# 2022 Global Legislative Predictions

Edited by IAPP Assistant Editor Libby Sweeney

# 2022 Global Legislative Predictions

Edited by IAPP Assistant Editor Libby Sweeney

The urgency to pass or update privacy laws around the world seems to heat up more each year, and 2022 is likely to be a hot one. This year's issue of the IAPP's Global Legislative Predictions is the largest to date since the IAPP began tracking predictions in 2017. Health data has been a center of attention in data privacy laws, another consequence of the COVID-19 pandemic. With the passage of China's Personal Information Protection Law and potential passage of India's Data Protection Bill, an additional one-third of the world's population will be regulated by a data privacy law. While many countries agree data privacy is an important issue to regulate, some countries are seeing the greatest obstacle resides in how best to regulate it.

*Editor's note: While we try to include as many countries as possible, we recognize this is not an all-encompassing list. If you are interested in submitting 2022 predictions for a country not featured on this list, please reach out to lsweeney@iapp.org.*

## Australia

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

This year we can expect to see the introduction of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill and further progress on the Australian government's review of the Privacy Act.

The Online Privacy Bill, released last year as an exposure draft, would enable a binding online privacy code for social media and certain other online platforms. Once passed, the industry has 12 months to develop a code or Australia's data protection authority, the Office of the Australian Information Commissioner, can step in to develop it. The "other measures" in the bill will substantially increase the civil penalties for breaches of the Privacy Act and improve the extraterritorial reach of the Privacy Act to protect the information collected from individuals in Australia, regardless of where the collecting entity is located or incorporated.

In October 2021 the government released a discussion paper containing proposals and options to modernize the Privacy Act. Some proposals and options have been inspired by other jurisdictions such as the EU, including introducing individual rights to object and to erasure. With submissions on the paper closing Jan. 10, the government will now consider the feedback and consult with stakeholders on specific issues before concluding its review report, which it intends to make public after consideration. The release of an exposure draft of Privacy Act amendments will then follow the review report, likely in the second half of 2022 or into 2023.

Organizations should take note of the OAIC's determinations last year regarding the privacy practices of Uber, 7-Eleven and Clearview AI last year as case studies on what to expect from the OAIC on enforcement of the Privacy Act, and what they need to be doing to protect personal information to comply with the Privacy Act.

## 🇧🇪 Belgium

**Diletta De Cicco, CIPP/E,**
**Charles Helleputte, CIPP/E**

2021 highlighted the need to reshape the Belgian Data Protection Authority. The existing setup allowed external members to hold key positions at the DPA and elsewhere. This raised concerns of potential conflicts of interest. Making the headlines throughout the year, it ultimately escalated to the European Commission with the launch of an infringement procedure. On the eve of the Jan. 12 response deadline, Belgium announced changes to strengthen the independence of the DPA's members. A new law is expected this year and will be closely monitored — "Brussels watching Brussels."

Let's also bet on the (upcoming) decision in the Interactive Advertising Bureau Europe, or when a focus on advertising technology consent mechanisms has a knockout effect on the privacy world. IAB Europe, known for its Transparency and Consent Framework, was investigated by its lead DPA. A leaked draft ruling qualifies IAB as a joint controller. This rather unpopular position may impact standard-setters, making them more accountable than they expected.

Speaking of accountability, last year saw the adoption of the EU Cloud Code of Conduct by the Belgian DPA, the first of its kind for cloud service providers. Adhering CSPs commit to strict data protection rules, achieving legal certainty and spreading customer trust. There is more coming on that front, with an addendum being negotiated to allow using the code as a legal transfer mechanism, a pioneer move by Belgium.

As we start 2022, let's hope Belgium finally adopts its (overdue) AI, machine learning and big data plan. It's great to be a country of data centers; it would be even better to be at the heart of innovative uses of data. The AI Act will then be close; the Belgian DPA must be ready to absorb more tasks and hire more experts, as their current contingent of lawyers might not do. And with Brussels being Brussels, 2022 will give us (again) a full EU privacy agenda — Digital Services Act, Digital Markets Act, ePrivacy. Let's be ready!

## 🇧🇲 Bermuda

**Nancy Volesky, CIPP/US**

The last few years could be categorized as an active preparatory period in anticipation of Bermuda's privacy legislation, the Personal Information Protection Act, 2016, being implemented. During this time, Privacy Commissioner Alexander White, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP, was appointed and it heralded the emergence of a professional privacy sector,

including the establishment of a Bermuda IAPP KnowledgeNet Chapter.

The time spent has been well served as the government confirmed 2022 will be a busy year for privacy-related legislation. It looks likely that the PIPA or parts of the PIPA may finally come into force. Overall, major changes to the PIPA are not anticipated, so organizations should do well to continue their preparations for compliance based on the requirements present.

There will, however, be some changes to the PIPA and the 2010 Public Access to Information legislation (Bermuda's approach to Freedom of Information) resulting from a harmonization exercise between the two, as PATI presently provides individuals with access to their personal information the government holds. In addition, we will see amendments to the Electronic Transactions Act, 1999 which contains data protection and privacy elements that must be aligned with the PIPA. The government also announced it will introduce a CyberSecurity Act, which will establish minimum standards for cybersecurity for critical assets.

The privacy commissioner spent the last year issuing guidance and that is expected to accelerate in the new year. With the announcement of Bermuda hosting the Global Privacy Assembly's Summit in 2023 and Bermuda's privacy commissioner sitting on the conference's executive committee, privacy in Bermuda takes on an international focus. Preparations may serve as a catalyst for further privacy initiatives.

## Brazil

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

Last year's hallmarks in data privacy legislation were the start of the effectiveness of sanctions applied by Brazil's DPA, the Autoridade Nacional de Proteção de Dados, which enacted a regulation for its due administrative process, and approval of an amendment to the constitution, including the protection of personal data as a fundamental individual right and establishing that the federal government has exclusive powers to legislate in data protection matters.

With enforcement on the radar and the dawning of awareness that the General Data Protection Law applies to any sector, controllers, processors and data subjects alike realized the LGPD is "for real," triggering moves in the legislative front. Many of them aim to carve out exceptions for certain sectors.

Agribusiness, for example, has been pushing for a sector-specific bill for "agricultural data," which may include personal data, to be processed by "providers of agricultural technologies." Likewise, non-profit sectors are propelling a bill aiming at an exemption of their own. However, none of those bills are on a fast track for approval, which means there will probably be plenty of room for debate if such exceptions will mature into law.

In addition, the ANPD's schedule for 2022 includes the issuance of regulation on data subject rights, the appointment and roles of data protection officers, international data transfers, and lawful basis for data processing activities. Finally, the ANPD has yet to issue a regulation on much-awaited criteria for the calculation of monetary penalties, which were not set forth in the due administrative process regulation.

## Canada

**Shaun Brown**

Quebec privacy law will align more closely with the EU General Data Protection Regulation once the changes under Bill 64

are phased in over the next three years. The inclusion of significant penalties and more resources for enforcement mean businesses should pay close attention to interpretive guidance provided by Quebec's DPA, the Commission d'accès à l'information du Quebec, this year.

Less transformational amendments to federal privacy legislation, introduced in Bill C-11 late 2020, died when the Liberal government called an election last year. The re-elected Liberal government has since indicated updating the law is a "top priority" and that a new bill will be introduced in 2022. Although the bill will be revised in response to criticism of C-11, a major rewrite is unlikely. The federal government also completed a consultation on modernizing the public-sector Privacy Act last year, so 2022 may see publication of concrete proposals for amendments to that act.

In late 2021, British Columbia very quickly passed amendments to its public-sector privacy legislation, notorious for its restrictive data residency requirement for personal information. British Columbia removed the prohibition on storage and access outside of Canada, making cloud-based technologies more accessible to public bodies. Disclosures of personal information outside Canada may still be subject to regulations though, which could be published in the coming year. A special committee convened to review the private-sector Personal Information Protection Act released a report recommending several changes to the law, including mandatory breach reporting and stronger enforcement powers for the Information and Privacy Commissioner. It seems likely that the PIPA will be amended this year to implement at least some of the committee's recommendations.

The Ontario government recently completed a consultation on proposals to develop an Ontario private-sector privacy law. Although 2022 is an election year in Ontario — which could slow down or even derail the process — this is an important development to watch.

## Chile

**Javiera Sepúlveda, Andrea Céspedes, CIPP/E, María José Díaz**

2022 will probably be a year with significant shifts in the local data privacy environment. First, due to substantial changes that will promptly be passed to the consumer protection regulations, the National Consumer Protection Service will become the DPA in Chile, but only in regard to the processing of consumers' personal data. SERNAC will have this role temporarily — as long as such powers are not invested in another authority — until the bill modifying current data protection law is approved. SERNAC has made some pronouncements in connection with the protection of consumers' data (including issuing interpretative opinions) in the preparation of its appointment as DPA.

Additionally, legislative discussion on the bill of law that modifies the privacy protection law is encouraging and moving forward. One of the most debated points of the bill, regarding if the authority in charge should be an autonomous DPA or the existing Council for Transparency, seems to have been resolved in the creation of an autonomous authority as proposed by the government.

