.

On the AI front, the IR acknowledged the importance of developing an AI governance framework, without taking any further steps. Data privacy guidance from the IR on AI would indeed be beneficial, although it is unlikely that full-scale AI regulations or laws will be promulgated in 2024.

Unfortunately, 2023 saw no pronouncements on an adequacy decision for South Africa by the EU. We remain hopeful for some advancement toward adequacy in 2024 to provide for the free flow of personal data.

There are various other aspects of POPIA which require additional regulation, like electronic direct marketing, legitimate interests and requirements for personal data transfers outside of South Africa. Guidance from the IR on these topics in 2024 would most certainly be a welcome addition.

South Korea 🇰🇷

Contributors: Kyoungjin Choi

2023 was a meaningful year with important changes in the history of South Korea's Personal Information Protection Act. The PIPA was comprehensively revised and went into effect on 15 Sept. 2023. While most articles are in effect, some involving sensitive or difficult issues, or which require time to prepare for enforcement or compliance, will take effect in 2024.

The biggest change expected in 2024 is the establishment of specific enforcement standards for PIPA surrounding AI. Since the large language model created a huge impact around the world in 2023, many countries have discussed AI regulation and international organizations, including the United Nations, have also begun discussions to establish common AI standards. PIPA's Article 37-2, which states automated decisions can be applied to AI, is effective 15 March 2024. Ahead of implementation, work on preparing a presidential decree and guide is in progress.

Similar to the GDPR, Article 37-2 recognizes the right to object if a fully automated decision made by processing personal data in a fully automated system significantly affects the rights or obligations of the data subject. However, exceptions to the right to object are recognized in case of the data subject's consent, legal provisions or contract. Separately, data subjects are granted the right to request explanations or appeal against fully automated decisions, regardless of the degree of influence exerted by the decision. Requests for reprocessing through human intervention are also possible. In addition, if it is recognized as a necessary measure, the data subject is permitted to exercise the right to take that measure. In order to ensure transparency of fully automated decisions, PIPA imposes an obligation to disclose to data subjects the criteria and procedures for the fully automated decision and how it processes personal data.

The presidential decree, guide and commentary to be released in 2024 will include the meaning and specific scope of fully automated decisions and specific examples and judgment standards in cases that significantly affect the rights or obligations of data subjects. It will also contain methods and procedures for exercising the data subject's rights regarding fully automated decisions, methods and extent of explanation or disclosure, and standards for fully automated decisions requiring disclosure or explanation. These specific laws and guidelines are expected to have a significant impact on the establishment of international norms and the innovation and development of AI in the future.

In addition, Article 35-2, the right to request transmission of personal data, and Article 35-3, the institutions specializing in managing personal information, which will play a key role in the Korean MyData scheme, are expected to have a significant impact on society and the economy when they go into effect in 2024 or 2025. The role and responsibility of the personal data protection officer, Article 31, is expected to be strengthened. Determination of adequacy for major trading partner countries under the newly introduced transborder data flow system and recognition of internationally accepted certifications, in addition to Korea's Information Security Management System, are also of great interest.

2024 will be the first year in which practical enforcement of the comprehensively revised PIPA takes place. As the legal basis for imposing a fine of up to 3% of total sales in case of violation has been established, it is expected various cases will emerge that can gauge the enforcement power of PIPA at home and abroad.

Spain 🇪🇸

Contributors: Joanna Rozanska

Throughout 2024, Spain will reaffirm its strong commitment to new technologies. The Spanish Agency for the Supervision of Artificial Intelligence launched toward the end of 2023, becoming Europe's first AI supervisory authority. In early 2024, the AESIA will take its very first steps advising, raising awareness and offering support to public and private entities for the proper implementation of the AI Act. We also look forward to the development (rather slow so far) of Europe's first AI Regulatory Sandbox launched by the Spanish government together with the European Commission.

Another interesting area in the Spanish digital landscape is initiatives aimed at combating deepfakes. Among others, toward the end of 2023, a law was proposed to regulate deepfakes that would amend several Spanish regulations, including the Spanish Data Protection Act, as well as the Spanish Criminal

Code.

