2023 Global Legislative Predictions

Edited by IAPP Assistant Editor Libby Sweeney

2023 Global Legislative Predictions

Edited by IAPP Assistant Editor Libby Sweeney

2023 could be dubbed the year data privacy and its relevant legislation come to the forefront of Parliaments and presses. In nearly every corner of the world, data privacy legislation can be found impacting everyday life — and not just because we're privacy professionals. This year, anticipate jurisdictions to iterate or build on pre-existing or proposed legislation to keep up with evolving technology while other nations scramble to get some skin in the game and establish a comprehensive privacy law. The IAPP gathered predictions from privacy professionals in 56 nations across six continents and presented them in this white paper so you can see what may play out across the world from on-the-ground experts.

Editor's note: While we try to include as many countries as possible, we recognize this is not a comprehensive list. If you are interested in submitting predictions for a country not featured here, please reach out to IAPP Managing Editor Michelle Clarke at mclarke@iapp.org.

Argentina

Pablo Palazzi

Argentina and the rest of the region will continue to be busy during 2023. Argentina's data protection authority, the Agency of Access to Public Information, led by Beatriz de Anchorena, initiated a public process to amend the country's 22-year-old data protection law. The proposal of the DPA is based on EU General Data Protection principles and a draft was subjected to a comment process during October 2022. The final bill will be ready and submitted to Congress for discussion this year. Hopefully, it will be approved at the end of 2023.

In addition, the enactment of Law No. 27.699 published in the Official Gazette of the Nation on Nov. 30, 2022, meaning Argentina adheres to Convention 108+. The purpose of the regulation is to ensure the protection of individuals regarding automated processing of personal data.

Additionally, Argentina became the first Latin American country to obtain an adequacy determination by the European Union.

Australia

Keith Eyre, CIPP/E, CIPM, CIPT, FIP

In 2023 we can expect the Privacy Legislation Amendment (Enforcement and Other Measures) Bill to come into force and see further reforms to the Privacy Act.

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill was introduced and passed by the House of Representatives in November 2022. The bill was introduced following several major data breaches that impacted millions of Australians and is expected to become law. If the bill comes into force, it will significantly increase the penalties for serious or repeated privacy breaches and provide the privacy commissioner a greater range of compliance powers. Note that there is no change to allow the Office of the Australian Information Commissioner to levy fines directly; it must still ask the federal court to levy fines.

By early 2023, the government will have completed its Privacy Act review report, which will recommend further reforms to the act. We can then expect a bill to amend the Privacy Act, which, if passed into law, could come into effect in the second half of 2023 or in 2024. It is possible that a draft bill may be made available for consultation before a bill is introduced into Parliament.

We can expect the reforms to cover stricter requirements for when and how consent is obtained, an updated definition of "personal information" to include technical data and online identifiers, an emphasis on accountability for privacy risk management, enhancement of the OAIC's enforcement powers including directly levying fines and further rights for individuals.

Austria

Rainer Knyrim, CIPP/E, CIPM, CIPT

The biggest development for privacy and data protection in Austria comes in the form of the national implementation of the EU Whistleblower Directive. It was implemented into Austrian federal law with Austria's Whistleblower Protection Act as well as a number of provincial laws only applicable in specific provinces of Austria, such as the Whistleblower Protection Act-Vienna.

The federal act requires private companies as well as legal entities created by federal law or owned by the Austrian state with 50 or more employees to establish internal whistleblowing systems. In addition, the law establishes pre-existing supervisory authorities (such as the Federal Office for the Prevention of and Fight against Corruption) as external whistleblowing reporting bodies. The federal law has not yet passed, but a respective draft by the Austrian Parliament has already been forwarded to the Federal Ministry of Labour and Economy.

The provincial laws require the establishment of internal whistleblowing systems for information on infringements related to the administrative bodies of the specific province and their legal entities. Additionally, they require the establishment of external whistleblowing bodies for reporting infringements related to provincial parliamentary legislation. The number of provincial acts varies for each province, with some opting for a single, all-encompassing act and others regulating specific sectors, such as civil servants, in a separate act. As of November 2022, there exist 14 acts for the nine provinces of Austria.

Both the federal and provincial acts aim to protect employees, civil servants and interns from the potential backlash of reporting infringements of the law in the sectors dictated by EU Acts, such as financial services and markets, product safety, or the protection of privacy and personal data.

Another interesting development can be expected concerning the implementation of the EU Directive on protection of the collective interests, which would introduce the possibility of a class action lawsuit against certain law infringements by companies. Violations of the GDPR are explicitly mentioned as an example. Although the transposition deadline ended Dec. 25, 2022, actual implementation can be expected this year.

🇧🇪 Belgium

Diletta de Cicco, CIPP/E
Charles Helleputte, CIPP/E

2022 was a bumpy year for data protection in Belgium, at least when looking at its primary enforcer, the Belgian Data Protection Authority. 2023 will serve as a year zero for the renewed ADP 2.0. Following too many press headlines, resignations and an infringement procedure launched by the European Commission, the time for a reshuffle in leadership has come. Historic and prominent figures were dismissed or resigned; new leadership took the rein of a reorganized body mid-2022.

This year will serve as a test case on at least three majors fronts for the ADP:

- Deliver on the use of codes of conduct as a transfer mechanism in the cloud area, a matter that has less to do with the pioneer position of Brussels in the sector and more to do with the country (in particular its capital) being home to many trade associations (and you can also say cloudy sky, if you happen to live here).
- Confront its reasoning in the International Advertising Bureau Europe case with the outcome of the proceeding that is pending in front of the Court of Justice of the European Union, which could have far-reaching implications.
- Lodge a call for additional funding with the government to prepare — on time for once — to deal with the upcoming new roles the ADP will play in the future, including following the upcoming adoption of the EU Artificial Intelligence Act.

2023 will finally be the last chance for strategic progresses in the long list of EU digital files (the AI Act, the Data Act, etc.) as well as the progressive entry into force of those files already adopted at the EU level. Their impact will reshape the landscape across the EU, including the stakeholder interest in the legislative process concentrated in Belgium.

🇧🇲 Bermuda

Nancy Volesky, CIPP/US

Destined to be a landmark year for privacy evolution in Bermuda, the government will finally implement the Personal Information Protection Act 2016, using a phased-in approach. While it is not clear what parts of the PIPA will come into force initially, organizations should be completing preparations to ensure full compliance in any case. In tandem, the government has on its agenda a few amendments to the PIPA, but they are not expected to be significant.

Other changes anticipated will be the result of complex work done to harmonize the PIPA and the 2010 Public Access to Information Act (addressing freedom of information) — legislation will be introduced to this effect. Efforts also continue on both the harmonization of the PIPA and the Electronic Transactions Act, 1999, as well as the development of a robust cybersecurity framework for the country.

It is anticipated that Privacy Commissioner Alexander White, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP, will proceed with staffing up his office, expanding its outreach and providing further resources, training and compliance capabilities in anticipation of the active year ahead.

On the international privacy front, all eyes are on Bermuda in late October, as the island hosts the 2023 Global Privacy Assembly. Welcomed by Commissioner White, global privacy regulators, data protection regulators and policymakers will meet for a week of activities and deliberations.

Bolivia

Ana Valeria Escobar Romano

2023 is likely to be a year of important changes in data privacy and protection for Bolivia.

Bolivia has recently been in a political turmoil, where changes in government gave greater preponderance to the economic recovery of the country. This meant putting on hold all the projects promoted by civil society related to privacy, causing them to be shelved by the legislative body.

However, as a state agency, the Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación has started to promote regulation on this matter by proposing a legal draft.

The AGETIC's proposal is a new crusade where a body of the government seeks to implement data protection rules, close to the EU GDPR, putting Bolivia at the forefront of personal data protection regulations.

The project is currently being socialized and commented on by experts for future consideration by a legislative commission. This would allow it to be reviewed by the legislature and Senate on the second half of 2023.

Brazil

Angela Bittencourt da Fonseca, CIPP/E, CIPM, CDPO/BR

Brazil's DPA, the Autoridade Nacional de Proteção de Dados, released a handy hint in November 2022: the much-expected Regulatory Schedule for 2023-2024, divided into four phases. The first phase starts with 12 outstanding themes from the previous 2021-2022 schedule, and the second phase, comprising of four themes, will start within the upcoming year. The third and fourth phases won't start until mid-2024.

The choice of themes reflect that the ANPD — which was upgraded in 2022 to an autonomous federal agency — has been building a solid foundation for the enforcement of monetary penalties for legal infractions, and for setting forth rules to other governmental entities' data processing activities. In addition, the ANPD has been quite responsive to the concerns and FAQs from the privacy community: The DPA consolidated many topics the General Data Protection Law left "to be further regulated," such as certain data subject rights, communication of security incidents, international data transfers, impact assessment reports for high-risk processing activities, processing of children's data, best practices and data governance.

On the legislative front, the Senate has been drafting a bill for artificial intelligence, which includes ethical use, fundamental rights, personal data, accountability, data mining and copyright. The work group has emphasized the need for a comprehensive law with a "risk-based approach," including "algorithm impact assessments" and "high-risk activities." It will probably mature into law this year, sooner than the ANPD's ruling on

AI in automated decision-making, which is expected for 2024 only, on the third phase.

Another Senate bill worth following covers tax incentives for companies adapting to the LGPD and other privacy regulations by compensating expenses from the adaptation, such as retention of privacy professionals and specialized software subscription, from their taxable income.

Canada

Shaun Brown

There are at least two significant developments to watch for in 2023. First, although the changes under Bill 64 in Quebec began September 2022, most of the changes take effect September 2023. Organizations doing business in Quebec will need to consider how to comply with new requirements that are not always clear, while the under-resourced DPA, the Commission d'accès à l'information du Quebec, struggles to keep up with demand for guidance. The new penalties inspired by the GDPR will introduce a level of risk not seen in Canada since Canada's Anti-Spam Legislation came into effect in 2014.

