iapp

2020 Global Legislative Predictions

2020 Global Legislative Predictions

Edited by IAPP Managing Editor Michelle Clarke

What does 2020 have in store for privacy and data protection regulation? A data protection law is on the horizon for India. The U.K. is gearing up for Brexit and all that entails. Almost all countries featured in this report are expecting increased regulation and enforcement this year and, as a result, are increasing their workforce accordingly. Facial recognition is a hot topic in a number of countries, with some calling for a ban, while others embrace the technology. And, in the U.S., there is still talk of a federal privacy law.

This year's report includes contributions from IAPP members all over the world outlining their predictions and hopes for the upcoming year.

Argentina

Pablo Palazzi

On Sept. 19, 2018, the Executive Branch submitted the Personal Data Protection Bill to Congress to reform the current Personal Data Protection Act. If the PDPB is approved as submitted, Argentine regulations will follow the provisions introduced by the EU General Data Protection Regulation.

Some of the main changes the PDPB will introduce in the local data protection regulatory framework are discussed below.

The PDPB establishes the obligation for data controllers and data processors to designate a data protection officer when data controllers and data processors are public authorities and organizations, the processing of sensitive data is performed by the data controller or the data processor as a main activity, and large-scale data processing is performed. It should be noted DPOs can be designated even though data controllers and data processors are not compelled by law. In this sense, the DPO's main role is to promote and supervise compliance with the personal data protection regulations.

With regards to security incidents and in contrast with current data protection regulations, the PDPB contains the obligation to notify incidents before the supervisory authority.

The PDPB introduces new principles related to data collection and data processing, such as

accountability and data minimization. Data controllers and data processors must adopt technical and organizational measures to ensure an adequate data processing and must collect and process only the personal data required for accomplishing the purpose of the collection or processing.

In addition, the PDPB foresees the extraterritorial applicability of the law, meaning the data protection provisions shall apply outside the Argentine Republic in certain cases.

It is thought the PDPB will be approved in 2020. The PDPB is based on the GDPR and, as such, its passage is important progress for the Argentine Republic.

Belgium

Tim van Canneyt, CIPP/E

Following the (belated) appointment of its directors in 2019, the Belgian Data Protection Authority will finally adopt its strategy for the next five years. A recently published draft version identified sectors like telecommunications, media, direct marketing and the public sector as priorities. Other focus points include the role of the data protection officer, rights of data subjects, online data protection and use of photos. In terms of enforcement, the Belgian DPA has increased the pace a little bit over the last six months in terms of the number of cases dealt with. Sanctions currently remain relatively lenient, ranging from a reprimand to a maximum fine of 15,000 euros. As the Belgian DPA is coming to grips with its new powers, it is possible we will see more enforcement in 2020. It will also be interesting to see whether sanctions will be confirmed in appeal, especially considering that two decisions were annulled by the Court of Appeal of Brussels, mostly for procedural reasons. Following the (belated) NIS Directive implementation into Belgian law, stakeholders are currently waiting for royal decrees that will formally designate the operators of essential services. With the federal government in "current affairs" mode and the coalition discussions for a new government seemingly not going anywhere at the moment, it is hard to predict when the royal decrees would be adopted.

Brazil

Renato Leite Monteiro, CIPP/E, CIPM, FIP

The Brazilian General Data Protection Law was approved in 2018 and will come into force August.

However, eight months is a long time, and a lot can happen before the law goes into effect. The national data protection authority still needs to be created and its five directors appointed by the president and approved by the senate. Once that happens, the directors need to create guidelines to support compliance efforts before the law goes into effect as several points still need clarification — both the controller and processor will need to appoint a data protection officer; flexible rules for small- to medium-size enterprises, startups and disruptive companies; and how to handle legacy databases.

There are already efforts to postpone the implementation of the LGPD. Despite the fact that such maneuvers are quite common in Brazil — lobbying by some sectors to change laws before their effects are felt — and even though there is no political will to achieve this objective, there is some anxiety in Brazil (and abroad) on how a postponement might impact when companies start their adequacy programs. However, that said, there is no reason to postpone the beginning of these projects.

Also, attempts to change certain aspects of the law are underway, regarding how penalties will be applied or elements of the right

to review automated decision making. As with the earlier arguments, waiting for changes is not necessary or advisable. This year will be exciting for data protection in Brazil, regardless of the scenarios that occur in the months to come.

Canada

Shaun Brown

The theme for this year is consultations and potentially more consultations. Don't expect any significant legislative change in 2020, but we could at least come away with a clearer picture of the changes to come.

Eyes will continue to be on the slow march toward revising the federal Personal Information Protection and Electronic Documents Act, which appears to be gaining momentum. The government has signaled a clear intention to make several changes that would bring PIPEDA more in line with the EU General Data Protection Regulation, including such things as data portability rights, rights to erasure, data security requirements and stronger enforcement powers for the privacy commissioner of Canada. This objective is reflected in a discussion paper published in May 2019, as well as the recently published mandate letter from the prime minister to the minister of innovation, science and industry. It's possible the government will engage in a formal consultation process in 2020 to seek feedback on options for legislative amendments.

The government has also been working toward modernizing the badly outdated Privacy Act that applies to the federal public sector. The government began "targeted stakeholder engagement" this past summer, with the goal to engage in broader consultations as more concrete proposals are developed.