Last but not least, the protection of minors online is currently a hot topic in Spain and is core to the strategy of Spain's data protection authority, the Agencia Española de Protección de Datos. We can anticipate intensified enforcement activity as well as numerous publications and initiatives aimed at raising public awareness on the issue. In addition, the AEPD at the end of December presented, jointly with other authorities, its age-verification mechanism certifying an individual's legal age without linking to their name and surname.

Sri Lanka 🇱🇰

Contributors: Ashwini Natesan

In March 2022, Sri Lanka became the first country in South Asia to pass a comprehensive data protection legislation, the Personal Data Protection Act No. 9 of 2022. The provisions of the PDPA, except Part V, are not yet in operation and the grace period for compliance is ongoing. The deadline for the remaining provisions to take effect is 19 March 2025.

In July 2023, Part V of the PDPA, dealing with the establishment of the Data Protection Authority, was brought into force. The DPA has not yet been formed but the president has appointed the board of directors that will supervise the authority. An acting director-general has also been appointed. It has been reported that the DPA will be fully functional by early 2024, which would mean other appointments, such as advisory committees and staff members, will also be made.

The upcoming year will be crucial not only in terms of the DPA's functioning, but also in framing of applicable rules, regulations and guidelines. Specifically, the PDPA calls for the appointment of a data protection officer at every "ministry, department or government agency," thus, training and awareness programs will be needed for state officials.

Sri Lanka already has in place a Right to Information Act, No. 12 of 2016, under which public authorities, including state entities, are required to disclose information. With the PDPA now in place, it remains to be seen how potential conflicts between disclosure of information and protection of personal information will be resolved.

Cross-border data transfers under the PDPA rely, among other things, on an "adequacy decision particularly for public entities." How this will be dealt with once the DPA is formed is another pertinent development anticipated to come in 2024. There have also been some concerns, especially for small- and medium-sized enterprises as to the cost of compliance. Whether certain provisions will be made for such entities will be known in the coming year.

Sweden 🇸🇪

Contributors: Sofia Edvardsen

A considerable amount has happened this past year. Sweden was accepted as a candidate for NATO and is now to implement its first cybersecurity law and regulatory progress on national security. The current conservative-liberal government's focus on digitalization and security can be seen in an investment in national law enforcement and the Swedish Security Service, which will receive an increase of SEK180 million.

Upcoming legislation for 2024: In March 2023, the Swedish government commenced an investigation on how to best implement the NIS2 Directive and Cyber Resilience Act into Sweden's legislative system. It will be the first cybersecurity legislation in Sweden. The expected outcome is February 2024, with a law due September 2024. There will also be enhanced protection for democracy and judicial independence.

Proposed legislation regarding acquiring electronic information in Sweden for coercive measures in criminal procedures is also anticipated.

Initiatives from the DPA: In 2023, Sweden's data protection authority, the Integritetsskyddsmyndigheten, initiated a Regulatory Sandbox Pilot regarding suppliers of machine learning/AI tools for health care. The pilot was considered successful and has resulted in future sandboxes for development and guidelines on federated machine learning in the health care sector.

Enforcement: IMY had 105 ongoing investigations by mid-October 2023, half of which were initiated in 2020 and 2021 and are still ongoing.

The following notable enforcement decisions have been appealed and are awaiting further judicial review:

An SEK58 million fine issued to Spotify over alleged failure to provide adequate information on data held to the data subject in the local language following a data subject access request.

Bonnier News was fined SEK13 million for alleged failure to ensure a valid legal basis for analytics and profiling.

An SEK12 million fine against Tele2 Sverige for alleged failure to protect data subjects' rights when using Google Analytics, an issue of widening the scope of the definition of personal data.

Switzerland

Contributors: Stéphane Droxler

Switzerland's new Federal Data Protection Act took effect 1 Sept. 2023. There is a noticeable buzz among businesses that, up until now, hadn't deemed it necessary to take steps toward compliance with the requirements of European law. Is it a flash in the pan or a sustainable effort? That's the question.