Bill C-27 was introduced in June 2022. The federal bill would replace the Personal Information Protection and Electronic Documents Act with the Consumer Privacy Protection Act and also create the Artificial Intelligence and Data Act. With no election on the near horizon, there is no good reason why the bill shouldn't be finalized in 2023. At minimum, the bill should be reviewed by the House of Commons Standing Committee on Industry and Technology, which will hopefully lead to improvements.

By now, the Ontario government should have had time to digest comments received on its consultations on privacy modernization on Ontario, which includes a proposal to develop new private-sector privacy legislation. Comments were due September 2021, so we should have an idea by the end of 2023 whether this initiative will move ahead or fizzle out.

Chile

María José Díaz
Javiera Sepúlveda

Many changes are expected in the regulatory field of Chile in 2023. Though we still wait for the bill that will modify the privacy protection law to pass, the bill did make made considerable progress in 2022. However, the legislative discussion will take longer than expected as the Chamber of Deputies has introduced several changes to the text approved by the Senate; therefore, the bill shall be discussed in a "Mix Commission" (composed of deputies and senators). It is expected to finally be approved and passed this year.

Another intense discussion that will continue is the bill that Establishes a Framework Law on Cybersecurity and Critical Information Infrastructure. Particularly, this bill creates a regulatory framework necessary for the development of cybersecurity, both in its operational and regulatory dimensions, regarding CII. The bill sets forth criteria to determine if a public or private institution has CII, and it creates new public institutions that aim to ensure cybersecurity at the national and sectoral levels, including the National Cybersecurity Agency.

Finally, smaller yet no less critical bills are being discussed in Congress, such as a bill to regulate digital platforms — particularly rights and obligations addressed to agents, providers, users and consumers of digital platforms — and a bill presented in October 2022 that establishes the right to be forgotten in financial matters.

China

Barbara Li

2022 was a remarkable year in China's data regime, as the Cybersecurity Administration of China (China's central data regulator), either individually or jointly with other Chinese central regulators, issued or adopted a considerable number of important rules to facilitate the implementation of China's three major data laws: the Personal Information Protection Law, Data Security Law and Cybersecurity Law. The CAC clarified the legal mechanisms and relevant compliance requirements and procedures. With the new rules, guidelines, national standards and draft standard contractual clauses for cross-border data transfers, business organizations now have more clarity and a better tool for self-assessment according to their specific business scenarios and can determine the proper mechanism for making outward transfers of locally generated data collected abroad.

2022 also witnessed a significant breakthrough in enforcement actions taken by Chinese data regulators. Multiple rounds of investigations of noncompliance of the PIPL, DSL and CSL were done by the governmental authorities. Thousands of mobile applications were removed from app stores. The CAC imposed a record-high fine of approximately US$1.2 billion on a major Chinese internet company for various violations of China's data and cybersecurity rules, including illegal collection of personal information without the proper authorization from data subjects and excessive collection of sensitive personal information, such as geolocation information and facial recognition images. Two senior management individuals of that company were each fined approximately US$140,000.

The forthcoming 2023 will continue to be a busy year in terms of data legislation and enforcement developments. Earlier in 2022, the lawmaking body issued the draft amendments to the CSL, and CAC issued the draft Measures on Administrative Enforcement Procedures for public comment. The proposed amendments to the CSL purport to significantly increase penalties: A corporate violator would face a fine of up to approximately US$7 million or 5% of the last year's turnover and the senior executives would face a fine of up to approximately US$140,000. The regulations on critical information infrastructures and important data are also expected to be finalized and so is the draft standard contract for cross-border data transfers, as they have all gone through public consultation and have been heavily discussed among lawmaking bodies, industry regulators and key stakeholders.

On the enforcement front, March will be an important milestone, as the grace period for security assessments for cross-border data transfers will expire end of February. Enforcement actions are anticipated against noncompliant business organizations next March.

Mobile apps have been the primary targets for enforcement in the past 12 months and this trend will continue, given China is the largest mobile app market in the world. The authorities are expected to adopt a wide range of enforcement measures including order for rectification within a prescribed period, suspension of app operation, removal of apps from the app store, and imposing fines on the app operator and senior executives. Investigations for complying with multilevel protection schemes and data classification requirements under the CSL and DSL will remain active, especially in regulated industries of financial, health care, technology, transportation, energy and public utilities.

Colombia

Luis Alberto Montezuma, FIP

2022 ended with the entry into force of the reform to the Credit Reporting Act, embedding strong accountability measures by requiring credit providers and credit reporting agencies to take reasonable steps to establish and maintain internal practices, procedures and systems that ensure individuals' interest in protecting their personal data. The law also works in compliance with other law, ensuring that credit providers have sufficient information available to assist them in deciding whether to provide an individual with credit or service.

The legal system governing privacy and data protection in Colombia has its roots in Articles 15 and 20 of the Colombian Constitution. The Constitutional Court of Colombia ruled that foreign nationals are also the subject of fundamental rights. In a recent judgment, the Constitutional Court ensured the right to the protection of personal data for an Israeli citizen and ordered Colombia's national police to provide access to the personal data relating to criminal convictions and offenses the entity holds about the person.

To facilitate the use of binding corporate rules for controllers as a mechanism to transfer personal data between data controllers within the same group, the Executive Decree 255 of 2022 establishes the Controller Binding Corporate Rules scheme in accordance with Article 27 of Colombia's general data protection framework, Law 1581 of 2012. Companies can apply through the website of Colombia's DPA, the Superintendencia de Industria y Comercio.

The Dubai International Financial Centre Commissioner of Data Protection issued a decision recognizing the equivalence of the Colombia data protection regime for international transfers. Colombia seeks an adequacy decision from both the European Commission and the U.K. Secretary of State.

2023 promises to be an exciting year for data protection in Colombia. The president of Colombia is expected to appoint the new Superintendence of Industry and Commerce of Colombia, which is responsible for appointing the new Superintendent Delegate for the Protection of Personal Data. The Superintendent Delegate is responsible for monitoring the application of Colombia's general data protection framework through guidance, supervision and enforcement. The new government has shown no interest in modifying the current Law 1581 of 2012, inspired by the EU's Data Protection Directive.

Czech Republic

František Nonnemann, CIPP/E

Since January 2022, new rules for the use of cookies and telemarketing have come into effect in the Czech Republic. The opt-in principle was introduced in both cases. The Czech Republic's DPA, the Úřad pro ochranu osobních údajů, issued guidance for both areas and will continue focusing on them in 2023.

Legislative change of the basic identifier of natural persons should be completed in the Czech Republic this year. The current system of birth numbers was introduced as an identification for the state social insurance system, but its use gradually spread to the entire public and a large part of the private sector. It reveals birthdate and gender of a citizen, but its use increased risk of linking information from different databases and ID theft. In 2025, the birth numbers will be discontinued, especially in the private sector. From January 2024, the birth number is to be removed from national ID cards and a national system of basic registers should fully replace them.

A general whistleblowing law is also anticipated in 2023. The draft law that transposes the corresponding EU Whistleblower Directive has already been published, and its effectiveness is expected in the second half of 2023. There are two important aspects from a data privacy point of view: For many private and public organizations, new obligations to receive and respond to notifications about possible privacy protection violations will be introduced. At the same time, this raises several questions about how to process and protect personal data within the entire whistleblowing process.

We do not expect any further significant legislative changes with direct impact on the protection of personal data in the Czech Republic this year. The year 2023 will instead be an opportunity to breathe before the wave of new regulation from the EU. From the NIS 2 and the digital operational resilience act to the Data Act, Artificial Intelligence Regulation and the Digital Services Act package, coming years will be interesting for the data and cybersecurity regulation.

Ecuador

Rafael Serrano
Pablo Dent
Christian Razza

2023 will be a year of great importance for privacy and data protection in Ecuador. It has been a year and a half since the enactment of the Personal Data Protection Law. Both the private and public sectors are implementing the law.

The presidency is working on the regulation of the Data Protection Law, which is expected to publish early this year. This regulation will include specific topics such as the headquarters of the data protection superintendence, the personal data protection delegate and its functions, the auxiliary control system, control mechanisms, and procedures for the exercise of rights recognized in the law.

The creation of Ecuador's Personal Data Protection Authority is expected early this year as well. The authority will be a superintendency. The presidency will send the shortlist to the Council of Citizen Participation (the body in charge of the appointment) of possible superintendents and once selected, they will oversee organizing and implementing the superintendency. Delays in the creation of the superintendency have generated uncertainty regarding the application of the law.

The sanctioning regime will enter into force May 26. Fines for minor infractions will be from 0.1% to 0.7% of the turnover and serious infractions from 0.7% to 1% of the total turnover of the preceding year. In addition to the sanctions, the authority may impose corrective measures, which may include the surcease of processing, deletion of the data and imposition of technical, legal, organizational or administrative measures to ensure proper processing of personal data.

This year will be the first year in which both the private and public sectors will have to implement a new regulatory system. There is great uncertainty as to how the superintendency will act; there remains doubt as to whether it will be an educating or sanctioning entity in its first months.

Ethiopia

Yohannes Eneyew Ayalew

2022 highlighted the need to enact a comprehensive data protection law in Ethiopia. This year we can expect to see the introduction of the Data Protection Proclamation and further headway on the Ethiopian government's commitment to establish an independent DPA. The Proclamation to Provide for Personal Data Protection, released in 2020 as an exposure

draft under the sponsorship of the Ministry of Science and Technology, seeks to regulate the processing of personal data and the protection of fundamental rights — and in particular an individual's right to privacy — with regard to automatic processing of personal data.

Moreover, the draft proclamation defines the rights and duties of data controllers and processors, governs data transfers and introduces a system that ensures a strong culture of personal data protection. Most of the provisions of the draft proclamation such as data subjects' rights and principles of data processing are drawn from the EU GDPR. As a result, the long arm of the GDPR commonly referred to as the "Brussels Effect" is visible in its operative provisions.