Although we just went through a federal election, the Liberals emerged with a minority government only, and because minority governments typically last a few years at most, a cloud of uncertainty now hangs over the legislative process. Priorities can change quickly in such an environment. And, as the Liberals depend on the New Democratic Party to stay in power, the NDP are likely to have more sway over any reforms that do occur, who can be expected to advocate for more stringent privacy laws.

Chile

Oscar Molina, CIPM

From a legislative point of view, 2020 is likely to be centered on the constitutional discussion initiated in late 2019. Legislative priorities will likely be given to social security initiatives, such as reform to the pension system, education and health care.

However, once these priorities are addressed, there may be an opportunity to move forward regarding privacy and cybersecurity initiatives that saw some movement in Congress during 2019. There is a general perception that the data protection bill, which was approved last year by the Constitutional Committee of the Senate, is unlikely to be finalized in the upcoming year. However, this may change if the government acknowledges the data protection bill is a necessary reform that may contribute to the social agenda currently under discussion. Other initiatives, such as the bill that seeks to update the computer-related crime law, may show some progress in its approval next year as it does not entail additional public financial resources.

Sectoral norms that further detail requirements for incident reporting and information security standards in the banking and finan

cial services industry should move forward in 2020 as they are issued by the regulatory authority and do not require congressional approval. Finally, in October 2019, the government was about to introduce a bill establishing common rules and obligations for critical infrastructure in relation to cybersecurity. However, this was postponed and will not likely be under discussion in 2020.

China

Galaad Delval, CIPP/E, CIPM

As 2019 was marked by the creation of the Multi-Level Protection System 2.0, new Cryptography Law and first expert draft of the Personal Information Protection Law, privacy professionals may wonder what to expect in 2020 after such a regulatory bounty.

Foremost on the legislative side, we can expect the expert draft of the Personal Information Protection Law to be further revised before being submitted to the National People's Congress for review and to potentially become a bill in accordance with the 13th National People's Congress Standing Committee Legislative Plan. A first draft from the NPC would be a valuable document to assess what type of future there is for data protection in mainland China.

Updates on the draft regulations on the Protection of Security of Critical Information Infrastructure are likely to happen in 2020 in accordance with the State Council 2019 legislative work plan. Beyond mid-2020, it is recommended that companies review the State Council 2020 legislative work plan when available around May to see the next regulatory documents involving data protection or cybersecurity that are in the process of being drafted or finalized.

Concerning standards, it is expected the Personal Information Security Specification will be finalized in 2020 as it has already been through multiple drafts. Given it was first enforced in May 2018, such a swift update would demonstrate a strong appetite to improve the guidance of data protection practices in mainland China.

As for enforcement, immediate application for the Cryptography Law is expected in early 2020 as law enforcement begins Jan. 1. Following the late 2019 app infringement of users' rights and interests' campaign, apps disregarding data protection are expected to remain in the regulator's crosshairs for early 2020. Finally, MLPS 2.0 compliance is expected to take off as a main data protection and cybersecurity compliance obligation for all companies dealing with personal information and information systems.

Colombia

Juanita Ramirez Roa

This year is shaping up to be very interesting for data protection and privacy in Colombia. At the international level, the Superintendence of Industry and Commerce of Colombia has become a key player in building convergence of data protection and privacy standards.

Although Colombia ensures an adequate level of protection for personal data transferred from the EU to organizations in Colombia, we do not yet have adequate standing under the General Data Protection Regulation. Therefore, it is not an exaggeration to say that Colombia is ready to embark upon a new, modern and dynamic partnership with the European Union. This Colombia-EU partnership would be a powerful tool to facilitate data flow freely, while ensuring the level of protection for the data of individuals in the EU when it is transferred to Colombia.

Data transfer to third parties outside of Colombia is already regulated, but now is the

time for organizations to demonstrate, in accordance with the accountability principle, that data transfer operations are ensuring an adequate level of data protection equivalent to that ensured within Colombia.

The DPA wants to exercise its regulatory powers in a way that has the greatest effect on achieving the target outcome on consistent regulation. At the same time, it promotes the development of new technologies, innovation economies and businesses opportunities.

Cyprus

Maria Raphael, CIPP/E

Following Cyprus' application for accession to the Schengen area in July 2019, EU officials have assessed Cyprus' infrastructure and began their evaluation beginning with assessing the Office of the Cyprus Commissioner for Personal Data Protection to determine if it can exercise adequate supervision over systems and procedures that the public authorities have or must have to fully and correctly implement the Schengen Agreement.

Assuming Cyprus receives a positive assessment in the field of personal data, further evaluations will be carried out in 2020 in other areas. The main challenge in 2020 will be to coordinate and implement the best practices and recommendations drawn up at the European level in the Schengen field. Cyprus will need to balance its legislation with the legal instruments of the Schengen Information System, the largest information-sharing system for security and border management in Europe.

Highly anticipated legislation will implement the regulations on the Customs Information System composed of a central database accessible through terminals in EU member states. Cyprus must also begin efforts to achieve synchronization with the new EU Directive on "the protection of persons who report breaches of Union law," designed to enhance the protection of whistleblowers within the EU.