To attempt to answer this, we can observe that this new law comes into effect in a context marked by a surge in cyberattacks, an increase in security breaches involving all types of data, and the emergence of new cyber risks driven by the rapid growth of AI. All these factors advocate for an awareness among leaders and the adoption of better cyber resilience practices.

Nevertheless, many companies or public entities still struggle to address the issue of data protection comprehensively and see the new act as an additional administrative formality. Others try to initiate actions toward better compliance but either struggle to maintain the necessary momentum for the adoption of a true data protection culture or mainly seek to limit their responsibilities.

On the side of Switzerland's data protection authority, the Federal Data Protection and Information Commissioner, staffing has indeed increased somewhat, but unfortunately, they remain very modest against the magnitude of the challenge.

In conclusion, even though businesses, public entities and authorities all agree that digital responsibility is everyone's concern, the reality tends to show that it is mostly someone else's concern.

Thailand

Contributors: Nop Chitranukroh, Gvavalin Mahakunkitchareon

Thailand's Personal Data Protection Act came into full effect on 1 June 2022 and various subordinate regulations have since been issued by the Personal Data Protection Committee. These include regulations on security measures to be implemented by data controllers, data breach notification requirements, a mandatory obligation to appoint a data protection officer when the processing activity requires regular monitoring of personal data or a system due to the large scale of personal data, administrative measures and data processors' record of processing activities.

As some areas under the PDPA still require further clarifications, a series of public consultations for the remaining draft subordinate regulations is anticipated in 2024. Potential areas include data protection impact assessments and cross-border transfers of personal data, which are crucial for organizations and particularly for entities with establishments in other jurisdictions.

PDPA enforcement by Thai regulators was silent until the last quarter of 2023, when the PDPC published details about complaints that have been lodged to the Expert Committee. The committee is designated by virtue of the PDPA and has the power to make determinations related to imposing administrative fines and other penalties. Enforcement in 2024 is expected to become more active and potentially more serious, which means organizations should pay closer attention to ensure compliance with the PDPA.

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

With respect to sector-specific data protection legislation, in September 2023, Thailand's National Broadcasting and Telecommunications Commission issued the Notification of the NBTC Re: Measures to Protect Telecommunications Service Users' Rights in regard to Personal Data, Privacy Rights, and Freedom of Telecommunications, which replaces the previous notification. The notification aims to enhance the protection of personal data and privacy rights for telecommunication users and to align its data protection requirements with the provisions of the PDPA. The development of specific data protection laws for other sectors is still silent.

Turkey

Contributors: Furkan Güven Taştan

As 2024 unfolds, Turkey is at a pivotal point in its push for comprehensive data protection reform. Despite the ambitious goals set for 2023, the intensity of the general elections pushed data protection improvements down the priority list. However, momentum wasn't completely lost, as two key policy documents were released, providing a roadmap for reform of the Turkish Data Protection Act.

The 12th Development Plan (2024-28) and the Medium Term Programme (2024-26) both emphasize the goal of aligning the TDPA with EU standards, using the GDPR as a key reference. The reform is divided into two main legislative efforts. The first concentrates on improving how personal data is transferred internationally and updating the rules for handling sensitive personal data.

This first package aims to introduce new protective measures, such as binding corporate rules and certifications, to address the current challenges faced by Turkish businesses. The draft, carefully developed by the Ministry of Justice's scientific committee, is still being reviewed. According to policy documents, it is very likely this package will be finalized in the fourth quarter of 2024.

This first package aims to introduce new protective measures, such as binding corporate rules and certifications, to address the current challenges faced by Turkish businesses. The draft, carefully developed by the Ministry of Justice's scientific committee, is still being reviewed. According to policy documents, it is

very likely this package will be finalized in the fourth quarter of 2024.

Will 2024 be the year when Turkey's data protection legislation aligns with European standards? Time will tell, but the groundwork is being established with clear commitment.

Ukraine 🇺🇦

Contributors: Dmytro Korchynskyi

It's been almost two years since Russia's invasion of Ukraine. However, victory in the war is not the only challenge, for the post-war future of Ukraine is being determined both on the battlefield as well as in the Verkhovna Rada's walls.