In October 2020, two bills of law regarding "neuro-rights and brain activity" were submitted to Congress. The first one, which already has been approved and entered into effect, was a constitutional amendment that aimed to include "neuro-rights" in the catalog of guarantees recognized in the Chilean Political Constitution. The second bill, which is still being discussed in Congress and is expected to be approved in 2022, seeks to give a legal

expression to these constitutional rights, protecting individuals' lives and the physical and psychological integrity in the development of neurosciences, neurotechnologies and their clinical applications.

Thus, we hope there will be actual news for 2022, with major changes for personal data regulation.

## China

**Barbara Li**

2021 was a significant year for data protection legislation in China, marked with the Data Security Law and the Personal Information Protection Law entering into force in September and November, respectively. However, people are waiting eagerly for the implementing rules and guidelines with more practical guidance and references.

On the national level, the Cyberspace Administration of China recently issued the consultation draft of the Administrative Regulations on Network Data Security and the Measures for Security Assessment of Cross-border Data Transfer, both of which are likely to be completed in 2022. The former Regulations provide some clarity on data classification and also impose certain vigorous requirements on companies in terms of data breach response and cybersecurity review for overseas investment, while the latter Measures lay down specific stipulations for the threshold, procedures and timeline for security assessment for cross-border data transfer. In addition, the Information Security Technology - Guideline for Identification of Important Data, the draft of which was published in 2021 for public comments, is expected to be finalized in 2022. This guideline, upon issuance, will provide helpful references for businesses to assess if the data they are handling would fall within the scope of important data and to take proper risk management actions.

Data legislation at the local level is also evolving at a fast pace. In Shenzhen and Shanghai, the cities with dynamic digital economies, local governments are spearheading the formulation of local rules for protecting personal data as well as unlocking the value of data. Both the Shanghai Data Regulations and the Shenzhen Data Regulations came into effect Jan. 1, 2022. With the launch of the Shanghai Data Exchange, Shanghai is exploring cutting-edge technologies and methodologies for creating innovative mechanisms for defining data rights and promoting data transactions.

The PIPL and DSL have significantly increased the penalties for noncompliance. The regulators have been targeting large internet platform companies to crack down on excessive collection of personal data beyond the business necessity and the use of big data and algorithms for discriminating customers. It has been reported that in 2022, Chinese regulators will continue to be active in enforcement actions and financial, transportation, auto, e-commerce, pharmaceutical and health care industries are likely to be targeted sectors.

## Czech Republic

**František Nonnemann, CIPP/E**

We cannot expect any important new rules in privacy and data protection to be adopted in the Czech Republic in 2022. The main reasons are two: Because of general elections in October 2021, there is no legislative plan for the coming years. Main priorities of the new government will likely not lay in the data protection area and there have not been recent discussions on any important topics to be newly regulated.

On the other hand, significant changes in the regulation of online marketing (cookies) and telemarketing became effective Jan. 1. The relevant amendment to the Czech Act on Electronic Communications was adopted by the former national parliament.

For both types of marketing — cookies (and similar tracking tools) and telemarketing — there will be a newly introduced opt-in principle. The previous situation was that the opt-out principle was applicable instead for both categories.

This change means that prior explicit consent is needed for usage or storage of cookies in the user's web, except technically necessary cookies or cookies necessary for providing the service asked by the user. Similarly, telemarketing in both the business-to-business and business-to-consumer sectors will be legally possible only with prior explicit consent of the called party.

## Cyprus

**Maria Raphael, CIPP/E**

Following Cyprus' application in July 2019 for accession to the Schengen Area, the supervisory authorities from the EU along with European Commission experts have been assessing Cyprus' infrastructure. Despite the Schengen Committee adopting a positive report in 2020 regarding the capacity of the Office of the Commissioner of Personal Data Protection to adequately supervise systems and procedures the public authorities needed, the assessment in other areas led to the European Union Home Affairs Commissioner announcing in June 2021 Cyprus was not yet ready to become the newest member of the borderless zone. However, the vice president emphasized that "in the turn of enlargement, Cyprus is clearly coming in the fourth position, and yes, Cyprus remains a candidate for Schengen." While still in the process of joining Schengen, Cyprus needs to harmonize its legislation with the legal instruments of the Schengen Information.

Cyprus, as of 2016, was making efforts to transpose into national law the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union Law (the Whistle-blower Directive), adopted October 2019. The Directive was set to be transposed into law by Dec. 17, 2021. However, this did not occur as there were inconsistencies to be tackled between the bill and a law proposal submitted in 2016 for the protection of public whistleblowers. On Jan. 20, the Plenary Session of the Cyprus Parliament voted for the passing of the national law transposing the Directive, titled "The Protection of Persons who report violations of EU Law and National Law of 2022."

There is imminent need to amend Cyprus Contract Law in order to allow the contracting parties to choose Cyprus law to govern the new standard contractual clauses, adopted by the European Commission in June to legitimize international data transfers. This will be achieved by incorporating provisions that confer third-party beneficiary rights to data subjects into Cyprus Contract Law or data protection legislation, which is a prerequisite for the governing law of the SCCs.

Lastly, it is expected that the Cyprus government will begin developing a legislative framework to ensure the availability of data with transparent regulations on data protection, taking into account the GDPR and the EU Regulation on the free flow of non-personal data, while facilitating the interoperability of data. The new legislative framework will enable digital services to use up-to-date and high-quality information while considering the protection of personal data. The Cyprus government has committed to creating a data ecosystem with guidelines and

regulations about data interoperability and data exchange agreements.

## Denmark

**Karsten Holt, CIPP/E, CIPM, CIPT, FIP**

At the Danish Parliament's opening session in October 2021, the Danish government published its legislation plans for the coming year. Five of the proposed acts have interesting privacy aspects:

- New national legislation governing social media platforms and their responsibility to delete illegal or false content on their platform, including requirements for increased transparency and a right to appeal the social media's decisions to a public body. It will be interesting to see how a national legislation will work with global social media platforms.
- Revision of the rules on telecommunications logging as a tool for criminal investigations.
- Revision on the rules on fingerprint and DNA collection and registration to improve the police's options for criminal investigations.
- New rules on tort claims for victims of digital (online) offences.
- Amendment of the Criminal Act to specifically address identity theft as a criminal offense.

The Danish DPA, Datatilsynet, has been busy the previous year, issuing new guidance material on a number of topics and making decisions in a number of cases, often leading to requests to the police for criminal proceedings and fines. Many of these cases have been related to insufficient security of processing (Article 32).

Since Datatilsynet cannot issue fines by themselves, we are still waiting to see if Danish courts agree to the proposed fines. To this day, only one case has been decided by a Danish court (in first instance), and it led to a reduction of the proposed fine (EUR 200,000) to only EUR 13,500 due to a number of mitigating circumstances. The ruling was appealed by the prosecution, so we still have no final court rulings on GDPR fines in Denmark.

## Finland

**Milla Keller, CIPP/E**

In 2022, we will likely see an update to the Act on the Protection of Privacy in Working Life. Anyone who has worked with employee privacy in the Nordics will have noticed Finland has one of the strictest approaches in this area in all of EU. The update will extend the possibilities to process employee personal data without the employee's consent.

In 2021, Finland updated cookie guidelines. The authority responsible for enforcing the cookie rules had to change its interpretation of the rules due to a ruling from the administrative court. This marked a 180-degree turn for Finnish cookie compliance: Before, the authority maintained its interpretation that it is possible to provide valid consent with browser settings. The new cookie guidelines set one of the strictest standards in the EU. In 2022, we expect to see how enthusiastically the authority intends to enforce the guidelines.

Lastly, European DPAs are cooperating on numerous cases concerning international data transfers following the "Schrems II" ruling, and some Finnish cases are pending the finalization of these cooperation procedures. In 2021, the Finnish Data Protection Ombudsman's Office did not publish any decision or detailed guidelines on the topic. Hopefully 2022 will bring clarity when some

of the cases are finally closed and we have a better idea of the local supervisory authority's approach to international data transfers.

## France

**Cécile Martin**

In 2022, it is highly likely health data will still be at the center of concern for France's DPA, the Commission nationale de l'informatique et des libertés. Indeed, this data, known as sensitive data in European law, has been widely collected and processed by many different data controllers and processors in the current health context to fulfill different purposes, such as access to the workplace for certain professions, allowing establishment of the sanitary pass, monitoring the evolution of the pandemic, establishing vaccination campaigns, deepening research, implementing health protocols for people suffering from COVID-19 and more.

In view of the numerous data breaches that have occurred in this field and the numerous interests this type of data can arouse, the verification of the conformity of the data processing implemented and security measures taken should still give rise to numerous controls by CNIL agents.

Similarly, it is anticipated employee monitoring systems will be subject to increased vigilance by the CNIL. As a result of the pandemic, many employees are now working in a hybrid work environment, with periods of office work and periods of working at home. This requires companies to adapt, since they must allow them to continue carrying out their remote missions under the same conditions as if they were in the office. Therefore, companies must give them access to personal data, such as data on customers, prospects, suppliers or even employees of the organization, under appropriate security conditions, all while controlling their activity (management of working time; respect of health and safety rules during telework; respect of instructions concerning the transfer of personal data of the persons concerned; respect of cybersecurity measures).