Ethiopia is yet to establish an independent DPA. Thus, in order to enhance individuals' and groups' control over their data, the forthcoming proclamation amongst other things needs to facilitate and create a strong and independent DPA as suggested by civil societies. It is hoped that the government will establish a freestanding and independent DPA by expressly granting the body with the institutional capability through budgeting, staffing, implied powers and jurisdictional competency, as well as guarantees against the interferences of private actors — mainly data controllers and market players.

However, there is a growing concern toward the rolling out of digital IDs by the Ethiopian National ID Office as the practice flouts the data protection and privacy rights of millions of Ethiopians. Given that the country is ruled by an ethnic federal system, the digital ID system could be misused by authorities unless backed by a proper data protection impact assessment and an adequate data protection law. Rolling out digital ID without observing these conditions is like putting the cart before the horse.

All the same, the commencement of private telecommunications in 2022 and further liberalizations of the market may serve as a catalyst for a robust data privacy initiative in Ethiopia. Finally, let's hope that there will be a major breakthrough in 2023, the proclamation will be enacted and the DPA will be established independently.

EU

Isabelle Roccia

2023 will be a year of continued legislative change in Europe — the rush to the finish line for EU legislators and implementation for privacy professionals as data protection rules become increasingly intricate across Europe. New rules enacted in the EU in 2022 will go into effect this year and beyond. In the data governance realm, these policies primarily touch on data sharing, content moderation, targeted advertising, transparency and cybersecurity. In addition, EU policymakers are negotiating further policies that may wrap up before the next EU legislative cycle soft-launches early 2024. Proposals currently on the table focus on artificial intelligence governance and liability, sectoral rules for data sharing (particularly in the health space), children's protection online and industrial data governance.

Enforcement of the GDPR and other privacy-related rules will also remain a priority for the European Commission and regulators alike. After a record year for GDPR noncompliance fines, enforcement is expected to ramp up in 2023. The European Data Protection Board is expected to launch its second coordinated enforcement action in February, with a focus on the designation and position of the DPO. The objective of the action will be to safeguard the position of DPO and its importance in organizations. Participating DPAs will conduct coordinated actions and evidence-gathering throughout

the year, leading to an end-of-year report that may include follow-up enforcement actions at a national level or guidance on an EDPB level.

Several significant cases are pending before national regulators and the Court of Justice of the European Union, which could lead to transformative decisions for privacy professionals in the next year on areas ranging from children's data, employee data processing, transfer mechanisms and more.

Finland

Eija Warma-Lehtinen, CIPP/E

The Nordic DPAs had their annual meeting in Helsinki in October where they decided some common goals.

In 2023, Finland's employee privacy law, the Act on the Protection of Privacy in Working Life, will be amended regarding collection of applicant/employee data. It is worth noting that Finland has specific employee privacy laws in addition to the GDPR and that Finland's DPA, the Office of the Data Protection Ombudsman, has given several decisions (including fines) for noncompliance of those laws. Also, the new whistleblowing directive will be implemented and controllers must draft data protection documentation, including a data protection impact assessment, in order to implement the channel properly.

The ombudsman recently launched the two-year project GDPR4CHLDRN together with the Finnish Information Society Development Centre that provides information on the processing of personal data to associations that organize leisure activities for children. The project, among other things, will create tools to support the application of data protection legislation by children's and youth clubs as well as improve awareness of children, young people and their parents.

The ombudsman receives approximately 10,000 new cases per year; about half of them are data breach notifications. The DPA actively reports their cases and decisions, which are increasingly appealed to the administrative courts. We can expect several interesting court decisions in the coming year.

France

Cécile Martin

Among the various privacy trends we can anticipate for France this year, we can probably mention the sphere of the working world and the willingness of France's DPA, the Commission nationale de l'informatique et des libertés, to regulate the increasing collection of personal data on smartphone apps.

Indeed, whether it is in the recruitment process, work contracts, attendance or interviews, companies have considerably invested in artificial intelligence. While not new, this massive arrival of algorithms in the work environment can systematize biases that could deprive certain job applicants or employees from opportunities in terms of hiring or promotion. It is therefore highly likely that litigation related to these issues will increase.

With regard to the collection of personal data by apps, the CNIL announced in its 2022-2024 strategic plan that, in view of the opacity of technologies and the heterogeneity of practices, it aims to make data flows visible and strengthen the compliance of apps in order to better protect the privacy of users. In order to implement this strategy, the CNIL intends to focus on certain topics to raise the awareness among users and lead a European version of the approach.

Germany

Ernst O. Wilhelm, CIPP/E, CIPM, CIPT, FIP

The European Commission's Data Act, which is intended to facilitate a framework for fair and innovative data sharing (both personal and non-personal), is expected to be adopted this year. This proposed regulation will have a massive impact on the German economy.

Along with major relevance of the automotive industry, according to the German Association of the Automotive Industry, "modern vehicles generate around 25 gigabytes of data material per hour," including but not limited to mileage, speed, location and driving behavior. The dispute about the best way to use and share this data has already gained momentum this year by the so-called ADAXO proposal from the German Association of the Automotive Industry and by a counterproposal giving more emphasis on the rights of the data subjects from the Federation of German Consumer Organisations. This discussion is expected to intensify this year in course of the finalization of the EU Data Act and the discussion of the planned German Mobility Data Act.

Last year, the European Commission launched the European Health Data Space, which aims to offer a trustworthy framework for primary use of health data by the patient and for secondary use cases including research, innovation, policymaking and regulatory activities. The Federal Association of Pharmaceutical Manufacturers recently published a statement claiming the need for access to patient data for the development of commercial health products and services. Only a few days later, the German DPAs released the so-called "Peterburger Declaration," emphasizing the rights and freedoms of the data subjects. The dispute is expected to intensify this year in the course of the discussion of the draft of the Federal Ministry of Health for a Patient Data Protection Law, in particular regarding whether opt-in, opt-out or broad consent should be required for the use of patient data for research purposes.

Greece

Antonios Broumas, CIPP/E

Compared to 2022, the national elections taking place in this coming spring are expected to influence the pace of data protection legislative developments and supervisory activity in the country.

An amendment of national data protection Law 4624/2019 has already been put into public consultation, following a letter of formal notice by the European Commission initiating the infringement procedure against Greece for failure to adequately transpose the Law Enforcement Directive. Apart from the LED, another amendment of Law 4624/2019 is bound to take place within the year, this time improving its provisions supplementing the GDPR. These twin amendments are expected to upgrade national data protection legislation to the benefit of public bodies, businesses and data subjects.

Other developments will mainly concern the implementation of EU cybersecurity legislation and the enactment of supplementary national legislation for major EU Acts, such as the Digital Services Act, Markets Act, Media Freedom Act and AI Act.

At the level of supervision, the Hellenic Data Protection Authority is expected to reap the benefits of its internal organizational restructuring, keep pace with supervisory interventions and milestone decisions at the same or similar level as in 2022, and gain ground on its backlog of pending cases. Nevertheless, the HDPA is likely not bound to take major horizontal or sectoral initiatives for the regulation or supervision of the market until next fall, when the newly convened Parliament will

be required to appoint its new head. In any case, the HDPA shall strictly align with the EDPB fine calculation criteria in its upcoming jurisprudence and impose increased sanctions to obligated entities, indicating to markets the high level of compliance maturity expected by them.

Hong Kong

Timothy Ma, CIPP/E, CIPM
Kieran Donovan

In 2023, doxxing is expected to remain a major area of focus and active enforcement by Hong Kong's DPA, the Privacy Commissioner for Personal Data. The PCPD made eight arrests against individuals for doxxing-related acts in 2022, and the first conviction for a doxxing offense was handed down in October. In the PCPD's 2021-22 annual report, the PCPD emphasized its efforts in combatting doxxing, reporting that since the commencement of the amended Personal Data (Privacy) Ordinance, it has handled 928 doxxing cases, issued over 600 cessation notices to various online platforms and commenced criminal investigations into 65 cases.

The PCPD also noted it will continue to work with the Hong Kong government in reviewing the PDPO, with a view to formulating substantial legislative proposals to align with the international norms and regulatory practices. Discussions on such updates to the PDPO began January 2020, when the Constitutional and Mainland Affairs Bureau proposed certain amendments, including establishing a mandatory data breach notification mechanism, requiring data users to devise a data retention period policy, empowering the PCPD to hand down administrative fines and directly regulating data processors. Whilst the timeline for the review is still unclear, this appears to also be an area of focus for the PCPD in 2023. Concrete legislative proposals are expected to be formulated as the next step.

In July 2022, Hong Kong's Law Reform Commission issued its consultation paper on Cyber-Dependent Crimes and Jurisdictional Issues, setting out proposals for a new cybercrime legislation (including the introduction of five new offenses) to address cybercrimes and cybersecurity in connection with advancements in information technology and the risk of exploitation for criminal purposes. This paper is the first of three to be published by the LRC, with the other papers expected to be published this year and focus on cyber-enabled crimes, macro challenges in the digital age, and evidentiary and enforcement issues.

Hungary

Tamas Bereczki, CIPP/E
Ádám Liber, CIPP/E, CIPM, FIP

We do not expect the adoption of any material new rules in privacy and data protection in Hungary in 2023. The main reason is Hungary's priority to resolve the corruption allegations by the European Commission and access cohesion and recovery funding from the EU. In response to the allegations, Hungary has introduced various legislative reforms and an anti-corruption authority with wide investigative powers.

We predict that the enforcement and fines will continue to increase on the part of Hungary's DPA, the National Authority for Data Protection and Freedom of Information. The NAIH priorities include direct marketing activities and customer satisfaction surveys, artificial intelligence and machine learning, CCTV and video surveillance issues, and the use of Google Analytics, cookies and similar technologies. Targeted sectors include the financial sector, debt collection activities and call center operators. Digital services will remain among the enforcement priorities of the Hungarian Competition Authority, which targets consumer data use activities and dark patterns.