It is also expected that the amendments for the Protection of the Confidentiality of Private Communications (Surveillance of Telecommunications and Access to Recorded Content of Private Communication) will be enacted enabling the general attorney to request the court an order allowing the surveillance of private communication under terms and conditions, provided the surveillance is required for the interest of Cyprus' security or for the prevention, detection or prosecution of specific criminal offenses.

Lastly, the Right of Access to the Information of the Public Sector Law of 2017, regulating the right of access of the public to information possessed by public authorities, was amended and will come into effect in December.

Czech Republic

František Nonnemann, CIPP/E

The legal acts implementing EU General Data Protection Regulation and law enforcement directive in the Czech Republic went into effect in April 2019. Therefore, we do not expect any material changes at that level. One important change took place Jan. 1, when the Office for Personal Data Protection gained new competences in the appellation process in the freedom-of-information area.

We can also expect important legislative changes in some sectoral laws, including bank identification, e-health and personal data monetization.

There is not a commonly accepted electronic ID in the Czech Republic. The Czech Banking Association drives the concept of bank ID, in other words, the legal possibility to prove one's identity online via banking identification. Relevant amendments to the existing

law are in the Parliament and expected to go into effect in 2021.

Legal regulation of e-health is fragmented in the Czech Republic. This situation should be improved by a new law that is now before Parliament and would define the standards for electronic communication, establish rules for patient data sharing between different health care service providers and give patients online access to their personal documentation.

Another important legislative proposal is the draft amendment to the Civil Code that transposes two EU directives on customer protection. The government, among others, proposes explicit possibility for the end-users to pay by using their personal data for the digital content. The Office for Personal Data Protection has strongly criticized the proposal, which has not yet been submitted to the Parliament.

Denmark

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

With the Danish Data Protection Act in place since May 2018, the legislative focus in 2020 is on privacy implications from proposed criminal legislation.

One important piece of legislation to watch is the so-called "safety package," which was put forward in Parliament last year but canceled due to the general election for Parliament in June. The bill was expected to be reissued in January and features increased video surveillance in the public space to prevent and solve crimes.

There is some debate about this legislation as some argue surveillance gives less freedom for the individual while others say surveillance gives more freedom. The argument for the latter contends surveillance generates a feeling of safety and more security (given that it actually prevents crime). Hence, safety and security are fundamental requisites for freedom.

On the regulatory scene, we are still waiting for the first court rulings on fines. Datatilsynet, the data protection authority, cannot issue fines by itself, but they have submitted two cases to the police to start criminal proceedings on violations of the retention principle in the EU General Data Protection Regulation's Article 5(1)(e) for not deleting customer data. The fines proposed by the DPA are 160,000 euros and 200,000 euros, respectively.

Finally, the Danish DPA was the first to have a template data-processing agreement reviewed by the European Data Protection Board, which issued an opinion in July 2019. The Danish DPA issued a revised template based on the opinion at the end of 2019. The template is available in Danish and English.

France

Cécile Martin

In France, 2020 should mark another important stage concerning data privacy.

In the course of 2019, the French supervisory authority carried out important work, in particular, by sanctioning violations related to video surveillance and facial recognition and should be less and less lenient toward violations of the EU General Data Protection Regulation.

It has put in place an action plan to ensure the protection of voters' personal data in the face of political canvassing for the 2020 municipal elections. More specifically, the CNIL plans to implement a platform enabling voters to report abuses of political parties.

Its work will be even more scrutinized as the draft budget bill for 2020 provides for the

possibility for tax and customs administrations to collect and use personal data made public by users on social networks and electronic networking platforms. This data-mining tool aims at detecting and punishing tax fraud more effectively.

In a deliberation handed down on this project, the CNIL called for great caution and explained it was a "significant change of scale" in terms of the means available to these administrations. In particular, the CNIL warned of the risk that such processing could have on the freedom of expression of internet users and their right to privacy.

Germany

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

In November 2019, the Second EU Data Protection Adaptation and Implementation Act entered into force and is expected to achieve full impact in 2020. Besides aligning more than 153 domain specific laws with the EU Data Protection Standards, the new Federal Data Protection Act has been amended, including but not limited to the following points.

The threshold for common cases at which a data protection officer has to be appointed has been raised from 10 to 20 people who are permanently involved in processing personal data. A new derogation for the processing of special categories of personal data on the basis of compelling and material public interests will replace the need for consent in such cases. An electronic form is valid for consent in an employment relationship and written consent is no longer required.

Uncertainty surrounding the implementation of the ePrivacy Directive in Germany led to the case of the German company Planet 49 before the Court of Justice of the European Union in October 2019. These ambiguities have not been addressed by the Second EU Data Protection Adaptation and Implementation Act, and similar cases in this area may occur in 2020 until the long-awaited ePrivacy Regulation, hopefully, eliminates these ambiguities.

The Digital Healthcare Act is expected to enter into force in 2020 and is meant to foster apps on prescriptions, online video consultations and access to a secure health care data network for treatment everywhere.

It is uncertain if IT-Security Law 2.0, which has been under discussion since March 2019, will be adopted in 2020. Under the law, more industry sectors will be included in the consideration of critical infrastructures; general conditions are planned to be defined for certifications, seals and liability; and the role of the Federal Office for Information Security is planned to be extended.