## Germany

**Ernst-Oliver Wilhelm, CIPP/E, CIPM, CIPT, FIP**

On Nov. 24, 2021, the formation of a new government in Germany resulted in a joint agreement of the so-called "Traffic-Light Coalition" from Social Democrats, Liberal Democrats and Green Party.

The Coalition Agreement contains commitments of the new government for the next four years, including: strengthen digital citizen rights and IT security, introduce a right to encryption, promote anonymization, establish criminal liability for unlawful deanonymization, support rapid adoption of the ePrivacy Regulation and an ambitious agreement with the U.S. to enable legally robust and compliant data transfers at a European level of protection, and enhance the Federal Data Protection Law, Bundesdatenschutzgesetz. It is very likely that the planned enhancement of the BDSG will take inspiration from an evaluation by the Board of German Supervisory Authorities, Datenschutzkonferenz, released in March 2021, and an evaluation from the Federal Ministry of the Interior (Bundesministerium des Inneren) released in October 2021. There seems to already be consensus in the new government that the institutionalization of the DSK and the refinement of the rules for Employee Data Handling should be part of the enhancement of the BDSG.

On Nov. 25, 2021, the German Federal Protection Act against Infections (Infektionsschutzgesetz) entered into effect. Among other things, this law established the

so-called "3G rule" (named for the German words for vaccinated, recovered and tested negative: geimpft, genesen and getestet) at the workplace and provided a legal ground to process employment health data until March 19, though this can be extended for three months.

On Dec. 1, 2021, the Telecommunication Telemedia Data Protection Act, known as the Telekommunikation-Telemedien-Datenschutz-Gesetz, will enter into effect. The TTDSG contains provisions that, among others, aim to clarify the application of the GDPR and the ePrivacy Directive in telecommunications and telemedia. For example, storage of and access to information in the end user's terminal equipment is generally only permitted with a GDPR-compliant consent; exceptions are defined in accordance with the requirements of the ePrivacy Directive. Furthermore, the TTDSG contains new provisions on digital estate, privacy protection for terminal equipment, consent management and supervision.

On Jan. 1, Article 327q of the German Civil Code, known as the Bürgerliches Gesetzbuch, entered into effect. This article deals with when a consumer provides their personal data for gaining access to some service and will be considered similarly if they had provided money for the service (while maintaining the data subject rights of the consumer). This enhancement of the BGB is considered highly relevant by consumer and privacy protection organizations.

## Greece

**Antonios Broumas, CIPP/E**

Compared to 2019 and 2020, 2022 is expected to be a year of increased legislative developments and supervisory activity for Greece in data protection. Forthcoming legislative developments include the enactment of the Whistleblower Directive and the law implementing the Decision 2008/615/JHA on cross-border cooperation in combating terrorism and cross-border crime (Prüm Decision). In addition, regulation will be introduced regarding measures against the COVID-19 pandemic, health records, e-health and teleworking. Finally, the government shall publish the National Plan for Artificial Intelligence.

Apart from the above, the Framework Law 4624/2019 supplementing the GDPR and incorporating the Law Enforcement Directive may also be amended according to the improvements proposed by the Hellenic Data Protection Authority in its Evaluation Report of the Law. Other possible legislative developments concern the adoption of secondary regulation by the Ministry of Digital Governance regarding the EU Cybersecurity Act and the implementation of Law 4727/2020 on digital governance, with an emphasis on public sector data interoperability.

At the level of supervision, Greece's DPA has already integrated additional highly qualified personnel into its organization and was expected to acquire a newly appointed council by the parliament in 2021. In 2022, the DPA will have the necessary resources and mandate to make a fresh start and execute a plan of regulatory interventions in hot areas of data processing and enforcement activities in high-risk market sectors. The authority may, on the one hand, issue guidelines and opinions in relation to video surveillance, body cameras worn by police, health data, employee data processing and whistleblowing, whereas on the other hand, it could conduct a plan of investigations and dawn raids in the markets of finance, insurance, electronic communications, e-commerce and marketing.

## Hong Kong, China

**Timothy Ma, CIPP/E, CIPM**

In 2021, the main piece of privacy and data protection legislation in Hong Kong underwent a major revamp. In October, the Personal Data (Privacy) Amendment Ordinance was published in the Hong Kong Gazette and became effective. Major changes include the criminalization of "doxxing," expanding the privacy commissioner's powers to carry out criminal investigations and prosecute doxxing and related offences, and demand disclosure of doxxed personal data cease. The Office of the Privacy Commissioner for Personal Data also set up a telephone hotline for handling inquiries or complaints regarding doxxing activities. The PCPD issued the Amendment Ordinance Implementation Guideline to explain the amendments, with examples to illustrate the scope and application of doxxing offenses, the powers conferred to the commissioner and how the public can lodge complaints with the commissioner.

Given the commissioner's focus on combating doxxing (having received 5,800 doxxing complaints through to June), it is expected the commissioner will actively exercise its powers under the Amendment Ordinance, carrying out investigations into alleged doxxing and prosecuting offenders to the extent doxxing constitutes a criminal offence. It is also expected the commissioner will issue cessation notices to individuals or entities (such as operators of social media platforms, internet service providers or hosting service providers) to take expeditious action to remove personal data subject to doxxing. The PCPD is expected to issue further guidance and materials to enhance public awareness of and compliance with the Amendment Ordinance.

The Legislative Council is also expected to consider amendments first proposed by the Constitutional and Mainland Affairs Bureau back in January 2020, which would further update the PDPO with a mandatory data breach notification requirement, data retention guidelines, regulate data processors, expand the definition of personal data and confer additional powers to allow the commissioner to directly impose financial penalties. There is no precise timeline for implementation at this stage. However, with passage of the Amendment Ordinance, it is expected attention will return to effecting these broader amendments to the PDPO.

## India

**Pranav Rai, CIPP/A**

"India—Confusion Raj…" was a chapter title in Graham Greenleaf's "Asian Data Privacy Laws" and it set out the severe deficiencies of India's data protection rules from 2011. Little did we know this title would age splendidly in 2021, and these rules — which only superficially resemble a data protection law — would continue to exist even today.

In late 2019, when the Personal Data Protection Bill, 2019 — largely regarded as "progressive" by many important voices, including Greenleaf — could not be tabled before Parliament amid protest from the opposition, it was referred to the standing committee for further scrutiny. The committee was expected to come up with its report by the budget session (March 2020) of Parliament, but managed to table its report only in December 2021. This report recommends substantial amendments to the 2019 bill and a phased approach to implementing the law.

The delay in tabling the report was, however, only one of the reasons impeding the passage of the law. The Ministry of Electronics & Information Technology has lately been reticent about providing details on the upcoming

law and even about its shift in focus to non-personal data legislation/framework, which adds to the ambiguity. Perhaps because of this shifting focus, the committee recommended an expansion in the scope of the bill by including non-personal data protections and renaming it "Data Protection Bill."

While there is nothing inherently wrong with this approach, it has some flaws and may even be premature. There are also some controversial provisions in the committee-proposed bill, like questionable independence of the DPA and the exceptions section that keeps government agencies out of the bill's purview. Uncertainty regarding the contents of the proposed law and timing of its passage was already aplenty and has only increased since the tabling of the report. The report remains but a recommendation to Parliament, and there is lack of unanimity even among the committee members' – with some prominent members dissenting.

Together these cast doubts regarding the government's determination to get the Personal (or possibly an all-encompassing personal and non-personal) Data Protection Bill passed swiftly. It cannot be a matter of government ability, though — after all, the political dynamics of the committee continue to be favorable to the majority, the ruling Bhartiya Janta Party. An official and unambiguous government version from the relevant ministry on the way forward on proposed legislation will be assuring; until then, the doubts regarding government resolve will remain.

If this incertitude continues and a comprehensive data protection law is not brought expeditiously, the constitutionally guaranteed right to life and personal liberty of the residents, trade (particularly India-EU FTA), and also the newfound purpose of "interest and security of the state" — made unmistakable by addition to the prefatory material of the committee-proposed bill — are under threat in varying proportion.

In 2022, the committee-proposed bill (or perhaps a legislative compromise of that bill) will likely continue moving forward — albeit in fits and starts — towards being passed as law. If the government can, however, regain its resolve — last displayed prior to the introduction of the 2019 bill before Parliament, but absent since then — a comprehensive data protection law would be possible in the next Parliament session (starting in February 2022). The hope still is that India will shed the "Confusion Raj" tag in 2022 and show others a fourth path: a "Fourth Way to Privacy, autonomy and empowerment," distinct from the approaches in the U.S., EU and China, as suggested by the Justice B.N. Srikrishna committee.

## Ireland

**Kate Colleary, CIPP/E, CIPM**

2022 will see the commencement of the final sections of the Data Sharing and Governance Act 2019, which provides a clear legal basis for the sharing of personal data between public bodies in certain circumstances. The aim is to reduce the administrative burden associated with the need for individuals to provide their personal data to numerous public bodies.

The Data Protection Commission published its Regulatory Strategy 2022-2027, which sets out its vision for a crucial five years in data protection law. The DPC emphasizes taking careful account of the needs of diverse stakeholders, and the fast-paced and non-traditional sectors it regulates. All strategic goals set out in the strategy have been proposed as a means of "doing more, for more." As the DPC has finite resources, it will prioritize complaints of systemic importance and will seek a collective approach to enforcement throughout Europe.

