2019 Global Legislative Predictions

Emily Leach, CIPP/E, CIPP/US

iapp

What will the new year bring in privacy and data protection legislation? Well, to name just a few highlights, we've got a handful of EU member states still needing to pass laws addressing the General Data Protection Regulation, India is in the midst of debate over a new law, Brazil's law will get the enforcement body it has been lacking, and there are talks of a U.S. federal privacy law. But that's just the tip of the iceberg. This week's Privacy Tracker roundup consists of contributions from IAPP members across the globe outlining their expectations (and occasionally their hopes) for privacy legislation in the coming year. With more than 30 contributions, this year's global legislative predictions issue is our most comprehensive yet.

Argentina

By Pablo Palazzi

The year 2019 will see Argentina with an important landmark in its history of data protection law. In September 2018 the government sent to congress the data protection bill, based on the EU General Data Protection Regulation. Now it is up to Congress (first the Senate, then the House of Representantes) to openly debate the bill and approve it. Argentina was the first country in Latin America to adopt a full fledged EU data protection law and the first country to be considered adequate by the EU. Now, nearly 20 years later Argentina has again the chance to follow EU law again.

Belgium

By Tim Van Canneyt, CIPP/E

2019 will be another important year for data protection in Belgium. First, we should finally see the appointment of the directors of the new data protection authority. At the moment, Belgium has an interim supervisory authority which is pretty much forced to act on a day-to-day management basis. When the directors of the DPA are appointed in 2019, the authority will be able to adopt its strategic vision, publish more guidelines to help companies and offer better protection to citizens. In addition, we should hopefully see the implementation of the NIS Directive into national law. Furthermore, the Belgian Supreme Court will have to assess the lawfulness of the recent government decision obliging every Belgian resident to provide their fingerprints for inclusion on the ID card's chip. Finally, it will be interesting to follow the class action brought against Facebook by consumer protection body TestAankoop.

Brazil

By Renato Leite Monteiro, CIPP/E, CIPM

2019: The year of compliance and the Brazilian Data Protection Authority!

What a year! Nobody could guess in the beginning of 2018 that Brazil would finally have its own General Data Protection Law, known as LGPD (I myself have written this column for the last three years and I always

thought my predictions were only in a wild guess!). And then, out of the blue, it was approved in August. However, the president vetoed one of its pillars: the creation of the national data protection authority. Even though some provisions would only have an effect if the authority was created. This lack of DPA made the LGPD weak.

Then, on the dawn of the year, Dec. 28, 2018, the Executive Order n° 869/18 promoted several alterations to the law. One of the most important was the creation of the Brazilian National Data Protection Authority. It is also altered the vacatio legis period for the LGPD to 24 months, changing the enforcement date from February 2020 to August 2020. During this period, the ANPD must exercise collaborative and consultative functions, aiming to provide assistance in the process of compliance to the new law. With the creation of the DPA, business will know to whom and what to look for. They will have a straight channel to communicate. The ANPD will provide for a much more stable application of the law, and, for instance, more legal certainty, what will probably spur technological and economic development.

Nonetheless, despite the DPA, enforcement actions might continue. The Distrito Federal and Territories Public Prosecution Office has been heavily conducting investigations on data breaches and other issues regarding personal data. Recently, the Minas Gerais Public Prosecution Office fined a drugstore chain for exchanging customers' personal Taxpayer Id numbers for discounts in products, which in fact is a common practice in Brazil. The total amount of the fine was R$ 7,930.801.72 (BRL), the largest related to data protection yet. This condemnation was vastly reported in mainstream media, national and international. Such actions are likely to continue.

Also, since LGPD will enter into force in August 2020, 2019 will be year companies will rush to become compliant, a practice that has already become a new niche market. Consulting companies and law firms are heavily investing in personnel and privacy software to take advantage of the escalating demand. Proof is that the IAPP has partnered with the first official training center of Brazil. Data Privacy Brasil will provide training courses for both CIPP/E and CIPM certifications.

Therefore, we can say that 2019 will be an interesting year for the data protection scenario in Brazil!

Canada

By Shaun Brown

The Minister of Public Safety announced in an interview last month that new cybersecurity legislation will be introduced this year. No details are provided on what this bill would include, but it may be related to recommendations made by the Senate Standing Committee on Banking, Trade and Commerce in a report entitled Cyber assault: It should keep you up at night, published last October.

Of course, in an election year (currently scheduled for October), the already glacial pace of law-making tends to slow even more, so it is practically impossible that anything would be passed. However, this could be the beginning of something significant.

It's also worth noting that the void in legislative activity will continue to be filled with regulatory guidance. The Office of the Privacy Commissioner began applying its Guidelines for Obtaining Meaningful Consent as of Jan. 1. Also, businesses are still digesting guidelines introduced late

last year by the Canadian Radio-television and Telecommunications Commission that would make service providers liable under Canada's Anti-Spam Legislation for activities that are neither within their control or knowledge.