Additionally, we expect the following initiatives of the supervisory authorities of Germany to gain full impact in 2020: a concept in the "Admeasurement of fines in proceedings against undertaking" harmonizing the categorization of undertakings, determination of their annual turnover and consideration of various levels of severity of deed and "Experience Gained in the Implementation of the GDPR" that proposes some adjustments of the EU General Data Protection Regulation that would streamline legal framework.

Greece

Antonios Broumas, CIPP/E

This year will find the Hellenic Data Protection Authority doubling the number of its investigators. As a result, the HDPA will be able to draw and execute a plan of sectoral investigations in high-risk or heavily data-dependent industries of the country. Taking into account its post–EU General Data Protection Regulation rulings, the HDPA holds strong opinions in core open issues of data

protection law, expects a high level of compliance by private and public entities, does not hesitate to impose sanctions as means of preventing or deterring violations and promoting compliance across markets. Boosted by new, fresh and highly specialized personnel, the authority is expected to increase the quantity and quality of its rulings and make headlines in the conduct of its powers much more often than in 2019.

In terms of regulation, the HDPA will continue to be less active than authorities in other member states due to its traditional abstinence from issuing guidelines and other soft law instruments. Nevertheless, in the beginning of 2020, the HDPA will issue its opinion on recent Greek Law no. 4624/2019, which supplemented the provisions of the GDPR. Such opinion was not requested during the relevant lawmaking process and is bound to point out legal discrepancies between Law no. 4624/2019 and the opening clauses of the GDPR, which may hopefully lead to corrective statutory amendments in the law, in 2020.

🇮🇳 India

Pranav Rai, CIPP/A

A key development to watch out for in 2020 will be India's new personal data protection law. The law will affect more than 1.3 billion citizens and residents of the world's most populous democracy.

The government has been working toward developing a comprehensive data protection law for many years, but really gained momentum in 2017 when the Supreme Court of India held privacy to be an inalienable and inherent fundamental right guaranteed under the constitution of India.

A committee was appointed to draft the new law, and in 2018, claimed the approach of its proposed law is a new "Fourth Way to privacy, autonomy and empowerment," which is distinct from the approaches of the U.S., EU and China.

The draft law was widely regarded as a modern data protection legislation but had its share of controversial provisions, such as nationalistic data localization requirements, wide discretion in the hands of the government and data protection authority to decide key matters, and broad exemptions in the interests of state security and criminal law enforcement. Many of these issues were brought to the attention of the government and a new draft was undertaken (see submissions from the EU and Professor Graham Greenleaf).

> ***On the whole, 2020 promises to be a year of privacy legislation in India and of wide-ranging public debates around the balancing of the resident's fundamental right to privacy with the economic and security interests of the state.***

The Personal Data Protection Bill, 2019 was introduced in the Parliament in December 2019. The PDPB is based on the committee's previous draft law but has a number of notable differences. However, the PDPB could not be tabled before the Indian Parliament amid protest from the opposition and was sent to a joint select committee of both houses of Parliament for further scrutiny. The committee is expected to submit its report before the end of the budget session of Parliament in 2020, and the law is then expected to be passed.

Additionally, the DNA Technology (Use and Application) Regulation Bill, 2019, which seeks to control the use of DNA technology for establishing the identity of a person, is expected to be passed in 2020. India is also

developing a nationwide facial-recognition system, potentially the world's biggest facial-recognition system, which may require a separate legislation.

The complex political and parliamentary system of India, however, requires taking legislative predictions with a pinch of salt. The non-passage of the PDPB was a surprise to many because of the Bharatiya Janata Party's inability to muster enough votes for PDPB passage in the upper house of the Parliament, where it lacks a clear majority. This happened only a few days after it pushed through tough and controversial bills in the same upper house.

On the whole, 2020 promises to be a year of privacy legislation in India and of wide-ranging public debates around the balancing of the resident's fundamental right to privacy with the economic and security interests of the state.

Ireland

Kate Colleary, CIPP/E

This year looks like it will be another busy one for privacy teams in Irish organizations and the Data Protection Commission.

Like many, we are awaiting the decision of the Court of Justice of the European Union in Case C311/18 CJEU (the "Schrems II case") on standard contractual clauses. Privacy pros may recall this case concerned a reference from the DPC to the CJEU raising a number of questions with regard to the validity of SCCs, a mechanism used to transfer data outside the European Economic Area. Advocate General Henrik General Saugmandsgaard Oe issued a non-binding opinion in December 2019 that the SCC mechanism remains valid. The CJEU will issue its opinion in 2020.

The DPC is also currently drafting a new Regulatory Strategy to cover the period of 2020 to 2025. The first consultation document on target outcomes was launched in December 2019 and is the first of two rounds of open public consultation as part of the development of the new Regulatory Strategy. The submissions received from the first round will be analyzed during the drafting of the Regulatory Strategy itself. The draft Regulatory Strategy is likely to be circulated in 2020 and further written submissions will be invited as part of the second round of public consultation. The DPC's aim is to ensure that it regulates with clear purpose — clear to the people whose rights they safeguard, clear to the organizations that they regulate, and clear to the DPC itself and to other regulators.