The strategy outlines five strategic goals:

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

We look forward to the DPC publishing the following guidance in 2022:

- Quarterly case studies based on common complaint issues.
- Guidance on complaint-handling processes.
- Updates on the development of codes of conduct and certifications to enable sectoral best practice.

The DPC published the final version of the Fundamentals for a Child-Oriented Approach to Data Processing in 2021. This is the culmination of an intensive project over three years involving three separate stakeholder consultation processes (including a direct consultation with children), engagement with experts on child rights, expansive research and a two-stage drafting process. With the publication of the fundamentals, 2022 could see a new age in the processing of children's data in Ireland, with controllers and processors more aware of their enhanced obligations and the issue stated as a priority for enforcement by the DPC.

The DPC received additional funding of 4.1 million euros for 2022, bringing their total allocation to 23.2 million. The funding will facilitate the recruitment of more than 40 new staff, with specialized skill sets in areas such as investigation, technology and legal.

In September 2021, the DPC concluded its investigation into WhatsApp, finding it had failed to discharge its GDPR transparency obligations. A fine of 225 million euros was imposed along with a reprimand and an order for WhatsApp to take a range of remedial actions.

WhatsApp appealed, seeking to quash the decision and an order that certain provisions of the Data Protection Act, 2018 are invalid, unconstitutional and incompatible with the European Convention of Human Rights. We await further developments in 2022.

In September 2021, the DPC also commenced two inquiries regarding TikTok. The first relates to platform settings for users under 18 and age verification measures for persons under 13 as well as transparency obligations. The second inquiry will focus on transfers of personal data by TikTok to China. We expect to see progress made in 2022.

In December 2021, the DPC submitted a draft decision (relating to Instagram's processing of personal data of children) to other concerned supervisory authorities across the EU. We await the views of the CSAs in early 2022.

## Israel

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

The Israeli government is moving forward with the enactment of two amendments to the Protection of Privacy Law, 5741-1981. The first, Amendment No. 13, will provide the Privacy Protection Authority with substantial enforcement powers that the PPA lacks under the current law, including considerable fines and police-like investigation authority. The

second, Amendment No. 14, is aimed at narrowing down the mandatory database registrations and modernizing definitions under the PPL, including personal data, sensitive data and data processing. So far, the legislation process of these two bills was suspended due to various reasons, but with the current government, there is a likelihood they will be enacted in 2022.

Israel continues to suffer from an increasing volume of cyberattacks on companies and public bodies, causing mass leaks of personal data. As a result, information security continues to dominate data protection compliance efforts. Privacy-related class actions are on the rise. They are focused mainly on claims for violation of information security statutory obligations, following cybersecurity events that have caused unauthorized access to personal data, and on use of personal data without appropriate notices and consents, in violation of the PPL. Class actions continue to be the dominant risk for companies doing business in Israel.

The discussions between the EU and Israel around the continuance of the adequacy recognition are still underway with no published end date. Currently, the EU continues to maintain the 2011 adequacy recognition decision.

## Italy

**Rocco Panetta, CIPP/E**

2021 was a busy year for Italy's DPA, the Garante, and 2022 will no doubt be the same.

The recent sanction to an Italian university for the unlawful use of software to monitor students during exams and the measures taken in relation to the still-persistent COVID-19 pandemic pave the way for a future in which the fundamental rights of citizens, students and workers will need to be protected even more, even when they are operating remotely. At the same time, the strong acceleration in digitization has led to a significant increase in cyberattacks; companies and public administrations are now called upon to invest more in digital security and staff training.

The other big challenge is social media. Although it seems to be an exclusively EU game, the Garante has been at the forefront of discussions with major social networks, such as Facebook and TikTok. The introduction on the market of new, potentially privacy-compromising smart devices and the difficulty in finding a reliable solution for the identification of minors made it necessary to have an honest discussion between the parties. The companies explained adopted solutions and the Garante provided indications necessary to ensure a higher coefficient of compliance with data protection regulations. Since these solutions need time to settle, the year 2022 will certainly be devoted to such discussions. It is therefore expected that in the year to come, the Italian DPA will be among the most active and attentive on these issues at the international level.

Finally, the digitalization of the public administration and the development of artificial intelligence will be at the heart of the Italian agenda, and the Garante and the protection of personal data will be at the forefront.

## Japan

**By Gabor Gerencser, CIPP/E**

As the EU Commission's adequacy decision demonstrates, Japan already has a robust data protection regime. Nevertheless, a significant amendment of the Act on the Protection of Personal Information is to enter into force on April 1, 2022, as the second comprehensive overhaul of Japan's data protection law, which was first enacted in 2005 and significantly

amended last in 2017. The current amendment further strengthens data subject rights in Japan.

Outlined more in detail in this article, the amendments, among other things:

- Expand data subjects' rights when demanding the cessation of use, cessation of third-party transfer, erasure and electronic disclosure of their personal data.

- Introduce mandatory obligations to report data breach incidents to the Personal Information Protection Commission and notify the affected data subjects in cases when the data subjects' rights and interests are likely to be infringed.

- Strengthen current regulations on data transfers to third parties outside Japan; for example, requiring the provision of certain information to data subjects.

During 2021, the PPC issued detailed enforcement rules, explanatory guides and Q&As on these amendments. Such detailed rules and guidance elaborate on important practicalities of the amendment, such as when and what data breach incidents are to be reported to the PPC.

Therefore, 2022 and especially its first quarter will be busy for privacy practitioners in Japan. With all the necessary guidance expected to be in place, Japanese businesses will have to thoroughly revisit their privacy management practices, including external privacy notices and adapting incident response manuals.

## 🇱🇹 Lithuania

**Natalija Bitiukova, CIPP/E, CIPM, FIP**

In 2021, the tensions between data protection and freedom of expression resurfaced in Lithuania when the Supreme Administrative Court found a local newspaper in violation of data protection rules for publishing personal data of the individuals allegedly involved in corruption. The case prompted a debate about the need to revise the outdated Law on the Provision of Information to the Public regulating data processing in the journalistic context, and the discussion is likely to continue into 2022. In addition, the court decided to conduct a judicial review of the case, and the decision, which will set the course for judicial enforcement in the future, is expected this year.

In 2022, Lithuania is set to create an independent oversight mechanism for intelligence activities by adopting a recently proposed bill on the Inspector of Intelligence Services. According to the bill, a newly established Ombudsman-type institution will, among other things, have a right to investigate complaints related to unlawful personal data processing in the context of intelligence activities. If adopted, the law will establish a third authority with responsibility for data protection oversight in Lithuania in addition to the already-existing State Data Protection Inspection and Office of the Inspector of Journalist Ethics.

It is planned that in 2022, 14 new positions will open in the DPA, increasing the number of its staff by almost 30%. Although a positive development, it is likely the DPA will face challenges competing for talent against large businesses and law firms and thus be required to hire more junior staff, potentially impacting its ability to handle rapidly growing numbers of complaints and enforcement cases.

Given the high ambitions of the current ruling government in the area of innovation and new technologies, a stronger emphasis on the implementation of the national artificial intelligence strategy is expected. This, coupled with the European developments around the AI Act, will likely generate national discussions (which were limited so far) around the tensions between new technologies and human rights, including the right to private life and personal data protection.

## Luxembourg

**Vincent Wellens, Yoann Le Bihan, CIPP/E**

2021 was busy for Luxembourg's National Commission for Data Protection, to say the least. The DPA made global headlines by imposing the heaviest GDPR fine ever — approximately 746 million euros — to Amazon regarding its interest-based advertising business in July 2021. The CNPD decision is being challenged before the Luxembourg administrative court of first instance, and the decision will shed further light on the basis of lawfulness for such activities and some aspects of the procedure before the CNPD. Amazon risks becoming a regular client of the CNPD as the non-governmental organization behind Max Schrems, NOYB, launched new actions against Amazon before the CNPD in 2019 (on the right of access regarding Amazon Prime service) and at the end of 2021 (on the deployment of algorithms discriminating users).

A more stringent enforcement of the rules on cookies and online trackers will likely come too, following the October 2021 publication of the long-awaited guidelines, which clarified the views of the CNPD and its interpretation of the law in practice in this respect. Furthermore, six audits on transparency in the e-commerce sector are ongoing.

To date, the CNPD also issued no less than seven different formal advices on bills of law related to the fight against COVID-19. In 2022, the measures to fight the pandemic are likely to remain high in the political agenda.

At the same time, the CNPD deals with "business-as-usual" operations, including the publication of 36 decisions (in a country where the population last year was estimated slightly under 650,000). Most of these related to the function of the DPO, CCTV monitoring and geolocation. In 2022, many more sanction decisions are to be expected.

In May 2021, the CNPD launched a second public consultation on its Article 42 certification framework project (GDPR-CARPA) but has not yet published the results. Delivering on this project is part of the 2020-2022 roadmap and the CNPD started working on it before May 2018, so we can expect new developments in the coming months.

Finally, an important topic that risks heating the debates in 2022 is the flow of data between public-sector entities and private or other public entities. The CNPD seems to require that the list of addressees of public-sector personal data must be included in the law governing the administration concerned, while at the same time, several legislative "open data" initiatives, such as the draft Data Governance Act on the EU level, favor the access to public sector data.