India

Pranav Rai

A key development to watch out for in 2023 will be the progression of India's new proposed Digital Personal Data Protection Bill. The Ministry of Electronics and Information Technology will hold a wide public consultation before introducing it in the Parliament.

This is the fourth version of a personal data protection law since 2017 — the year the Supreme Court of India held privacy to an inalienable and inherent fundamental right guaranteed under the Constitution of India. Since then, the government's efforts to develop a comprehensive data protection law only gained momentum.

The explanatory note to the bill suggests it will establish a comprehensive legal framework governing digital personal data protection in India and that the government has considered the global best practices (which includes "prospective federal legislation of the United States of America"). The bill is a compact one, containing 30 sections — the earlier bill had more than 90 — but seems to have a disproportionate share of potentially controversial issues, such as: questionable independence of the DPA, the Data Protection Board; broad exemptions in the "public interest" (defined to include "preventing dissemination of false statements") and for "instrumentality of the State;" certain unusual duties (accompanied by penalty) imposed on data subjects (e.g., to ensure that the information furnished is "verifiably authentic"); and perhaps most vital, several issues left at the discretion of the executive under the government's rulemaking power (with inadequate Parliamentary oversight).

The bill may not be an ideal personal data protection law, but the alacrity with which the government has approached this bill — in stark contrast to the manner it handled the 2019 bill — deserves due praise. It was quick and judicious in withdrawing the earlier 2019 bill, drafting this bill, and timing the public consultations so the consultation period ends before the start of the budget session of Parliament, thus increasing its chances to introduce the bill in Parliament early 2023.

Indonesia

Glenn Wijaya

The Law No. 27 Year 2022 on Personal Data Protection, enacted Oct. 17, 2022, envisages there will be at least two implementing regulations: a government regulation and a presidential regulation.

The government regulation will specify the following:

- Submission of objections to automatic processing (Article 10).
- Violations of the processing of personal data and procedures for the imposition of compensation (Article 12).
- Rights of personal data subjects to use and transmit personal data (Article 13).
- Personal data protection impact assessments (Article 34).
- Notification procedures (Article 48).
- Transfer of personal data (Article 56).
- Imposition of administrative sanctions (Article 57).
- Provisions on the procedures to implement the authorities of the PDP Institution (Article 61).

Meanwhile, the presidential regulation will set out the details about the future DPA, the PDP Institution (Article 58).

According to the Minister of Communications and Informatics, the government of Indonesia is now preparing the presidential regulation and other implementing regulations (without specifying what these are).

The PDP Law was originally anticipated to be promulgated in 2021, followed by one PDP Law implementing regulation (which the author believes is the said government regulation), one PDP Law implementing regulation establishing the PDP Law's implementation institution (which the author believes is the said presidential regulation) to come this year, and the establishment of three training institutions for DPOs, all of which would occur successively, one year apart from one another.

However, given that the PDP Law was only enacted October 2022, we should anticipate that its implementing regulations will not be issued until some time this year, the PDP Institution will not be established until 2024, and the establishment of training institutions will not happen until 2025.

Ireland

Kate Colleary, CIPP/E, CIPM

The Data Sharing and Governance Act 2019 introduced requirements for the sharing of information (including personal data) between public bodies. It provides a legal basis for public bodies to share this data. The 2019 Act also established the Data Governance Board, base registries and the Personal Data Access Portal. The aim is to reduce the administrative burden associated with the need for individuals to provide their personal data to numerous public bodies. The final phase of the DSGA's commencement occurred Dec. 16, 2022. Thus, 2023 is the first year where the DSGA is fully operational.

2023 is also the second year the Data Protection Commission seeks to implement its 2022-2027 Regulatory Strategy. The strategy consists of five goals:

1. Regulate consistently and effectively.
2. Safeguard individuals and promote data protection awareness.
3. Prioritize the protection of children and other vulnerable groups.
4. Bring clarity to stakeholders.
5. Support organizations and drive compliance.

The DPC will continue to prioritize complaints of systemic importance and will seek a collective approach to enforcement throughout Europe.

The deadline for the transposition of the EU Representative Actions Directive (EU) 2020/1828 was Dec. 25, 2022. The General Scheme of the Representative Actions for the Protection of the Collective Interests of Consumers Bill 2022 will implement the collective redress mechanisms set out in the directive. This legislation, which is set to take effect in June, will be the first piece of legislation in Ireland to set out a legal procedure for group action. It will undoubtedly have a significant impact on the litigation of data protection actions in Ireland.

2023 is likely to continue the trend of investigations, significant fines and appeals and will likely be (yet another) busy year for privacy pros.

Israel

Dan Or-Hof, CIPP/E, CIPP/US, CIPM, FIP

The discussions between the EU and Israel on the continuance of the 2011 adequacy recognition are still underway with no published end date. On Oct. 2, 2022, as an effort to maintain the adequacy recognition, the Israeli government established the independent status of its DPA, the Protection of Privacy Authority, through a government resolution. Furthermore, as an additional effort the satisfy the EU counterparties, the Israeli Ministry of Justice promoted the enactment of new regulations under the Protection of Privacy Law, which will provide additional

protection to personal data that originates from the EU.

The additional protections include the right of erasure and enhanced provisions related to data retention, data accuracy and the duty to inform via privacy notices. This effort was heavily scrutinized by privacy practitioners and scholars, who urged the Ministry of Justice to enact regulations that will apply the proposed additional rights to all personal data.

As a result of frequent elections in Israel, substantial amendments to the PPL are still pending. It remains to be seen if the current government will move forward with the enactment of the amending bills, which include providing the PPA with substantial enforcement powers and considerably reducing the mandatory database registration obligation. Class actions 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

Rocco Panetta, CIPP/E

Since 2022 proved to be a very busy year for Italy and its DPA, the Garante, this likely presages an equally intense 2023.

The DPA's interest in protecting minors and educating citizens to a greater awareness of what privacy is and its importance continued. On the one hand, the dialogue with social networks such as TikTok remains. On the other hand, the Garante signed several agreements bringing these issues to television and schools. Presented alongside other projects that covered the data economy scenario, the heart of the project was presented at the State of Privacy '22 initiative — attended by 250 private and public experts, including European Data Protection Supervisor Wojciech Wiewiórowski — to gather ideas around the major themes of the data economy.

In the past year, some media companies asked readers to pay a subscription fee if they do not want to be profiled. This issue and potential reaction from the Garante will lay the foundation for future data economy decisions. Professionals in the sector are divided between more conservative views and considering this possibility valid. This debate will see an acceleration in 2023, also starting from the fact that it is now the European institutions themselves that recognize services are paid for with personal data. In addition, continuing debate on artificial intelligence and the transparency of algorithms, I believe 2023 will be the year Italy will decide what kind of data economy it would like to see realized.

Japan

Hiroyuki Tanaka

On April 1, 2022, nearly all the Act on Protection of Personal Information amendments took effect, save for amendments regarding local governments and local incorporated administrative agencies, which enter into effect April 1 of this year.

The amended Telecommunications Business Act enacted in June 2022 that includes new cookie regulations will take effect no later than June 16 this year. This will introduce new obligations on telecommunication service providers that have non-trivial impacts on users' interests. When a TSP communicates a command for the external transmission of information (including cookies) from users to third parties, a TSP is required to either (a) notify certain information to users or make such information easily available to users, (ii) obtain opt-in consent or (iii) provide an opt-out mechanism. According to the latest

draft of the TBA Ordinance, a TSP will be an entity that provides (a) a service of intermediating telecommunication of others, (b) social media services, bulletin board systems, movie-sharing services, online shopping malls, etc., (c) online search engines or (d) various information, such as news, weather, movies and maps to unspecified people. So in practice, if your business is categorized as a TSP, then preparing cookie policy or the like will be required at a minimum, although offering opt-in consent or an opt-out mechanism is optional.

Kenya

Elias Okwara, CIPP/E, CIPP/US

2022 was a very active year for Kenya's DPA, the Office of the Data Protection Commissioner. The ODPC launched its Strategic Plan and Data Protection Curriculum and published three data protection regulations. For enforcement, the ODPC initiated an audit of 40 digital lenders and undertook enforcement action against a health care provider.

The ODPC also beefed up its manpower by hiring dozens of new staff and conducting training for senior staff. The commissioner and other officials also went to Europe, met with EU Justice Commissioner Didier Reynders and discussed collaboration between the EU and Kenya on data protection matters. Kenya was also accredited to join the Global Privacy Assembly during the assembly's 44th session held in Istanbul, Turkey.

2023 is set to become even more active and interesting for Kenya.

We should expect the ODPC to continue on the path of enforcement and potentially target "big fish" in the event of complaints or the ODPC's own investigations. It will be interesting to see which multinationals may be in the crosshairs given the existing imbalance in the provision of rights to data subjects in Africa. At the same time, Kenya has a culture of publishing highly personal information, particularly by public entities during human resource recruitment. We should look forward to guidance by the ODPC to public entities on such matters. Furthermore, Kenya was the only African country included on the U.K.'s list of priority destinations for adequacy, so we should expect movement toward making this a reality. At the same time, the commissioner indicated her support for harmonized approaches to data privacy, and therefore activity around the Network of African Data Protection Authorities is expected.

Latvia

Anna Vladimirova-Kryukova, CIPP/E

In 2022, Latvia's DPA, the Data State Inspectorate, focused on several aspects: cookies and related tracking technologies, anti-money laundering within data protection contexts, and the role of a DPO. For instance, it performed several preventive audits in the private and public sector regarding cookies and DPOs respectively. In addition, it elaborated data processing guidelines for anti-money laundering purposes. Then, it was entrusted in supervising know-your-customer service providers.

Thus, it is expected that one of the main new activities of the DVI will be related to monitoring whether KYC tools are compliant with the applicable requirements.

Also, taking into consideration the results of the preventive cookie audits, it is expected that cookies and other e-commerce and marketing-related data processing activities will be subject to further attention from different sides.