The DPC is also likely to issue the first administrative sanctions and/or fines under the EU General Data Protection Regulation early in 2020. While many expected the first of these to be delivered in 2019, the powers by which the DPC applies these measures were newly granted in the 2018 Data Protection Act and require certain statutory steps and public law principles to be followed. The DPC has adopted a cautious approach in utilizing these powers and indicated at the 2019 IAPP Congress in Brussels that any such findings must be robust and withstand appeals and judicial reviews.

Finally, next month brings an election in Ireland. The most recent polls indicate that the current government may have to enter a coalition with another party, if it is to remain in power. Either way, a ministerial shake up is likely following the election. Could this result in new roles for the Minister for Data Protection and the Minister for Business, Enterprise, and Innovation? If the latter is moved, it will be interesting in terms of the government's strategy in its litigation with the DPC over the Public Services Card.

Israel

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

A GDPR-like Israeli privacy law is not expected in 2020. However, efforts to enhance the Protection of Privacy Authority enforcement powers and amend the Protection of Privacy Law are still underway.

The new Credit Data Law has taken effect and will likely have a substantial impact on the Israeli market and consumers' privacy related to their financial information. The Ministry of Health introduced draft regulations for secondary uses of health-related data for research purposes, which steer a public debate over patients' privacy, anonymization techniques and information security. The Cyber Protection Bill's legislation process is undergoing. Most likely that bill will be enacted in 2020 and empower the National Cyber Security Directorate to have access to data, including personal information, on private companies' information systems.

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. Finally, privacy-related class-actions continue to be the dominant risk for companies who are doing business in Israel.

Italy

Rocco Panetta

Over the last couple of years, data protection became a regulatory hot topic across the globe. I believe this topic will become more entwined with other legislative and societal goals as time goes on — especially regarding sustainability and restrictions to unregulated technological development. Artificial intelligence, robotics and machine learning will be the trending topics of the year, as well as the diffusion of distributed ledger technologies, like blockchain. Ethics assessments should be on the agenda of both legislators, regulators, privacy professionals and academics.

As far as the Italian legal framework is concerned, it is important to keep in mind that it is still incomplete and uncertain regarding the processing of personal data relating to criminal convictions and offenses (judiciary data). Stakeholders are eager to read a long-awaited ministerial decree from Minister of Justice Alfonso Bonafede that should provide a list of authorized processing activities of similar data (e.g., Article 2-octies of the Italian Privacy Code).

The Italian Data Protection Authority will hopefully see the long-waited appointment of the new board. 2019 was a transitory year, both for the market and the DPA. I predict 2020 will be a year of massive enforcement and privacy pros should be prepared.

Japan

Gabor Gerencser, CIPP/E

In January 2019, the EU and Japan adopted decisions to acknowledge each other's data protection regime as an "adequate" level, thereby making data transfers between these jurisdictions subject to less paperwork.

However, the Personal Information Protection Commission of Japan proposed major amendments to the Japanese Act on the Protection of Personal Information aiming to further strengthen data subject rights in Japan. The additional regulations may have been triggered by Japan's biggest privacy scandal, which involved a job recruitment company selling data to its clients on the probability of graduating students declining job offers. The recruitment company gathered the data by analyzing students' browsing histories on a job information website.

According to the PPC's most recent announcement (in Japanese), the proposed amendments will include regulations on the provision of browsing data to third parties, strengthening data subject rights with respect to data access and erasures, the introduction of mandatory notification of data breaches, and tougher sanctions for APPI violations. These proposals will be drafted into a law on the agenda of the Japanese Diet during its 2020 ordinary session. It is possible the amended law will enter into force into 2020, but that will most likely happen during 2021.

🇱🇹 Lithuania

Natalija Bitiukova, CIPP/E, CIPM, FIP

In April 2019, I wrote the EU General Data Protection Regulation in Lithuania has generated, for various reasons, unprecedented attention for the data protection issues in Lithuania. The supervisory authorities have mostly focused on exercising their advisory and investigatory powers, including launching a series of ex-officio investigations and imposing the first GDPR-level fine in the country.

The general trend for 2020 is likely to continue toward increased enforcement of the law on Legal Protection of Personal Data with a possible closer focus on the financial, insurance and health care industries, which have not been thoroughly investigated yet. As Lithuania strives to become a European financial technology powerhouse, it will be interesting to see what approach the Lithuanian DPA will take toward the fintech industry and how it will ensure the effective collaboration with the financial regulators, especially in light of tensions between data protection and financial compliance requirements.

Based on the draft action plan for 2020 to 2022 recently released by the DPA, the authority is expecting to increase its limited human resources to focus on a more effective exercise of its powers. This will indeed be necessary as in addition to the local issues, the DPA will be grappling with the same pan-European challenges as its counterparts — international data transfers post-Brexit, effectively regulating cookies and pervasive tracking technologies (with or without ePrivacy Regulation), and finding its voice to meaningfully contribute to increasingly complex artificial intelligence and tech-related developments.

In addition, there is still unresolved tension between data protection and transparency values in the electoral context. New legislative measures are expected to be proposed to address the conflict; however, it is still unclear how the balancing of the competing rights will be ensured.

🇳🇱 Netherlands

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

The decisions rendered by the Dutch Data Protection Authority in 2019 will likely set the trend for legislative developments in the Netherlands. The key area being adequate security of personal data. In 2019, there were two notable decisions in that field. The AP imposed a fine of 460,000 euros, as well as administrative coercion up to 300,000 euros on the Haga hospital in The Hague due to insufficient security and inadequate access controls with regard to patient files. The AP also imposed an administrative coercion up to 900,000 euros on social security organization UWV for repeated insufficient security measures regarding its employer's portal.