## Mexico

**Gabriela Espinosa Cantu, CIPP/US, CIPM**

A handful of initiatives to amend the existing Mexican Federal Data Protection Law Held by Private Parties have been presented by different members in Congress. And while none of them has moved forward significantly through the complex legislative process,

indicating a fairly premature parliamentary stage, some of them are worth mentioning.

Although none of the current amendment bills are radical in modifying the law to mirror the EU's GDPR, some initiatives propose changes to provisions that would bring the Mexican Data Protection Law more in line with it, such as:

- Including data portability rights.
- Notification within 72 hours to affected individuals after a breach.
- Defining what constitutes a "risk of harm" to an individual's rights as a result of a breach.
- Providing extraterritorial effects to the law-defining obligations to controllers or processors regardless of where they are located when certain conditions are met.

While some of these initiatives could be worth reviewing and discussing thoroughly, it seems unlikely to happen given the political arena in Mexico. Most of these bills have been presented by lawmakers not part of the majority in Congress, meaning they are trapped at the chamber of origin. Moreover, the Mexican president suggested at the beginning of 2021 his intention to dissolve Mexico's DPA, the National Institute of Transparency, Access to Information and Protection of Personal Data, by questioning its autonomy and criticizing its cost. Given that the president is in the second half of his mandate and his party holds the majority of votes in the current legislature, it is unfortunately most likely that both chambers in Congress will push his agenda first rather than provide attention and efforts in setting a higher bar for data protection and privacy rights in Mexico.

## The Netherlands

**Abraham Mouritz, CIPP/E, CIPP/US, CIPM, CIPT, FIP**

2018 was all about having a privacy framework, and 2019 and 2020 were centered on organizations not having their technical and/or organizational measures in place. Several events in 2021 drastically shifted the focus to ensure transparency of data, especially with AI. It is this area where I see potential legislative data protection reform taking place in The Netherlands.

- Start with the verdict of the Hague district court in the SyRI case in mid-2020. SyRI is a citizen-risk profiling system designed by the Dutch government to process large amounts of data collected by various Dutch public authorities to identify persons that, according to the algorithms, are most likely to commit social benefits fraud. The court ruled SyRI was insufficiently transparent and verifiable, thereby considering the use of the system to be unlawful and noncompliant with Article 8 of the European Convention on Human Rights.
- In March 2021, the Amsterdam District Court ruled the AI systems of ridesharing companies Uber and Ola do not meet the requirements of transparency. The court ordered both companies to disclose data used to deduct earnings, assign work, suspend drivers and make clear how driver surveillance systems are used. My colleague Anton Ekker, the attorney representing former Uber drivers, is truly doing ground-breaking work in these cases.
- The Dutch government fell on 15 Jan. after the use of a child welfare system wrongly labelled thousands of parents as fraudsters ("toeslagenaffaire"). The system used by the Dutch Tax

> Authorities consisted of AI risk-based algorithms. Similar to SyRI, this system displayed a bias to certain groups more likely to commit fraud. This crisis also highlights some of the dangers of AI. To date, this crisis for many households has not been resolved and has left many people not just wrongly labeled in countless systems, but also with large debts. As a result, people have lost homes, their jobs and around 1,115 children were rehomed.

These matters illustrate the need to make the use of AI more transparent — not just to the data subjects but also to those who use the system to better understand why and how certain automated decisions are being made. It is not without reason that Article 22 of the GDPR places restrictions on decisions "based solely on automated processing." Currently the use of AI is predominantly governed by ethical rules, which, among other things, stress the need for AI to be transparent and explained — so-called White Box AI. The European Commission's upcoming regulation on the use of AI shifts the need for AI transparency from the ethical to the legal sphere. The standards for the regulation are not expected to be ready until 2024.

## New Zealand

**Daimhin Warner, CIPP/E**

2021 was dominated by implementation of the Privacy Act 2020. 2022 will be an exciting year of complementary developments, helping New Zealand regain its position at the forefront of future-proofed privacy regulation, but also signalling the emergence of an Aotearoa/New Zealand approach to privacy that reflects our unique bicultural foundation.

A bill implementing a new consumer data right will be introduced to Parliament in 2022. This will be New Zealand's version of the data portability right, describing a mechanism for consumers to securely share their personal information with trusted third parties. The right will be rolled out on a sector-by-sector basis, with banking likely to be the first cab off the rank. The primary legislation will create an overarching framework for the right, including basic obligations that will apply to designated sectors. The types of personal information in scope for the right will be specified in each sector designation, with more detailed obligations set out in sector rules and data standards.

The Privacy Act 2020 introduced a new requirement for the privacy commissioner to take into account cultural perspectives on privacy when exercising their functions. In Aotearoa/New Zealand, this includes Māori perspectives. According to outgoing Privacy Commissioner John Edwards, "we are beginning to engage in a process of understanding how (the Privacy Act), this human right, this commercial imperative, and this consumer protection might be informed by te ao Māori and engaged to meet the aspirations of tāngata whenua. This is exciting, and it saddens me to leave this role as we embark on this next stage in the evolution of privacy in Aotearoa."

This will be a legislative theme for 2022, with privacy-related legislative changes on the horizon that include a focus on Te Tiriti obligations, te ao Māori concepts and increased engagement with Māori. Examples include the Data and Statistics Bill and the Digital Identity Trust Framework. These changes are taking place against a background of increased visibility and discussion of concepts such as Māori data sovereignty.

Finally, we will have a new privacy commissioner in 2022, with John Edwards taking up the role of U.K. Information Commissioner in the new year. It will be exciting to learn what

the incoming commissioner's priorities will be, though they will likely include continuing compliance monitoring of the rental sector and perhaps an early flexing of statutory muscle with another enforcement action or two.

## Nigeria

**Ridwan Oloyede, CIPP/E, CIPM, FIP, Oluwagbeminiyi Ojedokun, CIPP/E**

2021 was an eventful year for privacy and data protection in Nigeria. The year witnessed the issuance of sanctions by the National Information Technology Development Agency. The revised National Cybersecurity Strategy was released. Lagos State legislature held a public hearing for its Data Protection Bill. There were also significant court decisions impacting data protection and 2022 is poised to be more eventful.

The most significant proposed legislation is the Nigeria Data Protection Bill 2020, which would establish an independent supervisory authority. The bill's progress has stalled since 2020 when it was first released for public contribution and has yet to make it to the legislature. However, there is a move to develop a new bill instead. As a result, the development, passage and signing of the bill are expected to be accelerated.

We should see progress with the Electronic Transaction Bill and Digital Rights and Freedom Bill. The president declined assent to the latter's previous version of the bill in 2019, now revised and introduced in the House of Representatives and expecting the House Committee report. In addition, the Electronic Transaction Bill is expected to see some progress. The bill is currently expecting the Senate Committee on Banking Insurance and Other Financial Institutions report. NITDA is also expected to amend its establishing Act, granting it additional regulatory powers over technology companies and data.

While some of the proposed laws advance privacy protection, some pose risks to privacy, like the integration of private closed-circuit TV infrastructure into the National Security Network in Nigeria Bill and the Internet Child Pornography Prevention Bill, 2019, pending before the House of Representatives.

There is a likelihood of more sector-specific frameworks from other regulators, increasing organizations' compliance landscape. For example, the Central Bank of Nigeria may finally release its Data Protection Regulation, mooted since 2018.

We expect progress with the National Electronic Health Record Bill, awaiting the Healthcare Services Committee report. In addition, we expect to see a revised version of the National Health ICT Strategic Framework after its mandate expired in 2020. Thus, we anticipate another five-year, strategic, action-driven framework.

With the effort by the Lagos state government to enact a data protection law, we may see the trend of other states releasing or passing laws with data protection or privacy implications. Another state in South West Nigeria reportedly has a draft law to present to its legislature.

The inclusion of an 8 billion naira fine for failure to store data locally was rumoured to be one of the reasons President Buhari refused to assent to the 2019 Data Protection Bill. However, there is suspicion that the mandatory data localization provision will find its way back into the 2020 version of the bill, albeit with specific categories of data.

There has also been much conversation on pervasive practices of digital lending companies, and regulators are starting to pay attention. There is a pending bill before the House of Representatives to regulate the activities of

the lenders and class action filed for violation of privacy. In addition, we expect coordinated action from the Central Bank of Nigeria, the Federal Competition and Consumer Protection Commission and NITDA (the substantive data protection regulator) to reign in the lenders. Finally, NITDA is expected to increase regulatory action through the issuance of guidelines and sanctions.

## Norway

**Martha Ingves**

The focus on AI is steadily increasing in Norway and will likely continue in 2022. The Norwegian DPA, Datatilsynet, started its Sandbox for Responsible AI in 2021, which aims to support the innovation of ethical and responsible AI solutions. The Sandbox will continue with new projects in 2022.

Regulatory reforms are also on the horizon, as Norway is likely to introduce changes to its ePrivacy rules. The Norwegian government recently proposed the adoption of a new Electronic Communication Act, even though it might be short-lived due to the possible adoption of a new ePrivacy Regulation at the EU level soon. Among other things, the proposed act could entail changes regarding the rules on consent for the use of tracking technologies (e.g., cookies), which under the current legal regime may be given through web browser settings.