Currently, the Ukrainian Parliament is working almost overtime to harmonize its legislation with the European Union. But the question of reform implementation lies not only in Parliament's jurisdiction, but also in a synergy between the Parliament and Cabinet of Ministers.

Unfortunately, yet understandably, Parliament did not address the question of the new data protection law this year, as its focus was aimed mainly at the war and anti-corruption issues. On the other hand, the Ministry of Digital Transformation began its work around AI, which heavily relies on personal data issues. Moreover, the Ministry of Justice completed the second phase of the self-screening procedure required by the European Commission. During such self-screening, Ukraine has demonstrated the current situation with data protection highlighted similarities, differences and gaps. Even though there is an ongoing war, Ukraine tries its best to take every reasonable step to join the EU.

That being said, data protection and adjacent regulations will be adopted as it is a requirement to become an EU member state. However, the pace of civilian reforms will be determined on the battlefield. Should Ukraine achieve its military goals in 2024, then reforms such as data protection will be very quick to follow.

United Arab Emirates 🇦🇪

Contributors: Benjamin Crew, Dale Waterman

The United Arab Emirates published the Personal Data Protection Law in 2021, which was scheduled to take effect in 2022. However, the Executive Regulations, a pre-requisite for enforcement, are yet to be issued. With the many regulatory advances across the wider Gulf region throughout 2023 — including implementation of the Kingdom of Saudi Arabia's Personal Data Protection Law — we may expect the release of the Executive Regulations to support the implementation of the PDPL in early 2024, with an enforcement date likely to follow later in the year.

In the UAE there has been increased appetite for legislation in the AI and virtual assets domains, where the UAE is vying to position itself as a global leader. Dubai's Virtual Assets Regulatory Authority established a comprehensive, principles-based framework to govern the virtual asset landscape in the Emirate of Dubai, with the introduction of Virtual Assets and Related Activities Regulations 2023. The regulations include compulsory rulebooks for all virtual assets service providers and incorporate requirements for governance controls and the protection of personal information.

In providing regulatory certainty and promoting protection for investors, the new regime is already drawing companies to the UAE, with interest in the region likely to continue growing into 2024. Inevitable questions are being asked about data privacy and data protection in the context of both AI and virtual assets, and 2024 will likely see a significant focus on addressing these, in conjunction with the UAE PDPL.

In the case of the Dubai International Financial Centre, adequacy with the U.K. is on the horizon, which will ease the impact of compliance obligations on companies operating in the free zone that depend on the free and secure flow of data across borders when conducting business.

The DIFC has not been standing still in other areas, also issuing amendments to its Data Protection Regulations, which incorporate comprehensive requirements around the operation of AI and generative machine learning technologies and add to its list of adequate jurisdictions. The Financial Action Task Force's continued listing of the UAE as a "jurisdiction under increased monitoring" has increased external focus on companies operating in the region as well as the scrutiny of the regulatory regimes in the UAE.

It is important to note that the increased focus on compliance by global regulatory authorities is not just limited to know your customer and anti-money laundering activities. As data protection regimes mature, organizations in the UAE must expect investigations and fines for noncompliance with local, federal and sectoral laws, especially those that govern data privacy.

United Kingdom

Contributors: John Bowman

The government of the United Kingdom has been highly active in data protection and AI governance during 2023 and this level of activity is set to continue into 2024. The Data Protection and Digital Information Bill is now in the report stage in Parliament having passed through the committee stage earlier in 2023. Parliamentary time is needed for the bill to be debated and amended, as required, before it is finalized.

When enacted, the DPDIB is expected to include reforms to the U.K. GDPR that are designed to promote innovation and alleviate burdens on business. These include taking a risk-based approach toward maintaining records of processing, making it easier to reuse data for scientific research; adjusting consent and legitimate interest provisions to facilitate data processing for marketing; and subjecting profiling to the same provisions as automated-decision making.