The DVI also imposed its highest penalty for GDPR violations: 1.2 million euros, which is now being examined by the local courts. The litigation should be followed by privacy professionals as it will help understand more about the procedural part of dealing with data protection violations.

Lithuania

Natalija Bitiukova, CIPP/E, CIPM, FIP

In 2022, in its long-awaited judgment, the Supreme Administrative Court of Lithuania found that a regional news portal did not violate the GDPR when processing the personal data of a local businessman in a publication alleging corrupt public procurement practices. Although the judgment clarified some aspects of the application of a legitimate interests assessment to media publications, likely, the national debate on the values attributed to data protection and transparency will continue into 2023.

The latter is particularly true since, in late 2022, the CJEU issued a landmark judgment in the case of OT v Vyriausioji tarnybinės etikos komisija, where it found a requirement under the Lithuanian law to publish online detailed private interest declarations of public officials incompatible with data minimization, necessity and proportionality principles. The authorities will need to look for new ways of reconciling the important legitimate interest in combatting corruption with the data protection law guarantees.

This year, Parliament is likely to vote on the liberalization of data protection rules related to the background checks of prospective employees, as proposed by the Ministry of Justice late last year. Other important tasks on the legislature's to-do list are likely to include the deliberation of proposals to harmonize the national legal framework with the recently adopted EU's Digital Agenda rules, including the Digital Services Act and the Digital Markets Act.

From the enforcement perspective, during the first half of 2022, the State Data Protection Inspectorate recorded 137 personal data breaches affecting over 400,000 individuals. In this regard, the regulator launched a number of significant investigations, including against an online marketplace, the Lithuanian Innovation Agency and a financial services company. It is expected that these investigations will conclude in 2023, potentially providing data controllers with new insights and lessons learned regarding the prevention and management of data breaches.

Luxembourg

Vincent Wellens

Yoann E. A. Le Bihan, CIPP/E

With the clear intention of becoming a pioneer in the field of certification under GDPR Article 42, Luxembourg's DPA, the National Commission for Data Protection, adopted the first certification mechanism under the GDPR and officially accredited the first certification body. Quite naturally, we expect some significant news this year regarding certification in Luxembourg, where some big players already expressed an interest in the new scheme or schemes from other DPAs.

For a second year in a row, the annual report of the CNPD mentions that some data controllers in the fields of banking and insurance are underrepresented in data breach notifications. Even though the global pandemic may have shifted the priorities of the DPA for some time, we believe the current return to normal might be the occasion for the CNPD to investigate those statistical anomalies, leading to further enforcement. This is on top of remodeling and strengthening existing industry-specific compliance frameworks (such as Circular CSSF 22/806, DORA and the

NIS 2 Directive) and could lead to a very busy 2023 for bankers and insurers.

Despite the publication of its guidelines on cookies and trackers in 2021, the CNPD has not published any decisions resulting from audits of online tracking practices by data controllers. At a time when many other DPAs are publishing decisions regarding Google Analytics not in compliance with the GDPR, the CNPD might choose to focus more on cookies and trackers. Furthermore, it is actively investigating the compliance with GDPR transparency (and information) requirements in the e-commerce sector. The findings of these investigations may lead to the need for many actors in the e-commerce sector and beyond to rethink their data protection notices.

Last but not least, with the deadline for implementation of the new standard contractual clauses Dec. 27, 2022, we would not be surprised to see old standard contractual clauses mentioned as an additional finding in audit reports in 2023. Of course, 2023 will be a decisive year to see whether the Biden administration's executive order will be sufficient as a basis for the European Commission's next adequacy decision that would replace the EU-US Privacy Shield.

🇲🇽 Mexico

Gabriela Espinosa Cantu, CIPP/US, CIPM

While several countries around the world continue passing privacy laws that mirror the EU GDPR, there is still not such a clear effort to do the same in Mexico. Several initiatives were presented to Congress in 2022 to amend the Mexican Federal Data Protection Law Held by Private Parties, targeting particular requirements, but no comprehensive bill has been discussed nor drafted to enhance privacy and data protection standards.

Current drafts address — separately — privacy-by-design and by-default requirements, the relevance to include biometric information within the sensitive data definition, or the possibility for affected individuals to receive monetary compensation by the infringing controller that failed to grant their data protection. None of these initiatives has had any significant movement.

Congress and public authorities have shown more interest in regulating cybersecurity after a significant hacking of Mexican Defense Ministry information that released millions of documents last September. The bill — which at the time of the writing of this article has not been passed yet — includes the creation of a cybersecurity authority, the definition of cybercrimes and fundamentals for defining authorities' jurisdiction, and enforcement actions. Both chambers in Congress are aligned in urgency to specifically regulate cybersecurity where they want to protect digital activity and information held by public authorities for national security, as well as prevent security breaches of confidential information.

Even though the Mexican data protection laws and regulations are based on several fair information privacy practices or principles, they are waiting a long-overdue update to catch up with the digital age. The Senate is still pending to define two missing commissioners from the national DPA. Current spotlight and interest on the cybersecurity law could be just the push both pending activities need.

🇳🇿 New Zealand

Daimhin Warner

2022 was an exciting year of complementary developments, helping New Zealand regain its position at the forefront of future-proofed

privacy regulation. Several developments were commenced but not completed, which means that 2023 will continue this theme.

At the end of 2021, the government signaled that a bill implementing a new consumer data right would to be introduced to Parliament in 2022. This has not yet occurred, likely overshadowed by other legislative priorities, but could be expected next year. This will be New Zealand's version of the data portability right. Readiness work has already begun in the banking and financial technology sectors in anticipation of the law's eventual implementation.

A decision on the regulation of facial recognition and other biometric technologies is likely to be high on the agenda of New Zealand's DPA, the Office of the Privacy Commissioner. This would come following the August 2022 release of a consultation paper seeking views on what action may be needed to address the increasing use of biometric technology in New Zealand. Whatever regulatory response is favored, the OPC has made clear it will seek to preserve the benefits of the technology while protecting against privacy risks and ensure the compliance burden is proportionate to the scale of the risk.

We should also see action on the Ministry of Justice's proposal to broaden the Privacy Act's notification requirements. Currently, there is no requirement for agencies to provide privacy notice to individuals when collecting personal information about them indirectly (that is, from other sources). Submissions — such as those made by the privacy commissioner — appear to favor an amendment to existing information privacy principle 3, rather than the insertion of a new privacy principle.

Finally, taking a cue from the commissioner's public comments, we can expect to see a continuation of the commissioner's engagement with the "privacy ecosystem" — including policymakers, organizations, nongovernmental organizations, industry groups and privacy professionals — to deliver privacy guidance and resources more efficiently.

Nigeria

Oluwagbeminiyi Ojedokun, CIPP/E, CIPM
Ridwan Oloyede, CIPP/E, CIPM, FIP
Dorcas Tsebee

The data protection landscape in Nigeria had another remarkable year. After previous failed attempts, a renewed effort was made in 2022 for another data protection bill. The Minister of Communication and Digital Economy announced in February that the president approved the establishment of the Nigeria Data Protection Bureau to replace the National Information Technology Development Agency.

In 2022, the government introduced a new data protection bill. We expect this bill to pass early 2023, as the Senate promised to do so within 30 days of its introduction. The bill is expected to be signed into law in the first or second quarter of 2023. The enactment of the law will ensure the complete transition and formal establishment of the NDPB as the country's DPA because it has been operating without an establishing law since February 2022. At the state level, the Lagos State Data Protection Bill is expected to pass and signed into law. We also anticipate some progress with Ogun State's own bill.

We anticipate more sector-specific guidance and regulations that will either directly address or impact data protection coming from multiple federal bodies: the Securities and Exchange Commission, the Nigeria Insurance Commission, the Federal Competition and Consumer Protection Commission, and the Central Bank of Nigeria.

The Nigeria Communication Commission is also expected to release an amendment to the Registration of Telecommunications Subscribers Regulation, which opened for public comment in 2022. We anticipate significant progress on some pending legislative proposals, such as the Electronic Transactions Bill and the National Electronic Health Record Bill. Finally, we anticipate that the proposed amendment to the Cybercrimes Act will be presented before the end of the current legislative cycle.

Norway

Martha Ingves

The Norwegian Intelligence Service Act, which would allow the intelligence service to access any information that has crossed the Norwegian border by digital means, is expected to be a hot topic in 2023. This act, which was adopted in 2020 but since then only partially implemented, has raised concerns amongst privacy experts and advocates. It is likely to trigger further debate and possible legislative proposals from the Norwegian government.

In September 2022, the Privacy Commission, a consultative body appointed by the Norwegian government, published their report on the state of privacy in Norway. The report, which is intended to lay the foundation for future legislative and policy initiatives, identified several areas that raise privacy concerns, especially in connection with the digitalization in the public sector and processing of children's data. The commission suggested, amongst other things, to further regulate and supervise the use of digital tools in the education sector, as well as focus more on the need for better competence in privacy within municipalities and schools.

The commission also highlighted that further regulation on online tracking is necessary and found cookie banners to be an insufficient tool to protect users' privacy online. However, there was disagreement within the commission regarding online behavioral advertising, with some members suggesting that the government should consider introducing a general ban on such practice, whereas others called for a more nuanced approach.

While action from the Norwegian government following the commission's report will likely span over several years, the first follow-up initiatives are likely to take place in 2023.

Finally, the sandbox for responsible AI that Norway's DPA, Datatilsynet, started as a trial project in 2020 has been granted a permanent budget by the Norwegian government. Therefore, the sandbox will soon be transformed into a more structured program. This is a clear sign that AI and digitalization as well as data privacy are high priorities at a governmental level in Norway.

Paraguay

Cecilia Abente

2023 will likely be an interesting year for data protection in Paraguay. Legislative discussions are expected to occur on the comprehensive data protection bill submitted to Congress May 2021.