Multifactor authentication is likely to become the prescriptive norm.

The Dutch Act on the Resolution of Mass Claims in Collective Action went into effect Jan. 1. Under the law, individuals can now claim damages as part of a class-action suit.

This may pave the way for class-action privacy suits seeking compensation for damages.

A record of processing activities is not required when processing of personal data is "occasional" (and the organization employs less than 250 persons, e.g., Article 30(5) of the EU General Data Protection Regulation). This open norm often leads to questions to what extent small- to medium-sized enterprises may rely on this exception. Certain clarification is likely to come in the form of guidance from the AP on this point.

Cybersecurity, internet of things, robotics and artificial intelligence remain hot items. While there is not specific legislation on these topics, it is anticipated there will be in the near future.

As a result of the implementation of the NIS Directive, there is already some cybersecurity legislation in place in the Netherlands. However, this law deals only with data breaches in so-called vital sectors, such as energy and drinking water.

The Netherlands GDPR implementation act became law at the same time the GDPR went into effect. We may see several amendments to the UAVG this year, specifically when it comes to special categories of personal data. For example, it is possible processing sensitive personal data may be allowed by accountants in the process of their auditing tasks. The same applies to the processing of biometric data to identify persons for rightful access to certain places, buildings and information systems (with a lower threshold than the current exception for security purposes).

New Zealand

Leah Parker, CIPM

Another year has passed without Privacy Law reform in New Zealand, which means the current Privacy Act blew out 26 candles on its birthday cake, along with the original "Jurassic Park" movie and the first World Wide Web software in the public domain.

The Privacy Bill, first introduced March 2018, aims to considerably amend NZ's Privacy Act and bring better alignment with international changes. The bill progressed through its second reading this year, resulting in clarification on its extraterritorial scope (if you are carrying out business in New Zealand, take note!) and the establishment of a serious harm threshold for mandatory notification of privacy breaches.

There is a lingering question as to whether these changes will go far enough to maintain NZ's EU Adequacy status — given that the changes do not include the additional data rights (i.e., right to be forgotten, data portability and algorithmic transparency) and the substantial punitive fines introduced in the EU General Data Protection Regulation. The shortcomings have been acknowledged by NZ Justice Minister Andrew Little, who has stated that "these issues can be considered as part of any future work on privacy reform." Will we lose adequacy? Will we enter a period of continuous reform? Only time will tell, so watch this space!

This Privacy Bill is now likely to take effect in mid-2020.

Nigeria

Ridwan Oloyede, CIPP/E

2019 was an exciting year for Nigeria's Data Protection space. The year saw the release of the Nigeria Data Protection Regulation by the National Information Development Agency. It also saw the rejection of the Digital Rights and Freedom Bill and the Nigeria Data Protection Bill by President Muhammadu Buhari. The coming year is poised to be more eventful, and these are some of the things to expect.

Enforcement action is expected from NITDA. The announcement of sanctions is also expected to deepen compliance. In July 2019, NITDA announced it is investigating some organizations for breach of the NDPR.

Buhari declined assent to the initial draft of the bill. There is currently a revised bill that has scaled the first reading pending before the House of Representative.

It is reported that the Central Bank of Nigeria is working on a draft Data Protection Regulation. This is a more sector-specific framework that will increase the compliance landscape for organizations.

It is expected that a new data protection bill will take wider consultation and remediate the inadequacies of the previous bill that was not assented to.

There is a possibility of sector-specific framework. The move by the Apex Bank to regulate data protection could possibly spur other regulators in to release their data protection regulation to specifically cater for their sector.

We expect to see some clarity regarding e-health policy. The Federal Ministry of Health spent time working on a proposed national e-health policy in 2019, and it is thought the policy will have implications on privacy in the sector. It is expected this will increase the compliance landscape for players in the industry in addition to the existing body of laws.

🇵🇱 Poland

Marcin Lewoszewski and Anna Koylanska

Last year was busy regarding data privacy legislation in Poland, particularly due to amendments made to about 160 legal acts, assuring compliance with the EU General Data Protection Regulation. It was also an election year in Poland, and the new Parliament discontinues any legislation that may have been in process, which can impact the legislative activity, so we don't expect to many changes in this field.

In 2020, however, we expect a few interesting court decisions related to data breach sanctions that were imposed based on GDPR violations, rights from Chapter III of the GDPR or data transfer agreements. We also expect 2020 to be marked by further progress in the field of cybersecurity, as a National Cybersecurity Strategy has been published in recent months, and a plan implementing its provisions is anticipated in 2020.

🇷🇸 Serbia

Aleksa Andjelkovic

2019 was a pivotal period for data protection and privacy in Serbia. The Personal Data Protection Law implementing the EU General Data Protection Regulation and transposing the Data Protection Directive for the police and criminal justice sector went into force Aug. 21, 2019. The election of the new commissioner for protection of personal data in July enabled more functional work of the National Assembly following the adoption of the new law. On Nov. 22, 2019, Serbia signed the protocol amending the Convention of the Council of Europe no. 108 further enhancing data protection regulatory framework.