The government has signified its intention to maintain its EU adequacy status which was agreed in 2021 and will continue to work on its own data decisions for transfers from the U.K. to third countries. The government also recently announced a U.K. extension to the EU-U.S. Privacy Framework, known as the U.K.-U.S. Data Bridge. This enables organizations in the U.K. to export personal data to organizations in the U.S. that are already certified under the EU-U.S. scheme without needing to apply additional data transfer safeguards.

While the bill will be the focus of activity in Parliament, and the road ahead for Royal Assent by March or April is clear, in policy terms the U.K. is also emerging as an international voice in AI governance. The government held a consultation exercise following the publication of its white paper "A pro-innovation approach to AI regulation."

This white paper sets out principles existing regulators will be expected to implement in their respective fields. These regulators are the Competition and Markets Authority, Ofcom (the U.K.'s communications supervisory authority), the Financial Conduct Authority and the U.K. Information Commissioner's Office.

The consultation exercise closed in June 2023 although it is not known when the government's response will be published. The prime minister will need to call a general election before the end of 2024 at the latest so it remains to be seen whether further policy developments will emerge during the concluding period of the current administration.

The government's AI Safety Summit was held in November 2023 at the historic Bletchley Park site near

London. The event brought together countries, industry and academic leaders from across the globe to discuss how best to manage risks from the most recent advances in AI and to develop a process for future international collaboration.

The summit focused on "frontier AI" which the government considers to be "highly capable general-purpose AI models that can perform a wide variety of tasks and match or exceed the capabilities present in today's most advanced models."

The Bletchley Declaration was agreed by countries attending the Summit. This concluded that future cooperation would focus on identifying risks of shared concern and building a shared understanding of these risks. This includes building risk-based policies to ensure safety through increased transparency, appropriate evaluation metrics, tools for safety testing and scientific research.

The conversation on these topics will continue in 2024 with South Korea agreeing to host a mini virtual summit on AI within the next six months and France hosting the next in-person Summit before the end of the year.

United States 🇺🇸

Federal Law

Contributors: Joe Duball

The landscape for finalizing comprehensive U.S. federal privacy legislation shifted dramatically again in the last year. The momentum U.S. Congress had for a consensus framework leading into 2023 has fallen by the wayside as 2024 begins. Federal lawmakers had only a handful of formal discussions on the proposed American Data Privacy and Protection Act early in 2023 while other privacy bills — mostly targeted rather than comprehensive — were introduced.

As of now, odds of comprehensive privacy legislation in 2024 are not favorable. Congressional priorities beyond privacy legislation are stacking up quickly in an election year. A surprise can never be counted out, but a lack of focus and ongoing dialogue with so many policy points still very much up in the air creates an uphill battle.

Potential artificial intelligence regulation overshadowed Congress' urgency on privacy at the end of 2023 and that focus isn't expected to change in 2024. Unless lawmakers conclude AI and privacy must be addressed simultaneously — a consideration being discussed loosely among lawmakers at this point — the developing competition over which issue gets resolved first will be the story to watch throughout the year. Interestingly, AI legislation debates have been characterized by partisan views on balancing innovation and user safety — a familiar refrain in privacy debates.

There could be a path for children's privacy legislation to emerge this year. A proposed update to the Children's Online Privacy Protection Act remains available for a full Senate vote. It's unclear whether the House would entertain COPPA 2.0 if its provisions could simply go into a comprehensive bill for consumers of all ages. However, pressure from President Joe Biden to do something to protect kids online may tip the scales.

For all U.S. Congress may not accomplish on privacy and AI, U.S. state legislatures are expected to attempt to fill in the gaps. It's hard to ballpark whether the eight comprehensive state laws passed last year were luck or a brewing trend. The proliferation of common provisions might make passing legislation that much more palatable in other states, as seen already in 2024 with bills gaining final passage in New Jersey and New Hampshire. Additionally, Kentucky, Maine and Minnesota each have chances to hit the ground running toward finalization during the 2024 legislative session given past efforts and off-session bill drafting.

Federal Trade Commission

Contributors: Cobun Zweifel-Keegan

2024 is set to be another busy year for the U.S. Federal Trade Commission. Thanks to its consumer protection mandate, the FTC serves as the primary data protection enforcer in the U.S., while also pursuing limited rulemaking authority.