The bill's content mainly follows the provisions of the EU GDPR and the Ibero-American Data Protection Standards. It creates a complete data protection framework including principles, data subjects' rights, controllers and processors' obligations, international transfers, supervisory authority roles and other issues related to data processing.

The bill is still being discussed in its chamber of origin, the Deputy Chambers, and is expected to have amendments proposed by the Constitutional Affairs Commission, which

is one of the seven commissions assigned to study the content of the proposed law.

One of the most controversial points of the bill could be the creation of a new and independent authority as it was proposed in the original bill. It is very likely that the functions of the authority in charge would be allocated to an existing public entity.

In late 2020, the Credit Data Protection Law entered into effect, and it is currently the only data protection law in force in the country. Its reglementary decree should be issued sometime this year. Nevertheless, this will not replace a comprehensive law.

Additionally, it is possible that specific legislation involving personal data such as electronic health records and mandatory storage of traffic data to combat child pornography and related punishable acts may be in put on to the parliamentary agenda.

Peru

Catherine Escobedo Paredes

The most important lesson 2022 left for Peru in terms of personal data protection is that it urgently needs to update its legislation and policies, particularly regarding cybersecurity.

Following multiple cybersecurity incidents in 2022, it is imperative Peru approves its National Cybersecurity Policy as a priority for 2023 and allocates enough budget for its implementation and dissemination. The Secretariat of Government and Digital Transformation announced it is working on this, so we may expect a first draft soon.

Other pending laws and regulations that will ensure better handling of the personal information kept by the government include the long-awaited approval of the Cybersecurity Law, which received some observations from the Executive Branch back in 2019 and has yet to be revisited by Congress. Also pending is the drafting of both the regulations of the Cyber Defense law (Law No. 30999) and the regulations of the Digital Trust Framework (Urgent Decree No. 007-2020) which — among other things — will clarify the timeframe and procedures for reporting data breaches and personal data security incidents.

On the other hand, the legislative agenda for 2023 includes two proposals for the modification of the Digital Trust Framework to strengthen the National Digital Security Center and promote the creation of a National Cybersecurity Council.

Finally, we should expect either a modification to the current Data Protection Law or the issuing of special directives on the use of cookies (most likely the latter) since the only special guidance on the subject currently is an advisory opinion that Peru's DPA, the National Authority for the Protection of Personal Data, issued early 2022. It has been disclosed that the ANPD is supervising the use of cookies on different websites and imposing fines if they find the websites fail to obtain the consent of the data subject for the treatment of their personal data when using marketing cookies.

Philippines

Irish Krystle Almeida, CIPM

The Philippines' DPA, the National Privacy Commission, underwent major organizational changes in the past year, starting with the appointment of Deputy Commissioner John Naga as the new privacy commissioner. He succeeded Privacy Commissioner Raymund Liboro and is joined by newly appointed Deputy Commissioner Nerissa de Jesus and Deputy Privacy Commissioner Leandro Aguirre.

The commission is anticipated to focus on heightened enforcement of the Philippines' privacy law, the Data Privacy Act. We may begin to see administrative fines in line with NPC Circular No. 2022-01. Under this circular, personal information controllers and personal information processors may face fines ranging from 0.5% to 3% of their annual gross income for grave infractions and 0.25% to 2% for major infractions. This, on top of criminal penalties including imprisonment — already provided by the privacy law — is geared toward increasing organizational accountability and enhancing overall compliance. Privacy Commissioner Naga stated: "We hope that PICs and PIPs would not view the administrative fines as adversarial, but as a motivation to protect and safeguard the personal data they collect and process."

The proliferation of targeted spam and scam texts bearing mobile subscribers' names also took center stage in 2022. In response to these criminal schemes to defraud Filipinos reeling from the effects of the pandemic, the commission convened technical working group sessions to determine how the government and private sector, particularly telecommunications companies, can work together to better protect the public.

We may see significant improvements in this space with the passage of the SIM Registration Act. The requirement of providing personal details, including a government-issued ID, for the purpose of identity verification prior to mobile SIM card activation may prove to deter fraud actors and cybercriminals who could no longer hide behind the veil of anonymity.

🇵🇹 Portugal

João Lamim, CIPP/E, CIPM

In 2022, Portugal saw a new directive from its DPA, the National Data Protection Commission, on direct marketing electronic communications (Directive 01/2022). In June 2022, the CNPD ordered telecommunications providers to eliminate data retained under Law 32/2008 after the Constitutional Court issued its ruling 268/2022 April 19, 2022, declaring some of its rules unconstitutional following the Digital Rights Ireland case.

There are some legislative initiatives in Portugal's Parliament, the Assembly of the Republic, that should be on privacy professionals' radars.

- Bills 70/XV, 79/XV 100/XV, to amend Law No. 32/2008 on conserving metadata in electronic communications. The CNPD warns of the risk of generalized storage of personal traffic data — that is, data relating to almost the entire population — revealing the identities of individuals that others communicated with electronically, contrary to Judgment No. 268/2022 from the Constitutional Court recommending some changes to the project.
- Bill 11/XV aims to regulate access to metadata relating to electronic communications for criminal investigation, with the risk, according to the CNPD, of a disproportionate restriction of fundamental rights to privacy, informational self-determination and freedom of personality development.
- Regarding Draft Law 19/XV, which changes the legal regime for the entry, stay, departure and removal of foreigners in the national territory, the CNPD considers that some provisions are too vague and need clarification, such as the processing of biometric data for the identification of foreigners.
- Bill 347/XV reinforces the protection of victims of crimes of nonconsensual dissemination of intimate content, amending the Penal Code and Decree-Law No. Internal and Processing of Personal Data.

Romania

Adriana Neagu, CIPP/E, CIPM, FIP

We cannot expect any new data protection regulations for 2023. However, there are other laws and projects with impact on data protection such as the whistleblower law, the law on cybersecurity and defense, and the governmental cloud.

As expected, the whistleblower law is meant to facilitate reports regarding violations of the law within private entities, public authorities, institutions or other legal entities under public law. It transposes the EU Whistleblower Directive adopted in 2019 after Romania failed to meet the directive implementation deadline in 2021. The initial draft law approved by Parliament was sent back by the president for new discussion as certain elements raised public discord, such as requiring anonymous whistleblowers to provide their data. Likewise, concerns were also raised over the Recovery and Resilience Plan. Private companies with more than 50 employees must have set up an internal communication channel and placed proper procedures by Jan. 1 of this year.

The draft law on cybersecurity and cyber defense of Romania was made public. The draft mandates legal entities responsible for networks or systems owned by public or private entities and used by authorities or institutions to notify any cybersecurity incident within 24 hours of becoming aware of it. As these legal entities are also subject to the GDPR and most of these incidents affect personal data, the deadline for reporting cyber incidents might indirectly apply to reporting data breaches as it becomes clear that they will be aware of the incident once reported under this draft law.

Another project raising public debate is the governmental cloud. This project will take some years to be implemented, though the main decisions have passed. The authorities promise the platform will allow citizens to access their own data. This will be a big step for Romania and for the digital transformation, though how this will be implemented remains to be seen.

Saudi Arabia

Ben Crew, CIPP/E

In Saudi Arabia, the latest draft of the Personal Data Protection Law includes significant changes that have been set forward by the Saudi Data and Artificial Intelligence Authority for consultation. These changes include the addition of data portability into the data subject access rights, relaxation of data transfer restrictions, clarifications of rules for certain types of data such as health data and the removal of certain criminal offences. Additionally, it now includes a legitimate business interest basis for legal processing, which is a fundamental change.

The changes also introduce a requirement for organizations to provide an opt-out from the use of personal data for marketing and prohibit the use of sensitive data for marketing purposes.

Comments were open through Dec. 20, 2022. Similar to the United Arab Emirates, executive regulations are likely to come forward in the first several months of 2023, with the enforcement date beginning 12 months after. Overall, this is a positive move by the authorities to engage in wider discussion about data protection requirements and ensure the final legislation strikes a fair balance between protecting sensitive information without hindering business progress.

Serbia

Petar Mijatović

In March 2022, Serbia's DPA, the Commissioner for Information of Public

Importance and Personal Data Protection, adopted its official yearly report. 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 main 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 LPDP are also an impediment.

During 2022, the Working Group of the Government of the Republic of Serbia worked on the preparation of the new Data Protection Strategy with an Action Plan.

It is expected that the most important priority of the new Data Protection Strategy in 2023 will be adoption — or at least initiation of procedures for adoption — of the amendments and supplements of the LDPD. These will mitigate the normative flaws concerning the provisions that echo the EU's Law Enforcement Directive by putting these provisions in a separate law or section of the LPDP and also introduce the provisions on processing personal data through video surveillance.

Singapore

Pranav Rai

Over the past few years, Singapore has made significant changes to its Personal Data Protection Law to better protect consumers and keep pace with technological and business developments.

Following the first comprehensive review of the PDPA, Singapore introduced these changes by a PDPA amendment in 2020 and is implementing them in batches. The first (2021) batch of amendments expanded the scope of the PDPA to include personal data processors on behalf of public agencies, gave the DPA more authority, strengthened controls on spam, introduced a mandatory breach notification system, and allowed certain organizations to use personal data without consent for purposes such as understanding customer behavior, subject to certain conditions. The second (2022) batch increased the penalties for violating the PDPA and imposed penalties on certain new classes of organizations. Maximum penalties — which were SGD 1 million earlier — can be up to 10% or 5% of the breaching organization's annual turnover in Singapore if the annual turnover exceeds SGD 10 million or SGD 20 million, respectively.

In 2023 we can expect the commencement of the third (and final) batch of changes: data portability provisions. While already one of the fundamental data subject rights in the GDPR, the data portability provisions will be new to the PDPA. Singapore's rationale for their incorporation is to provide individuals with greater autonomy over their personal data as well as help the innovative and more intensive use of applicable data in the possession or control of organizations — for example, to support the development of services provided by them. More in tune with the latter rationale and expectedly wider than in the GDPR, the data portability right will also have a list of exceptions and restrictions, such as situations where transmission is contrary to national interest.