If 2019 was the year of tectonic changes in data protection and privacy regulatory framework, 2020 is expected to be the year of implementation and activities aimed toward compliance with the new law.

At the end of 2019, there were numerous data protection compliance workshops organized by the commissioner and various privacy organizations aimed at both the public and privacy sectors. There was also an influx of requests made by companies related to

fulfilling the obligations of the new law and ensuring they are in compliance with the new regulatory framework. It is expected this trend will continue in 2020.

We should see the commissioner taking a more proactive role in a number of ways. There should be increased education of both the public authorities and the business community regarding their obligations arising from the new law. The commissioner should also propose relevant bylaws, supervising and fining for the breaches of the new law.

Singapore

Pranav Rai, CIPP/A

Singapore's privacy landscape is set to see two significant changes in 2020.

First, the Personal Data Protection Commission is considering introducing data portability and data innovation provisions to the Personal Data Protection Act 2012. The proposal results from the issuance of a public consultation and the PDPC's ongoing review of the PDPA. The proposal aligns with the PDPA's earlier pro-business approach and attempts to harmonize the EU General Data Protection Regulation and PDPA to enable data transfers.

Recognizing that data portability has been introduced by several jurisdictions, including the EU, and many countries, such as India, Japan, New Zealand and the U.S. (California), are also considering the right to data portability, the PDPC is considering adding the data portability to the PDPC.

The provision would also promote business innovation and protect individuals who develop and introduce innovative products to the marketplace first. Under the proposal, organizations will be able to use personal data for relevant business purposes without user consent.

Second, until now Singapore's public sector has been outside the purview of the PDPA. However, personal data protection systems in the public sector are set for an overhaul after two major data breaches (see SingHealth cyberattack and HIV data breach) made headlines in 2019. Singapore's government has confirmed it will implement new security measures across public sector systems by the end of 2023 in a bid to protect personal data. One specific recommendation would make third-party suppliers subject to PDPA regulations for the first time, with penalties up to SG$f1 million for misuse of personal data.

Sweden

Sofia Edvardsen, CIPP/E

The Swedish government has laid the groundwork for modern data protection over the last few years. The Swedish Data Protection Authority received increased funding and the government presented the first strategy for information and cybersecurity for 2019 to 2022. During the spring of 2020, it is expected Parliament will create a new government agency for cybersecurity.

Law enforcement agencies will have greater use of video surveillance. Beginning Jan. 1, law enforcement does not need to seek approval from the DPA to use the technology.

The U.S. Clarifying Lawful Overseas Use of Data Act sparked an intense debate in Sweden last year over the question if public authorities could or should, outsource their IT operations or use public cloud services, which might have to provide access to data from U.S. law enforcement, if requested. A cluster of government agencies took the stance that they should not use suppliers subject to the CLOUD Act at all. Other agencies have taken a less absolutist approach and are deciding on a case-by-case basis. A report detailing the mapping and analysis of the Swedish govern-

ment and its agencies' IT operations and legal preconditions is expected in mid-2020.

In the privacy field, many of the data protection authority's investigations are coming to a close. At the end of 2019, there were 45 pending investigations, the oldest of which is from June 8, 2018. Several of the investigations are running behind schedule, primarily due to heavy workloads and complex investigations. We are waiting for several decisions involving administrative sanctions in early 2020.

Switzerland

Stéphane Droxler, CIPP/E, CIPM

The revision of the data protection law has been approved by both houses of Parliament, and the final vote for passage will likely be on the agenda for the 2020 spring session. While the delay is disappointing, it is welcome news that the Council of States reconsidered the amendments proposed by the National Council to more closely align with the Federal Council's version of the bill. Half a victory while waiting for the next step.

In May, the European Commission will give its verdict on whether to maintain Switzerland's adequacy status. It will be interesting to see if the signing of Convention 108+ in November, along with the current revision of the Swiss Data Protection Act will allow Switzerland to maintain adequacy. Even if both the Swiss and EU General Data Protection Regulation come close in broad outline, a significant gap remains with regards to the sanction regime. The very limited powers of the federal data protection officer, as well as the low fines intended, could be considered ineffective by the commission.

Turkey

Furkan Güven Taştan

In 2019, the Turkish Data Protection Authority provided data controllers with nine resolutions and clarified 28 individual acts in a wide range of sectors from telecommunications to health. These decisions have pushed the private sector to act, but the public sector has not yet reached the desired level of compliance.

To meet the EU visa liberalization process, it is predicted the DPA will launch a legislative process limiting the exceptions of explicit consent this year. Moreover, it is expected to make arrangements for the protection of personal data with the Human Rights Action Plan, which is being prepared by the Ministry of Justice.

In 2019, the Constitutional Court annulled the provision that requires an individual "to have security clearance and archive research check" before entering public office because it does not comply with Article 20 of the Constitution (regulates the right to protection of personal data). One of the 2020 agenda items is to reenact this provision by determining safeguards and fundamental principles of processing of personal data.

Turkey was one of the first countries to adapt the second Payment Services Directive with Law No. 7192, which was published in 2019. The law authorizes the Central Bank to determine the principles and procedures of personal data sharing within the scope of open banking services and goes into effect in 2020.