Norway might witness some high-profile litigation in the privacy area in 2022. In December 2021, Datatilsynet issued its highest fine so far — 65 million NOK (around 6.5 million euros) — against Grindr for failing to comply with the consent requirements under the GDPR. Grindr is likely to appeal the fine before the Norwegian Privacy Board of Appeals, Personvernnemnda, which could issue its decision in 2022.

Finally, in 2022, the privacy commission will issue its report on the state of privacy in Norway. The commission is a consultative body appointed by the Norwegian government to map the existing data privacy landscape in Norway and identify the most significant challenges going forward. The findings of the commission are intended to lay the foundation for further policy development regarding privacy in Norway.

## The Philippines

**Irish Salandanan-Almeida, CIPM**

The Philippines' privacy law, the Data Privacy Act, was enacted in 2012, with its Implementing Rules and Regulations issued in 2016. Five years into its implementation, there are proposed amendments to the DPA introduced by way of a house bill lodged before Philippine Congress.

Among the proposed amendments are the inclusion of financial data in the definition of sensitive personal information and a clarification on the requirements for personal data breach notification.

There are also suggested changes to the criteria for lawful processing of sensitive and personal information, allowing processing for public health purposes and humanitarian emergencies, among others, to align the criteria with international standards. Further, to address concerns around child online protections, there is a recommended provision that will require parental consent for online services offered directly to children 15 years old or younger.

Lastly, to strengthen the implementation of the DPA, the house bill declared definitive functions of the National Privacy Commission, the Philippines' privacy regulator, in the exercise of its quasi-judicial powers and in the effective enforcement of its orders.

Another upcoming development is the issuance of a circular by the NPC, with guidelines on administrative fines, designating a range of 1-5% of annual gross income for certain privacy violations.

In November, the NPC launched the Philippine Privacy Trust Mark with NPC Chairman Raymund Liboro stating that it comes at an opportune time, as the Philippines aims to fully embrace digitalization for our economic recovery. He goes on to say this will not be achieved without strengthening the foundation of trust in every action and transaction we make online. While completely voluntary, organizations acting as personal information controllers and processors are expected to secure PPTM certification in the coming year to demonstrate operational privacy compliance and to increase trust among their data subjects.

## Poland

**Marcin Lewoszewski, Anna Kobylańska**

For 2022 we predict further, intensive enforcement actions taken by Poland's DPA, Urząd Ochrony Danych Osobowych. In 2021, we witnessed some interesting court decisions overturning UODO decisions. Once such decisions are annulled, the supervisory authority must revise all such cases. We expect revised decisions on data retention, notification of data breaches and calculation of administrative penalties.

Regarding data retention, the UODO took the position that a controller should delete the data right after a relationship with a data subject ends. As a result, the controller cannot claim it has a legitimate interest to keep the data later on for the purposes of exercising or defending legal claims. The DPA stated if the controller cannot prove it has good reasons to believe such claims will be raised, the controller should not store the data for the purpose of potential future claims. Polish courts overturned such decisions, stating a controller cannot predict if and when a data subject may raise claims. But this does not exclude such claims being raised, and the controller has a right to store data to defend itself or exercise its claims.

Regarding notification of data breaches, the UODO issued decisions where data controllers were found responsible for mail lost by professional mail deliverers (such as Polish post or private couriers). It will be interesting to observe how the situation develops and whether controllers will be obliged to control more entities that act on their own.

We predict the DPA will change the way it calculates administrative fines. This is based on the court cases where the current method of calculation was successfully questioned by one of the controllers. Results of the dispute should be visible soon in practice of the authority.

Also, we expect enforcement actions of the UODO in relation to cross-border proceedings held by the UODO and other EU DPAs. This will likely be related to some of the consumer protection organizations and their activities in Poland.

We expect new legislation related to COVID-19 security measures, such as an act on employers' access to employee vaccination status information. We also expect new legislation enabling employers to check employees' sobriety and an act regulating protection of whistleblowers' identities.

In terms of sectorial regulation, we envisage a new law on clinical trials, supplementing EU regulation. Under the new law we should see provisions regulating the situation of a sponsor of clinical trials regarding personal data of clinical trial participants.

We also expect new developments concerning the interplay between personal data protection and access to data in the public domain. Under new laws, information on all agreements entered into by public institutions will be made public. As a result, a lot of information included in such agreements, such as salaries of employees of public institutions, will be made available to anyone. This may influence the way personal data is protected and how it may be used by third parties.

## Russia

**Stanislav Rumyantsev, CIPP/E**

In 2021, Russia adopted several laws demonstrating a trend towards strengthening data protection. Supervisory authorities will likely focus on the enforcement of new rules in 2022.

Beginning March 1, 2021, Russia imposed restrictions on the processing of publicly available personal data. Data operators (Russian equivalent of the term controllers) must obtain data subjects' consent to the publication of personal data. In the consent form, a data subject may specify conditions and limitations for the processing of his/her data by anyone who accesses it. Data operators must publish these conditions and limitations. The DPA, Roskomnadzor, has not checked the fulfilment of these rules yet. 2022 may bring first case law on the matter.

Next year, Roskomnadzor will inspect companies according to the recently adopted state supervision and control procedures.

Parliament is hearing a bill amending requirements to the consent form. Written consent serves as a lawful basis for disclosures of HR data by employers, cross-border transfers into some countries and in other cases. If the bill turns into law, data operators will have to update their templates and retrain HR personnel.

After Jan. 1, some foreign internet companies are required to open offices in Russia. The new law applies to internet giants having more than 500,000 Russian users daily, hosting providers storing Russian users' data and others. The law requires that such companies, among other things, obey the personal data localization requirement (conduct certain processing operations with Russian nationals' data in databases physically located within Russia). If they fail, Roskomnadzor may prohibit them from collecting data, restrict money transfers, and/or block access to their websites and applications from the territory of Russia without recourse to courts. There is a general trend towards enforcing the localization requirement.

## Serbia

**Petar Mijatović**

According to the official yearly report of Serbia's DPA, the Commissioner for Information of Public Importance and Personal Data Protection, adopted in March 2021, the main impediments in exercising data subject rights in Serbia are the normative flaws of the Law on Personal Data Protection, noncompliance of other laws with the LPDP and lack of implementation of the current Data Protection Strategy. In June, the government of the Republic of Serbia formed the working group for the preparation of the draft of the new Data Protection Strategy with an action plan.

It is expected that in 2022 this working group will come out with some suggestions regarding the country`s future plan in the field of data protection, especially in terms of better implementation and potential revision of the LPDP, which in August celebrated two years of its application and harmonization with the GDPR.

In 2021, only a couple binding corporate rules were adopted by the commissioner for the transfer of personal data between groups of entities.

Keeping in mind that many of the international companies operating their businesses through Serbian affiliates obtained approval by an EU DPA on their BCRs, it can be expected that in 2022 many of them will implement the requirements of Serbia's LPDP and initiate the procedure of obtaining the approval from Serbia's DPA on their BCRs as well. In this case, Serbian affiliates will have the right to rely on BCRs as an appropriate safeguard for transfer of personal data within the group of entities.

## Singapore

**Pranav Rai, CIPP/A**

The previous few years saw the first comprehensive review of Singapore's Personal Data Protection Act since its enactment, resulting in an amendment with the aim to continue safeguarding consumers' interests and keep pace with technological advances and new business models.

The amendment takes effect in phases and 2021 saw its first batch enforced. Some are innovative, like the amendment removing consent requirements — subject to certain conditions — for organizations that use personal data to improve or enhance their products, services, methods or processes, and even understand customer behavior and preference.

There are others that are perhaps not so imaginative, but nevertheless in line with Singapore's privacy ambitions and aims, like including a mandatory breach notification system, bringing personal data processors on behalf of public agencies within the PDPA's ambit, further empowering the commission and enhancing controls over spam, which now includes spam sent using instant messaging services.

This brings us to what to expect in 2022. Data portability and enhanced penalties are two other important provisions in the amendment that still have not been enforced and we may see these happening soon. Already a fundamental data subject right in the GDPR, data portability will be enforced soon, albeit with a list of exceptions. Those include a case where the transmission can cause immediate or grave harm to or threaten the safety or physical/mental health of the individual concerned, or is contrary to national interest. Singapore was already in the "million-dollar penalty" club — a rarity in the rest of the region — and the penalties for organizations will soon be enhanced further and imposed on new classes of organizations: Up to 10% of the breaching organization's annual turnover in Singapore if the annual turnover exceeds SGD 10 million, and for use of dictionary attacks and address-harvesting software, up to 5% of the breaching organization's annual turnover in Singapore if the annual turnover exceeds SGD 20 million.

## South Africa

**Nerushka Bowan**

2021 was a significant year for data privacy in South Africa. On July 1, the long-awaited Protection of Personal Information Act, 2013 commenced following a 12-month grace period. As a result, we do not anticipate any further major legislative changes this year, but we do anticipate various developments and a busy year.