Chair Lina Khan's FTC hit its stride in 2023, at least when it comes to data privacy enforcement actions. On the enforcement side, expect similar trends in 2024, with a focus on children, biometrics, health and other sensitive data types. Currently operating with only three out of five commissioners, the agency is likely to see the final seats filled by two republican nominees, Andrew Ferguson and Melissa Holyoak.

This year also saw the FTC's first case focused on biased AI systems, in a groundbreaking settlement with Rite Aid. Expect more of this in the coming months, as similar one-off enforcement actions help to define the common law of AI governance, informing best practices in this emerging field and expanding on the creative remedies the FTC has pursued, including algorithm disgorgement.

Since this report is focused on legislative trends, we would be remiss not to note the commission's three major ongoing rulemaking activities. If finished, these will have lasting impacts on privacy rules in the U.S., whether Congress acts on privacy or not. The most impactful of these could be the FTC's next step in the long process of promulgating a trade regulation rule on commercial surveillance and data security. The pending NPRM will clarify and streamline the FTC's approach to regulating harmful data practices — and open another comment period for stakeholders to weigh in. Meanwhile, commenters are already busy weighing in on a proposed update to the Children's Online Privacy Protection Act Rule. And the agency will finalize its attempt to "strengthen and modernize" the Health Breach Notification Rule.

In short, expect the FTC to provide more clarity on the expanded expectations for privacy practices precipitated by the fast pace of new technologies like AI.

Health Care

Contributors: Kirk Nahra

The field of health care privacy is undergoing significant disruption. I'm watching several related developments. On the Health Insurance Portability and Accountability Act front, the Biden administration is in the process of evaluating two separate privacy rulemakings — an older one, initially launched by the last administration, related primarily to disclosures of information to social service organizations and to family and caregivers of opioid patients, and the other newer initiative related to privacy implications of the Dobbs decision, focusing on new restrictions on disclosure of reproductive rights information to law enforcement. Dobbs is also driving many of the related issues stemming from the U.S. Federal Trade Commission.

While the U.S. Department of Health and Human Services' Office for Civil Rights remains the primary specific regulatory agency for health care privacy, in recent years OCR has taken a modest back seat to the FTC, which is pushing the envelope on a variety of health-related initiatives. The agency is bringing cases against, for example, a data broker involved in the sale of location data because these activities could potentially reveal locations, including reproductive rights locations. The FTC is redefining the decade old health data breach notification — both through a rulemaking and enforcement actions that seem to presume the rules are already changed — that will both define how health data can be disclosed and then define failures to meet the standards as data breaches.

On the legislative front, the key initiative to watch in 2024 involves Washington state's My Health My Data

Act. Passed in 2023, the law applies explicitly to health data not subject to HIPAA. It broadly defines the scope of health data, far beyond any traditional definition — an expanding trend in many areas — and will apply to restrict the activities of many businesses which do not view themselves as operating in the health sector. Two other states quickly passed similar laws in 2023 and we can expect significant state legislative activity in this area in 2024. We will be watching these independent "health-specific" state laws, as well as how the MHMDA impacts potential "comprehensive" state privacy laws. These laws will have a meaningful impact on how anything encompassed within the definitions of health data can be used and disclosed.

We also are watching initiatives at the congressional level, again driven primarily by Dobbs concerns. While these proposals to provide additional protections for reproductive rights data are not likely to pass on their own, they will drive attention to the issue involving unregulated health data, forcing companies collecting and using any kind of data that might be perceived as health data to act cautiously and carefully. To the extent that a comprehensive federal privacy law comes back on the agenda in 2024 — very much an open issue — this focus on health data at the state and federal level, along with meaningful expansions of what is considered health data, likely will impact some of the terms of any eventual federal privacy law. We also likely will see overlaps with health data in any AI legislation that emerges, with health care being one of the most complicated AI use cases.

Vietnam 🇻🇳

Contributors: Nop Chitranukroh, Phuc Nguyen Huu

On 17 April 2023, the Vietnamese government issued the Personal Data Protection Decree, which is set to take effect 1 July 2023 without any transitional period. The PDPD is considered to be the first comprehensive document on data protection in Vietnam. Accordingly, it provides detailed regulations on the rights of data subjects, consent requirements and requirements for data processing impact assessments and outbound transfer impact assessments.