South Africa

Nerushka Bowan, CIPP/E
Gilad Katzav

The end of 2022 marks approximately a year and a half since the Protection of Personal Information Act came into effect in South Africa. The POPIA's implementation has been slow, staggered and — encouragingly — steadfast.

As anticipated, the Information Regulator has spent most of 2022 gradually operationalizing the POPIA's legislative framework. This includes approving banking and credit reporting Code of Conducts, publishing several guidance notes and prescribed forms, implementing an online registration platform for DPOs and establishing the Enforcement Committee. The IR also issued media statements relating to processing activities of public bodies, investigated various reported data breaches, and hosted and spoke at a number of public events and engagement forums.

In 2023, we expect the IR to continue to play an active role and further operationalize. We anticipate that the IR will initiate investigations into allegations or complaints of unlawful data processing as well as referring such matters to the Enforcement Committee for further consideration. It is feasible that we may see the first fine or penalty imposed under the POPIA for unlawful data processing practices in 2023.

Whilst we have seen a handful of POPIA-related cases come through the courts, there are still many aspects of the POPIA that are yet to be authoritatively interpreted. It remains a concern that the EU Commission has not determined whether South Africa provides an adequate level of protection relative to the GDPR. Similarly, the IR has also not made any determinations regarding the GDPR's adequacy status in comparison to the POPIA. Given that juristic persons may be considered data subjects under the POPIA, further guidance for cross-border data transfers would be welcome. We are hopeful that this issue will be dealt with this year as such recognition or guidance is necessary for the free flow of information between South Africa, the EU and the GDPR-approved nations.

🇪🇸 Spain

Joanna Rozanska, CIPP/E, CIPP/US

This year we can expect to see the introduction of the (overdue) Spanish law implementing the EU Whistleblower Directive. The current draft of the referred law states that any and all entities obliged to implement a whistleblowing scheme by having at least 50 employees shall appoint a DPO, which will considerably broaden the scope of such an obligation in Spain.

Let´s also bet on the upcoming appointment of the new director of Spain's DPA, the Agencia Española de Protección de Datos. This is expected within the coming months, which may bring new developments in the institution's strategy.

In addition, the AEPD is negotiating a code of conduct with the financial and telecommunications industries, which will serve to promote, enhance and reinforce mediation to resolve complaints. In general terms, the idea is that, when a complaint arrives, it will be referred to the supervisory body of this code of conduct, which will coordinate with the financial or the telecommunication entity concerned, which, in turn, will refer it to the DPO.

The focus on disruptive technologies is steadily increasing in Spain and will likely continue in 2023. Following this tendency, the AEPD is likely to publish some new guidelines on the interplay between data protection and such technologies, with a special focus on artificial intelligence and the use of biometric technologies.

Finally, the AEPD may comment on some new European regulations that entered into force recently or will do so throughout the 2023 with an impact on data protection, such as the Digital Services Act, Digital Markets Act or Data Governance Act.

Sweden

Sofia Edvardsen, CIPP/E

At the Swedish Parliament's opening in October, a new liberal-conservative government took office. The new government renewed focus on communications and security. For the first time, the government appointed a national security advisor. Sweden is continuing its application process to become a NATO member, with possible final acceptance during 2023.

Also notable is that Sweden has the EU presidency from Jan. 1 to June 30. The finalization of the ePrivacy Regulation is expected to be on the agenda.

Upcoming legislation for next year includes extended possibilities for data surveillance to prevent crimes. Additionally, Swedish platform operators must provide information to tax authorities about the income of the platform users when selling goods or services. The existing legislation on data protection was found sufficient and did not need any changes.

In April 2022, the EU Commission criticized Sweden, saying it failed to fulfil its "obligations as regards the right to effective judicial remedy for data subjects in certain cases" and failed to "transpose and communicate to the Commission how national measures transpose the EU Electronic Communications Code."

Sweden's DPA, Integritetsskyddsmyndigheten, has been quite busy the past year with initiating enforcement actions and guidance.

At the beginning of November 2022, IMY had 143 ongoing investigations — a slight decrease compared to 2021. The oldest ongoing investigation is from June 2019. Hopefully, an increased budget will improve the statistics and lead to more decisions.

IMY initiated the supervision of several internet-based pharmacy companies and their use of the Facebook pixel and ancillary services from Meta. Since it potentially concerns the sharing of sensitive personal data (health information), future supervision decisions are crucial in using the Facebook pixel and processing sensitive personal data.

Switzerland

Stéphane Droxler, CIPP/E, CIPM

The new Federal Data Protection Act will finally come into force Sept. 1. Formally approved in September 2020, it will have taken three years to deliver its implementing ordinance. It should be noted, however, that this new law will be immediately and fully applicable, such that there will be no delay for data controllers and their processors to adapt. On the other hand, it will not have a retroactive effect either, which means that the application of certain clauses (for example, the obligation to carry out data privacy impact assessments or to implement privacy-by-design measures) will not concern processing initiated under the current law.

The question of the renewal of the adequacy status by the EU currently remains open. If the main lines of this new FDPA undoubtedly tend toward a rapprochement with the requirements of the GDPR, its lack of ambition is regrettable. This is particularly true regarding the weak reinforcement of the powers of the supervisory authority as well as the absence of administrative sanctions, which would certainly have been more dissuasive than hypothetical criminal measures against individuals who will be difficult to track down in practice.

It will therefore be interesting to see what extent organizations that would not already

comply with GDPR requirements for commercial or extraterritoriality reasons will mobilize to adapt their security and compliance measures.

Thailand

Rubkwan Choldumrongkul
Yulia Askhadulina, CIPP/E

On Jan. 18, 2022, Thailand's DPA, the Personal Data Protection Committee, consisting of the chairperson and the nine honorary commissioners, was formed and as of June 1, 2022, Thailand's first comprehensive Personal Data Protection Act fully went into effect.

In 2022, the PDPC issued eight subordinated regulations clarifying the requirements set under the PDPA. Among them are regulations addressing the administration of the new law by the PDPC, the appointment of the Expert Committee, and framework for the determination and enforcement of the administrative sanction by the Expert Committee. Notifications on security measures for the data controllers, rules governing records of processing activities for the data processor and corresponding subject matter expert exemptions were published.

In 2023, we expect the PDPC to finalize the public consultation process that began in 2021 and issue group one subordinated regulations addressing some of the pressing practical issues. The PDPC has already published the guidelines for obtaining consent and notifying purposes for personal data collection. In the pipeline are the regulations addressing the role and qualifications of DPOs, cross-border data transfers and binding corporate rules.

Before the adoption of the comprehensive data protection law, the sectorial approach in addressing privacy issues proved to be effective in Thailand. The Thai Bankers' Association set forth procedures and standards pertaining to data protection and privacy for the banking and financial sectors. We expect other data-heavy industries will follow suit, and there will be more sectoral guidelines and regulations designed in consultation with the private sector in the upcoming year.

To date, it appears there were no fines issued or formal cases filed. However, throughout 2022, the PDPC conducted activities to raise awareness, enhance knowledge and address common misconceptions to ease the fear of the new data protection framework. As a result of these campaigns, we anticipate that the general public and private sectors will become more informed of their rights and corresponding obligations and cases will be brought to the attention of the recently established Expert Committee and precedents will then be established.

Turkey

Furkan Güven Taştan

2022 witnessed quite interesting developments through the legislator on information technology-related issues. Various regulations on digital services, disinformation and social media platforms were enacted this year thanks to the determination of the Turkish legislator throwing their hats into the ring for IT law issues. Unfortunately for data protection issues, the prospective reform agenda stipulated by the presidency's policy documents has yet to be achieved. Thus, the goals set by these documents are still on the table for 2023.

The reform agenda consists of two legislation packages regarding the Turkish Data Protection Act. The first and prioritized package deals with the means for transfers of personal data abroad and conditions for the processing of special categories of personal data. Provided means for the transfers in

the act in force will possibly be extended with novel appropriate safeguards such as binding corporate rules, codes of conduct and approved certifications. Moreover, this package also includes the readjusting of the conditions for the processing of special categories of personal data that are currently proving a challenge for the business world in Turkey. This part of the package especially is prioritized by the Turkish government and will most likely be enacted in the first quarter of this year.

As for the remaining part of the reform agenda, Turkey plans to change the whole act in harmony with the GDPR. The core of these changes will likely include a risk-based approach and the accountability principle. The scientific committee formed by the Ministry of Justice has prepared the first draft of the package. However, general elections for Parliament and the presidency in 2023 might upstage data protection policy improvement efforts. So, it will be enthusing to monitor whether the whole reform package will be prioritized after the general election.

Ukraine

Dmytro Korshynskyi, CIPP/E, CIPM, FIP

With its official recognition as a European Union Candidate, Ukraine will further implement changes into the legislation. However, Ukraine is still repelling the Russian Federation's full-fledged invasion, so a law on personal data protection unfortunately may not be the top priority for lawmakers. Ukrainian Parliament, the Verkhovna Rada, has failed to enact the law already twice this year due to the fact that MPs weren't able to reach enough votes. It is unlikely that such a law will be passed before the end of the war since complying with it will put a rather heavy burden on Ukrainian businesses, which are currently facing other difficulties brought by the war.

Moreover, according to the new law, there must be a dedicated DPA, the creation of which is rather complicated during martial law. However, once the war is over Ukraine will almost certainly pass a GDPR-like law on personal data protection which will replace the current law that is like the EU's Data Protection Directive. Since the current law is familiar with most data protection concepts such as controller and processor, principles of data protection, legal basis and data subject's rights, the new law will further elaborate on GDPR novelties such as data protection-by-design and by-default, the need to conduct DPIAs, expand data subject's rights and more. As mentioned above it will also introduce a dedicated DPA and increase the responsibility of the data controllers.