Over the course of the year, we anticipate businesses continuing to get to grips with their compliance obligations from POPIA, the further operationalization of the DPA, the Office of the Information Regulator,

additional guidance published by the regulator, approval and publication of codes of conduct for industry bodies and sectors, the publicizing of data breaches, civil action regarding the right to privacy and POPIA, and enforcement actions taken by the regulator. We also anticipate an increase in the number of data subject access requests received by responsible parties as well as access to information requests, courtesy of the Promotion of Access to Information Act, 2000.

We anticipate guidance from the regulator on a number of topics, including cross-border transfers of data, data breach reporting and the handling of juristic person information. South Africa is one of the only jurisdictions in the world that recognizes and protects the personal information of existing juristic persons in addition to living natural persons.

The regulator reported that it received a number of data breach notifications already. However, we have not yet seen any enforcement action from the DPA. POPIA gives the regulator strong powers to enforce compliance with the Act, including issuing notices, launching investigations, taking on lawsuits on behalf of data subjects and issuing administrative fines of up to ZAR 10 million.

Although South Africa now has comprehensive data protection legislation, we do not yet have adequacy status in terms of the GDPR. We hope to achieve this status in 2022. Similarly, we hope to receive guidance from the regulator deeming the EU to be adequately protective regarding POPIA.

Another significant regulatory development at the end of last year was the commencement of the Cybercrimes Act, 2021 in December. The Cybercrimes Act creates a host of new cybercrimes, such as cyber fraud and revenge porn.

There are certain sections that have not yet come into force: the prosecution of cybercrimes, the handling and preservation of evidence, and the reporting obligations for telecommunications providers and financial services institutions. We anticipate the date for commencement for the remaining provisions of the Cybercrimes Act will be announced later this year.

## South Korea

**Kyoungjin Choi**

In 2020, South Korea allowed the compatible use of personal data and the processing of pseudonymized data for archiving in the public interest, scientific research purposes or historical research purposes through the revision of the so-called "Three Data Laws," in response to the data era. And the Personal Information Protection Committee was reborn as an independent supervisory administrative authority. However, there were criticisms the revision of the "Three Data Laws" did not reflect all the diverse demands of changes in the data age. The PIPC prepared a drastic amendment bill through the Drafting Committee for Amendment of Personal Information Protection Act, and several amendments, including the government bill, are currently pending in the National Assembly. An alternative that integrates several laws is being prepared, and in 2022 the PIPA is expected to be revised in the following direction:

- The distinction between online and offline disappears and the same basis for processing personal data applies.

- As new rights of data subjects, the rights related to automated decision-making, such as the right to object or the right to explanation as well as the right to data portability are introduced.

- A new system for international transfers of personal data is introduced by stipulating adequacy decisions or certification as the legal basis for transborder data flow.
- The self-regulation system is strengthened.
- The scope of the law is extended to mobile image data processing devices in addition to closed-circuit TV.
- A unified legal basis for legitimate processing of personal data is established by integrating without distinction according to collection/use or provision to a third party.
- The dispute mediation system is strengthened.
- Blind spots in the PIPA are eliminated by reducing the exclusionary rules and incorporating them into the legal basis for legitimate processing.
- The existing criminal sanctions significantly shift to economic sanctions, such as administrative fines (less than 3% of total turnover).

As PIPA is expected to be significantly revised in 2022, global data controllers must prepare with special attention.

## Sweden

**Sofia Edvardsen**

At the beginning of 2022, there were over 100 ongoing investigations by Sweden's DPA, the Integritetsskyddsmyndigheten, which is an increase compared to previous years. The oldest investigation is from March 2019. A case that garnered a lot of media attention was the police's use of facial recognition without any legal basis through the AI application Clearview. The DPA declared the usage was a breach of the GDPR. The DPA has shifted strategy in its enforcement actions, now prioritizing complaints before risk-based proactive enforcement of specific processing activities. We expect to see a speedier process in 2022 and receive more interesting case law in the coming year, e.g., use of consent for cookies, use of Google Analytics in view of the "Schrems II" judgement, role of joint controllers and more.

During 2021, the Swedish government sought to improve the infrastructure and the use of e-identification within the public sector. The current system, which has relied on private identifications systems, has been considered not sufficiently secure. Therefore, a report was presented with a proposal of a legal framework regarding acceptance and verification of e-identification services that can be used in contact with the public sector. In 2022, it is expected legislative proposal shall conclude and may open the government to new services.

Following the discussion of whether public authorities could or should outsource their IT operations or use public cloud services, the government presented an interim report at the beginning of 2021. The interim report analyzes the government agencies' need for secure and cost-effective IT operations, security and legal conditions for coordinated government IT operations, and analyzes the legal conditions for public authorities, municipalities and county councils to outsource IT operations and cloud services to private suppliers with maintained security. The report provided a framework for assessing risk much like the European Data Protection Board framework on "Schrems II" and did not rule out cloud service providers as such. A new Swedish Government Official Report on the

subject was issued Dec. 15, which specifically addressed the Swedish authorities' need for a secure and cost-effective IT operation. Furthermore, it addressed the appropriateness and legality to use cloud services in the public sector.

In the beginning of 2022, the government presented a bill with a revision of the Swedish Consumer Sales Act that applies to the purchase of goods as well as digital content and digital services. The proposal aims to adapt Swedish law to two EU directives and entails, among other things, clearer rules for assessing errors in digital content with some relevance for data protection.

The government's work on cybersecurity proceeded with the foundation of a new Swedish Cybersecurity Centre. Sweden implemented the EU Regulation (EU) 2019/881 (Cybersecurity Act) in July 2021. We except to see much activity in this field in 2022.

Further, the implementation of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law entered into force mid-December 2021, aiming to increase the possibilities for employees in both the public and private sectors to report misconducts.

## Switzerland

**Stéphane Droxler, CIPP/E, CIPM**

After more than three years of parliamentary discussions, the revision of the Data Protection Act was finally approved in September 2020. The new law aims to achieve EU recognition of data protection equivalence.

To this end, it provides new tasks for data controllers and processors, such as:

- The introduction of the principles of privacy-by-design and default.
- The possibility (but not the obligation) for private data controllers to appoint a DPO.
- The obligation to carry out impact assessments.
- The encouragement made to professional associations to draft their own codes of conduct and submit it to the supervisory authority for approval.
- The obligation for private companies with more than 250 employees to maintain a record of processing activities.
- The duty to notify security breaches as well as some reinforcement of individuals' rights, in particular regarding the right of access and data portability.

In terms of sanctions, fines of up to CHF 250,000 may be imposed on private individuals in the case of intentional behavior and omissions only. Negligence will therefore not be sanctioned. It should be noted that if the identification of the person responsible within a company requires disproportionate investigative measures, the company itself may be sanctioned, but up to a maximum of CHF 50,000. In contrast to the European authorities, the commissioner will still not be able to impose administrative sanctions. Offenders will therefore be punished by the cantonal criminal prosecution authorities, to which the commissioner may report offenses.

The enforcement of this new law is not expected before the second half of 2022, or even early 2023. At the time of writing, the consultation period for the draft implementing ordinance just ended. This highly controversial text does not provide the substance expected for the implementation of the law to be achieved. Many privacy pros think either it will have to be rewritten or many provisions will have to be amended.

## Thailand

**Yulia Askhadulina, CIPP/E**

On May 27, 2019, Thailand adopted the Personal Data Protection Act 2019, the country's first general data protection law with GDPR-like extraterritorial reach. The law prescribed a one-year grace period for the formation of the Personal Data Protection Committee, issuance of subordinate regulations and businesses to prepare towards compliance. In 2021, the PDPA's enforcement date was postponed to June 1 of this year following the Ministry of Digital Economy and Society's request to enable its stakeholders to cope with the effects caused by COVID-19 and allow for the formation of the Personal Data Protection Committee. Despite the general delay of the PDPA, data controllers are required to implement security measures under the Personal Data Security Standards B.E. 2563 (2020) set forth by the MDES.

The PDPA prescribes the general requirements applicable to personal data processing and the specific requirements are left out to be addressed in the subordinate regulations. Throughout 2021, the MDES acted as the temporary Office of the Personal Data Protection Committee and conducted a series of public consultations for the draft subordinate regulations, two of which were conducted in English. The subordinate regulations are organized into three groups. Group 1 covers consent requirements, privacy notices, responsibilities of data controllers, cross-border data transfers, DPOs, qualifications and requirements, security measures, compliance processes, and sensitive personal data processing. Group 2 covers, among other things, scope clarification and representative designation, cooperation and consistency mechanisms, derogations, data subject rights, the responsibility of data processors, archiving purposes in the public interest, and research and statistics. Group 3 covers codes of conduct, automated processing, data protection impact assessments, data protection standards, certification and international cooperation.

The PDPA was enacted as part of the Thailand 4.0 plan, a countrywide reform aimed to create an innovation-driven economy, as shown in the PDPA Master Plan. Unfortunately, the current economic outlook is not looking great for Thailand, as the economy is heavily reliant on tourism and COVID-19 travel restrictions continue to impact the country negatively. Should this trend continue in 2022, the government may need to focus on more pressing issues.

## Turkey

**Furkan Güven Taştan**

Turkey celebrated the fifth year of its first-generation data protection code in 2021, which has made bold moves to enhance Turkish data protection culture. In 2022, eyes will be on the march toward the revision of the Turkish Data Protection Act, a move that appears to be gaining momentum. It is possible we will see an act more compliant with the EU's third-generation regulation, the GDPR.