In 2024, the adoption of the Law on the Protection of Consumer Rights and the Law on Electronic Transactions will play a vital role regarding data protection. The LPCR will require traders to obtain consent to collect consumer data and establish a mechanism enabling consumers to select the information they consent to traders collecting. Consumers must also be allowed to express consent in a suitable form. For special processing purposes — such as sharing, disclosure, or transfer of personal data to third parties, and use of personal data to send advertisements and to introduce products — the LPCR requires a mechanism which enables data subjects to clearly opt in to give, or not give, their consent. This requirement is similar to procedures currently required for regulated stakeholders under the PDPD. In the same vein, the LET strictly forbids the acts of trading data to protect Vietnamese personal data.

The government is anticipated to provide more details relating to data privacy guidelines after the issuance of the Draft Law on Telecommunications. Accordingly, the draft requires enterprises to provide the requisite information — such as service user's name and address, number and location of transmitting or receiving servers, call times, IP address and other personal information supplied by the service user when entering a contract — to the relevant authority, as per a request which is made in accordance with the law.

Amendments to Decree 72/2013/ND-CP on the management, provision and use of internet services will be adopted in 2024. A new draft provision that will be applicable to both onshore and regulated cross-border social network service providers is the requirement to authenticate social network user accounts via their mobile phone numbers in Vietnam. This regulation was proposed by the Ministry of Information and Communications in response to the growing prevalence of cybercrime and aims to enhance state management of social networks and protect personal data, while also increasing user awareness and responsibility around uploading content on the internet.

The Draft Sanction Decree is expected to be issued at the end of 2023 and adopted in 2024. Following the adoption of the PDPD, this will be a supplemental tool used to deal with PDPD violations. Violations, depending on severity, may result in warnings, discipline or administrative penalties or criminal prosecution.

Simultaneously, the Ministry of Public Security established a National Portal on Personal Data Protection to receive reports concerning PDPD violations. Once the portal officially launches, companies are likely to be more vulnerable to inspections, as it will enable data subjects — including company employees or clients — to report noncompliance or personal data breaches more easily.

Therefore, 2023 was a busy year, and 2024 will no doubt be the same.

Zimbabwe 🇿🇼

Contributors: Tsitsi Mariwo

Zimbabwe is on course in terms of implementation of the Cyber and Data Protection Act, promulgated in December 2021. The designated data protection authority, the Postal and Telecommunications Regulatory Authority of Zimbabwe, made significant progress in 2023 in unpacking the law through various awareness raising initiatives held on virtual and physical platforms.

Following issuance of Regulatory Notice 1 of 2022, which sought to kick-start the process of designating data protection officers and notification by controllers of their processing activities, the authority received an overwhelming response in 2023 which enhanced the appreciation of the data protection ecosystem in the country. The response from industry, government and civil society enabled the authority to conduct a snapshot survey on the level of awareness of data protection among the public and level of compliance among the registered controllers. The results of the survey assisted the authority in developing appropriate interventions and mobilizing resources necessary for progressive implementation, which is a process and not an event.

Beyond issuing a public advisory notice on the provisions of the law related to sharing and distribution of intimate pictures without consent, the authority entered into a Memorandum of Agreement with a local university to develop the capacity to implement the law in their various institutions.

Looking to 2024, anticipated developments include the promulgation of the draft Cyber and Data Protection (Licensing of Data Controllers and Appointment of DPOs) Regulations, 2023, which was at consultative stage. The regulations seek to provide more detail on the licensing and registration of DPOs.

In addition, the authority lined up various draft guidelines for consultations with stakeholders. These will guide on matters relating to cross border transfer of personal information, processing of children's data, consent and additional information for DPOs. In partnership with the Harare Institute of Technology, the authority will roll-out training for data protection practitioners in the Zimbabwean ecosystem. The authority also looks forward to deepening international cooperation and exchanging notes and ideas with other data protection authorities.