United Arab Emirates

Benjamin Crew, CIPP/E

In 2021, the United Arab Emirates published the Personal Data Protection Law, which was scheduled to become applicable in 2022. That has now been delayed, however. We believe that the executive regulations required to support the implementation of the PDPL will happen in early 2023, with an enforcement date likely to be towards the end of 2023 or early 2024. In addition to the PDPL, there are a plethora of other laws pending enforcement dates at both a federal and freezone level covering artificial intelligence, cryptocurrency and adtech that are likely to come into force in 2023.

In addition to the new laws, the existing Abu Dhabi Global Market and Dubai International Financial Centre data protection laws are consistently being updated and improved.

In the case of the DIFC, a possible adequacy decision with the U.K. is on the near horizon. The ADGM is also seeking to attain an adequacy decision with the U.K.; however, this is more likely to come to fruition in 2024 or 2025, not 2023.

Aside from the new and changed laws, there are a number of external factors impacting all companies in the region. In 2022, there was a significant rise in data breaches among companies in the UAE, and that trend is not expected to diminish in the coming year. If anything, companies in the UAE are likely to struggle more with data protection and data privacy compliance in 2023.

The Financial Action Task Force listing 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. This includes ensuring how companies actually handle their data and manage know-your-customer requirements. It's important to note that the increased focus on compliance by global regulatory authorities is not just limited to KYC and anti-money laundering activities. Organizations must expect and prepare for more in-depth, substantive investigations and fines for noncompliance with local, federal and sectoral laws, especially those that govern data privacy.

United Kingdom

John Bowman, CIPP/E, CIPM, FIP

Since the United Kingdom left the European Union in January 2020, a stream of initiatives has emerged from the U.K. government as it steers a distinctive course in data protection in the post-Brexit era. Following a public consultation on the U.K.'s data protection regime, in July 2022 the government introduced to the House of Commons the Data Protection and Digital Information Bill, which included reforms to the U.K. General Data Protection Regulation and Data Protection Act 2018.

These reforms include transferring the role of the information commissioner to a new information commission with an obligation to take into account economic growth and deregulation issues in carrying out its role. The reforms would also enable the U.K. government to make its own adequacy determinations, introduce standard data protection clauses and determine derogations where they support the public interest.

With regards to data exporters making their own assessments of third countries, the proposed test is whether the standard of data protection in the recipient country would not be materially lower than that in the U.K. For data controllers, some changes to the accountability regime were proposed, including the easing of specific obligations to compile a record of processing activities, conduct data protection impact assessments and appoint DPOs.

The most recent statement from the government on the state of play of the bill was issued in September. This confirmed that the second reading of the bill in Parliament would not take place to allow ministers to consider the bill further. Therefore, now in 2023, privacy professionals will want to maintain a watching brief on the passage of the bill and in particular if — and in what form — it returns for a second reading in Parliament.

Another development to follow this year is a planned government white paper and public consultation on the U.K. National AI Strategy. Questions under consideration may include whether the proposed framework adequately addresses prioritized AI-specific risks; the roles, powers, remits and capabilities of regulators for AI; and how this should be delivered across the range of regulators (statutory and non-statutory).

United States federal law

Joe Duball

Action toward U.S. privacy can be viewed in two ways entering 2023. The optimistic outlook is that the work on the proposed American Data Privacy and Protection Act will ultimately carry over to 2023. On the opposite end, watching Congress rehash the same old issues — private right of action, preemption, etc. — without arriving at a solution could mean we're further away from passing legislation than the strides made in ADPPA negotiations indicate.

The new year brings a new structure to Congress, where Republicans flipped the House and Democrats retained the Senate. The differences between chambers will ultimately be what decides the fate of federal privacy this year.

House Republicans said Big Tech regulation, including privacy, will be a priority they'll focus on with the majority. It wouldn't be surprising to see the ADPPA or a similar bill finally be brought to a floor vote by Republicans and passed out of the House with bipartisan support. But then there's the Senate, where Democrats remain focused on getting a complete bill — stronger consumer redress, protections for women's reproductive health as some of the specific asks — while showing little willingness to compromise.

On the state front, comprehensive laws in California, Colorado, Utah and Virginia are online or will come online at different points in 2023. Compliance with those laws will be the focus, but it's easy to overlook the states that may have appetite to pass laws of their own. Massachusetts, Michigan and Minnesota are states with prior Democrat-backed privacy bills and have Democratic control of the legislative chambers, governorship and attorney general's office in the upcoming year.

We're likely to see less than a handful of states pass comprehensive privacy legislation, following the trend we've seen in recent years. Depending on the substance of those potential bills, U.S. Congress may be compelled to put aside its differences and reach long-awaited federal legislation.

United States Federal Trade Commission

Cobun Zweifel-Keegan, CIPP/US, CIPM

Under the leadership of Chair Lina Khan, the U.S. Federal Trade Commission continues its role as an active enforcer of privacy and data security standards while also laying the foundation for future rulemaking activities. Currently down one of five commissioners, the FTC should soon see a Republican nominee to return to full strength. With or without this voice, the agency will continue advancing matters in the consumer protection sphere.

Expect to see a quickening pace of one-off privacy enforcement actions now that this FTC has hit its stride. New cases are likely to highlight issues in vogue among U.S. privacy wonks, including data minimization and the protection of sensitive data such as health, location and children's data.

On the rulemaking front, the FTC will finish the work of reviewing and analyzing the thousands of public comments it received in response to its Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security. If the agency determines that the record supports the creation of a new trade regulation rule, it will take the next step in this lengthy administrative process. The next iteration, a formal Notice of Proposed Rulemaking, will be significantly narrower and more targeted than the ANPR. Based on the record of public comments and its own

evidence, the agency will propose a rule to address privacy practices that are widespread in the industry but harmful and unavoidable for reasonable consumers. Such a proposed rule could address issues like reasonable data security, data subject access rights or unexpected secondary uses of personal data.

🇺🇸 United States health care

Kirk Nahra, CIPP/US

Health care privacy has become a hot topic once again — and we expect meaningful developments in the legislative, regulatory and enforcement areas in 2023.

There are two main regulatory issues to focus on. First, the Biden administration is in the middle of a rulemaking process — initiated by the last administration in its last days — focusing on the potential for expanded information-sharing in connection with both social determinants of health and opioid-related situations. These issues are complicated, with certain heath care goals conflicting with privacy interests. Second, as a result of the Dobbs decision, the administration is also looking for ways to enhance privacy protections for reproductive rights information, including evaluating whether there can be changes to the Health Insurance Portability and Accountability Act privacy rule to better protect this information.

The agency tasked with primary responsibility for these issues — the Department of Health and Human Services Office for Civil Rights — continues to face its own challenges. Aggressive enforcement will likely continue in relation to HIPAA access cases, with more than two dozen cases brought in the past few years. At the same time, other enforcement has slowed somewhat, due in part to fallout from the controversial M.D. Anderson decision in the Fifth Circuit, which imposed new restrictions on the OCR's enforcement approach. The OCR also is part of a broader effort to review data collection activities on health care provider websites — evaluating whether use of common web analytics tools create privacy concerns.

Beyond HIPAA issues, health care privacy increasingly involves laws and regulations other than HIPAA. The Dobbs decision has placed a renewed emphasis on data collection activities — even for data that does not appear to be "health data" — which will have implications and concerns in connection with reproductive rights information. The Federal Trade Commission — in a wide-reaching new complaint — accused data broker Kochava of unfair data collection practices in connection with location-related data, which can be used to track individuals to reproductive rights or other health care providers. We are watching this case carefully and expect others like it. We expect both the FTC and state attorneys general to continue to look at collection of health data outside of the scope of the HIPAA rules — including from a wide range of mobile apps. These enforcement agencies are examining how data is collected, where it is going, and what consumers know about these issues and their related rights. Companies involved in health care mobile apps — broadly defined — should be thinking about these issues carefully.

On the legislative front, state privacy laws continue (for the most part) to exempt HIPAA-covered entities and business associates, creating a new framework for "non-HIPAA" data driven by these state laws (and thereby cementing the confusion about different rules). The federal legislative efforts may continue this complexity by creating different standards for health information depending on what the entity is, rather than based on the information itself.

Zimbabwe

Kuda Hove

Zimbabwe passed its Cyber and Data Protection Act Dec. 3, 2021, and republished it March 11, 2022, with a correct title. The act is an improvement on the country's previous privacy-focused law, the Access to Information and Protection of Privacy Act, which was repealed in 2020. This meant Zimbabwe had gone for a period of close to two years with no comprehensive privacy legislation.

The Cyber and Data Protection Act is modeled mainly after the EU GDPR. Some of the GDPR influences evident in the Zimbabwean law include outlining the different data protection principles and classifying different types of data including sensitive personal information and biometric data. The act also refers to the automated processing of personal information.

However, there are some concerns with the law that are likely to affect the protection of privacy in Zimbabwe. For example, the law establishes a DPA, but this function is assigned to Zimbabwe's existing telecommunications regulator. This regulator has in the past been accused of lacking independence or transparency. There are also fears that the regulator does not have the capacity to effectively oversee privacy rights in Zimbabwe.

Furthermore, the law calls for DPO appointments, but the DPA is yet to publish guidelines on the minimum requirements or qualifications for DPOs. This may further delay the establishment of data protection policies within Zimbabwean organizations. In other African countries such as Uganda and Kenya, the implementation of their data protection laws was crippled by an indefinite delay to pass the regulations needed to provide guidance on applying the law.

Finally, Zimbabwe heads to elections this year and the new law is likely to be used to target individuals who criticize government. Since the Cyber and Data Protection Act was gazetted, at least three media practitioners have been charged with cybercrimes. None of those charges have led to any convictions, demonstrating the charges are meant to harass media practitioners to silence their dissenting opinions. It is expected that this pattern of harassment through the law will increase as the country draws closer to national elections.

For more privacy-related resources, including legislation trackers, tools, guidance, surveys and in-depth reports, check out the IAPP Resource Center.