According to the recent DPA decision about the extension periods for registration to the Data Controllers' Registry, data controllers

both in country and abroad are expected to enroll in the registry this year. It is also expected the DPA will publish a safe country list as part of the transfer of personal data abroad. Apart from this regulation, the DPA will certainly publish more guidelines to help companies and offer better protection to citizens.

UK

John Bowman, CIPP/E, CIPM, FIP

The general election held Dec. 12, 2019, marks a significant turning point for data protection in the United Kingdom. Given the large parliamentary majority held by the Conservative government, the U.K. exited the European Union Jan. 31. The U.K. will no longer participate in the institutions of the EU, including the European Parliament and the Council. Similarly, the U.K. Information Commissioner's Office will no longer have a permanent seat at the European Data Protection Board. However, it is envisaged that during the Brexit transition period, which is expected to end Dec. 31 (although it may be extended for one or two years by agreement), the Information Commissioner's Office can attend European Data Protection Board as an observer when there are deliberations on ICO-led one-stop-shop cases.

After the end of the transition period though, the amended rules of procedure of the EDPB appear to preclude the U.K. from attending EDPB. Those amended rules, published Dec. 2, 2019, include a new condition that observer status can only be granted to countries in the process of acceding to the EU. This would exclude the U.K. from further deliberations once the transition period is over unless alternative arrangements can be agreed.

In terms of applicable law in the U.K., the EU General Data Protection Regulation will be replaced by the U.K. GDPR at the end of the transition period. However, from the date of exit, the European Commission and U.K. government will seek to negotiate an adequacy decision by the end of the transition period. Both sides have made a political commitment to doing this in the political declaration on the future relationship between the EU and the U.K. The main issue though is whether an adequacy decision can be made within 11 months if there is no further extension to the transition period. This would be a record time to conclude an adequacy decision but both sides have acknowledged the importance of reaching an agreement. It remains to be seen how smoothly the negotiations will proceed though, particularly if issues such as data processing for national security purposes become a matter of contention.

US—federal law

Michelle Clarke

In 2019, there was a flurry of activity toward a federal privacy law in the U.S., some would say was spurred by the impending California Consumer Privacy Act that went into effect Jan. 1. There were calls from a number of camps for a federal privacy law from a number of camps, including big tech and privacy advocates, some calling for preemption while other argued the California Consumer Privacy Act or EU General Data Protection Regulation should serve as a guideline. Shortly before the end of 2019, two separate comprehensive federal privacy laws were introduced in the Senate. IAPP Senior Westin Fellow Müge Fazlioglu, CIPP/E, CIPP/US, broke down the differences and similarities in the white paper "COPRA and CDPA: Similarities, Gray Areas and Differences." Until a federal law is in place, expect more individual states to work towards creating their own data privacy laws. Check with the US Federal & State Privacy Watch page in the IAPP Resource Center for the latest information.

US—health care

Kirk Nahra, CIPP/US

Health care privacy has been in the news a lot lately, as enforcement from the Office for Civil Rights heats up. OCR explores meaningful Health Insurance Portability and Accountability Act changes through the rulemaking process (potentially), and tech companies and others are moving into the traditional health care industry space. There is still a lot of confusion about how the HIPAA rules apply and to whom they apply, in a growing range of solutions where health care data is being created and analyzed outside of the scope of HIPAA rules.

The key issue in the federal privacy debate for health care will be how the health care industry will be treated under a new federal law, if we are to see one. Many of the bills carve out those entities currently regulated by HIPAA. Other bills simply create new obligations across the board and impose them on top of existing laws, such as HIPAA. At the same time, the health care industry — broadly defined — is struggling with the implications of today's regulatory structure where there are different rules for different parts of the health care industry. In California, for example, there now are three categories of health care companies (four, if you include employers). There are HIPAA-regulated entities (covered entities and business associates), companies regulated by the California Confidentiality of Medical Information Act and then those companies now regulated by the California Consumer Privacy Act.

We will be watching — and the industry should be thinking about — whether this fragmented system is a good means of protecting privacy and operating the health care industry going forward, both for consumers and industry. HIPAA works well where it applies, but the challenge is to make it fit an evolving structure that isn't solely dependent on health care providers and health plans.

Zimbabwe

Kuda Hove

The Access to Information and Protection of Privacy Act is the main Zimbabwean law that deals with privacy, as well as data protection. In 2019, the government conceded that most of AIPPA is unconstitutional and announced it was repealing the law and replacing it with the Protection of Personal Information Law and two laws that will regulate access to information and the regulation of the media sector respectively. There is no word or timeline on when the Protection of Personal Information law will be drafted or gazetted.

The Freedom of Information Bill is currently before Parliament and, if passed, would repeal AIPPA in its entirety, including the sections relating to privacy. If this bill is passed into law before the proposed Protection of Personal Information Law, Zimbabwe will have no legislation regulating privacy or data protection.

In October 2019, the Zimbabwean government announced that Cabinet had approved drafting principles for the Cyber Crime, Cyber Security & Data Protection Bill.

This consolidated law regulates three spheres of information technology law, including data protection. No versions of this draft law are in the public domain, but the law would seek to establish a national data center, a national data authority and regulate the transborder flow of data. The government has made similar announcements in the past without anything come to fruition.

Zimbabwe will most likely continue without any adequate privacy and data protection laws as these seem to be at the bottom of the current government's list of priorities.