One of the Turkish presidency's strategic aims in the 11th Development Plan is the revision of the Turkish Data Protection Act to comply with EU standards. The Ministry of Justice correspondingly set the timeline for the reform process. The legislation is anticipated to be enacted in April 2022 after receiving public opinion. Turkey will likely follow the same path as the EU by adopting a risk-based approach and the accountability principle with this reform package. These adoptions may be considered the essence of the prospective act.

As for the details, conditions for processing special categories of personal data that are challenging in Turkey's corporate world will

be readjusted in harmony with the GDPR. Moreover, the means for transfers of personal data abroad as provided in the law in force will possibly be extended with novel appropriate safeguards such as BCRs, codes of conduct and approved certifications. Another critical prospective revision might be presented in the increase of the current administrative fines that are insufficient to enforce the law effectively. In sum, the new legislation package may prove that Turkey will be increasingly considered a strict follower of countries with relatively more harmonized data protection regulations.

## United Arab Emirates

**Ben Crew, CIPP/E**

Organizations across the country are going to feel a profound impact from the recently enacted UAE Personal Data Protection Law. As a Dubai-based data privacy consultant with more than a decade of experience in this space, I expect the executive regulations, due in March, will see a final version of the law being a more business-friendly, slimmed down version of the GDPR, similar to the data protection laws recently established in the Dubai International Financial Centre and Abu Dhabi Global Market.

Beyond the passage of the UAE Data Protection Law, we expect to see additional activity across the country. For example, the DIFC is strengthening its data privacy position, including making impending changes to its 2020 Data Protection Law to remedy shortcomings revealed since it was enacted. An adequacy decision from the Department for Digital, Culture, Media & Sport in the U.K. for the DIFC is also expected this year, something that would significantly improve the business environment for companies operating under that jurisdiction. Additionally, the ADGM, DIFC and Qatar Financial Centre (which is expected to approve a new data protection law building on the existing QFC regulations and aligning closer to the DIFC and ADGM legislations) will begin negotiating a tri-partite data adequacy agreement between the three financial centers, as well as joining the DIFC in pursuing adequacy approval from the U.K.

The broader region is also set to experience significant momentum in terms of regulatory developments that emulate the GDPR and impact corporate and governmental data privacy obligations. This will include clarification around data localization requirements in various jurisdictions and ratifications relating to penalties and criminal accountability (particularly in Egypt's Data Protection Law). Free zones in Saudi Arabia, specifically Neom and the King Abdullah Financial District, will develop their own unique data privacy laws to compete with the DIFC and ADGM as major business centers. In parallel, additional countries will follow the lead of Saudi Arabia and the UAE in an attempt to lay the groundwork for a long-term, Gulf Cooperation Council-wide data privacy accord that will likely come into force in the next five to 10 years.

## United Kingdom

**John Bowman, CIPP/E, CIPM, FIP**

The U.K. government hit the ground running in the second half of 2021 with the publication of its ambitious plans for data reform to boost innovation, economic growth and protect the public. The results of the government's consultation on reform should emerge in 2022. It will be interesting to see if feedback received from industry, privacy advocates and other interested parties is taken into account as the government firms up its policy proposals. Whether this results in new legislation during 2022 remains to be seen. However, policymakers in the EU will likely monitor developments closely to see if

any potential reforms to the data protection regime diverge too far from the standards necessary for the European Commission's U.K. data adequacy decision to remain valid. In the meantime, the U.K. government will be advancing its own program of data adequacy partnerships with the U.S., Australia, South Korea, Singapore, the Dubai International Finance Centre and Colombia, all named as priority candidates for U.K. adequacy determinations.

Another key development is the appointment of a new information commissioner for the U.K. John Edwards moved from New Zealand to the U.K. to take on this high-profile role in succession to Elizabeth Denham, who stood down after more than five years in the post. The government has proposed some changes to how the Information Commissioner's Office operates and to the role of the commissioner, including empowering businesses to use data to drive innovation and growth in a way that protects the public. In the meantime, institutions should monitor developments in regulatory enforcement under the new commissioner to see if there are changes in priorities or approaches.

## United States

**Michelle Clarke**

2022 promises to be another busy year for U.S. privacy legislation. California will begin its rulemaking process and Virginia lawmakers are slated to review seven amendments to its privacy legislation. More than a dozen states have introduced or reintroduced privacy legislation since Jan. 1. It will not be a surprise if we see two or three states pass comprehensive privacy legislation before the end of the year.

Will the increase in state privacy laws spur the passage of a comprehensive federal law in 2022? It's unlikely, as Congress has other priorities to deal with, including the ongoing COVID-19 pandemic and the upcoming mid-term elections. It is possible legislation concerning specific issues like children's privacy and biometric privacy may be passed.

On the enforcement front, the U.S. Federal Trade Commission is expected to begin rulemaking on privacy and AI. Currently, the Build Back Better Act is under Senate consideration and, if passed, would grant the FTC $500 million, stronger enforcement authority and additional resources.

Check with the US Federal & State Privacy Watch page in the IAPP Resource Information for the latest information.

## United States — health care

**Kirk Nahra, CIPP/US**

Health care privacy, as both a legislative and a regulatory matter, is becoming more complicated and less stable with each passing year.

On the legislative front, the most likely developments will continue to focus on the implications of health care under the "comprehensive" state privacy laws. These new laws — in California, Virginia and Colorado — treat health privacy in mostly consistent ways by creating wildly inconsistent frameworks for health information and health privacy.

In California, for example, health information of California residents can be regulated under at least six different frameworks under the California Consumer Privacy Act and California Privacy Rights Act. This includes the Health Insurance Portability and Accountability Act and information regulated by the Confidentiality of Medical Information Act (a sort of — but not quite —

"mini-HIPAA" specific to California), which are both exempt from the CCPA.

The CCPA then kicks in to regulate in some of the gaps left by these other laws, but does not apply to health information of non-profits or most health information held by employers about employees (including virtually all COVID-related information, especially vaccine information). This general approach applies in Colorado and Virginia as well to create different rules for similar information depending on who holds it and for what purposes. We will watch to see whether other states follow this pattern as they try to pass their own state privacy laws. We will also consider if this same approach will apply under federal privacy proposals as they move forward next year.

On the HIPAA front, the U.S. Department of Health and Human Services is reviewing various information-sharing rules to address issues related to opioid use and social determinants of health. Specifically, it is debating whether to expand the scope of permitted disclosures to allow more disclosures to family members, social service agencies and others in the interests of individuals even when the individuals do not seek or approve these disclosures. These regulatory evaluations also may lead to legislative provisions, as there is meaningful debate about whether these disclosures should actually be permitted.

The FTC is also entering the regulatory debate about health privacy through a statement of principles related to the personal health records data breach notification rule. Because of the broad gaps left in the protection of health information due to the limited scope of the HIPAA rules, the FTC is seeking to expand the scope of this breach notification rule and apply it to a broader range of health care mobile applications, beyond the personal health records that were the original focus of the rule (and of the relevant Health Information Technology for Economics and Clinical Health Act provisions).

We also can expect to see health privacy addressed in discussions about COVID information, primarily in the ongoing political disputes about vaccine mandates and the like. To be clear, in most situations, vaccine information is not regulated by HIPAA — when your employer asks for your vaccine information, HIPAA is not relevant. Same with your airline, neighborhood restaurant, gym or movie theater. We are likely to see proposals to address the privacy of vaccine information, but in isolation rather than as part of a more comprehensive look at health care privacy.

## Zimbabwe

**Kuda Hove**

On Dec. 3, 2021, the Data Protection Act of Zimbabwe came into effect. This law has been in development since 2013. According to the act's long title, the law seeks to "provide for data protection with due regard to the Declaration of Rights under the Constitution … to establish a Data Protection Authority and to provide for their functions." Additionally, the act also makes amendments to the Criminal Code (Codification and Reform) Act to provide for investigation and collection of evidence of cybercrime, unauthorized data collection and breaches, and to provide for admissibility of electronic evidence for such offenses. Lastly, the act amends the Interception of Communications Act to establish a Cyber Security and Monitoring of Interception of Communications Centre.

The Data Protection Act defines key data protection concepts such as personal information, biometric and other sensitive data, data subject, data processor and data controller. Additionally, the act outlines the circumstances under which the transborder

flow of data may be undertaken. The act designates the country's existing telecommunications regulator, the Postal and Telecommunications Regulatory Authority of Zimbabwe, as the national DPA.

Apart from these positive provisions, the act has several provisions that undermine the constitutional right to privacy and data protection in general. For example, the amendment to the Interception of Communications Act that establishes a Cyber Security and Monitoring of Interception of Communications Centre places the center under the president's direct control. There is currently no provision for any kind of judicial oversight of the operations of this interception center.

This focus on the interception of communications is in line with the government's announcement in November 2021 about the creation of "a cyber-team that is constantly on social media to monitor what people send and receive since we cannot wish social media away." In 2022, it is expected there will be an increase in state-sponsored surveillance, which includes the interception of communications, especially considering the country is expected to hold elections sometime in 2023.

---

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