Chile

By Oscar Molina, CIPM

This year is likely to be a period of clear advancement in various legislative initiatives concerning privacy and cybersecurity in Chile. The authorities have finally given proper attention to a series of legal initiatives included in the National Cybersecurity Policy issued in 2017, perhaps in response to the various cybersecurity incidents reported in the past year. As a result, it is likely that by mid-year Congress should approve the reform to our Data Protection Law, which will raise our current norms to a standard closer to the GDPR. In addition, the bill that seeks to update the computer-related crime law is likely to move forward in its discussion in Congress.

A General Cybersecurity Bill, aimed at consolidating the institutional framework and incident management related with information security throughout the country in both the public and private sectors, is likely to be forwarded to Congress for discussion. Sectoral norms, issued by the respective regulatory authority in relation to banking and financial services, which detail additional requirements for incident reporting in this industry, should also see substantial progress.

Finally, although one of the immediate objectives of the NCP is to issue a law establishing common rules and obligations for critical infrastructures in Chile, given the complexity of the task to several industries and stakeholders involved, it is unlikely that there will be any relevant developments.

China

By Galaad Delval, CIPP/E

With 2018 marked by the finalization of the E-commerce Law, 2019 could be marked by further progress on cybersecurity. First, a second draft or a final version of the Regulations on Cybersecurity Multi-level Protection System is expected this year from the Ministry of Public Security. It would likely be preceded by a new draft or final version of the Guidelines for Grading of Cybersecurity Multi-level Protection System by the National Information Security Standardization Technical Committee. Together, they would provide Article 21 of the Cybersecurity Law with a renewed framework for networks to comply with, which would impact all companies operating in Mainland China. We can also expect for 2019 to know more about the Guideline for Internet Personal Information Security Protection, how it will impact personal information lifecycle processes and how it will be implemented across Mainland China. 2019 should also bring more progress on how the new Multi-Level Protection System will be implemented on an industry basis. For example, either the People's Bank of China or the China Banking and Insurance Regulatory Commission could release, in late 2019, a notice or guideline on the implementation of the new MLPS framework for banking institution. Finally, further information on the Social Credit Score implementation (both locally and nationally) are likely before its expected official launch on 2020.

Colombia

By Luis Alberto Montezuma, CIPP/C, CIPP/E, CIPP/US, CIPM, FIP

2019 most certainly promises to be an exciting year for data protection in Colombia.

The Superintendence of Industry and Commerce of Colombia, or SIC, has appointed Nelson Remolina Angarita as chair of Colombia's Data Protection Authority (Superintendent Delegate for the Protection of Personal Data).

In his first decision, Chair Remolina stressed that the accountability principle requires organizations to put in place procedures, practices, and measures that effectively protect personal data, rather than simply writing ineffective policies that fail to protect.

In his speech commemorating the 50th anniversary of the Superintendence of Industry and Commerce, Chair Remolina also called on the importance of strong international relationships particularly in the context of trans-border data flows between the European Union and Colombia. Colombia aspires to obtain an adequacy decision from the European Commission.

Following in the footsteps of Argentina, Mexico and Uruguay, Colombia also hopes to join the "Convention 108" and its Additional Protocol soon. The Convention will support Colombia with strategies and best practices to facilitate the flow of data across borders while providing effective safeguards when personal data are used.

Finally, the obligation to register the databases by public authorities before the National Database Registry of the Superintendence of Industry and Commerce will continue in 2019.

Cyprus

By Maria Raphael, CIPP/E

The drafting of this text coincides with the Cyprus Commissioner's 2017 annual report, submitted to the President of the Republic of Cyprus Dec. 18, 2018. It is anticipated that in 2019 the commissioner's activities will be intensified and that the Cyprus GDPR implementation law in regards to derogations will be enriched.

Dec. 22, 2018, the Right of Access to the Documents of the Public Sector Law, enacted back in December 2017, came into effect establishing and regulating the right of access of the public to information possessed by public authorities with the exception that such right does not exist where the access request concerns personal data either of the applicant or a third person.

The law does mention that, in the latter case, the Processing of Personal Data (Individuals' Protection) Law is applicable, however, this law has been abolished and Cyprus's GDPR implementation law specifically provides that personal data in official documents possessed by a public authority for the purposes of performing a duty for the public interest are disclosed, subject to the provisions of the Right of Access to the Documents of the Public Sector Law. It remains to be seen how this law will be applied within 2019 and if further legislative interventions will be required in order to safeguard the proper exercise of the right of access.

As the proposed ePrivacy Regulation is likely to come into force in 2019, it is reasonable to expect major legislative harmonizing efforts with the active support and advice of the commissioner.

Czech Republic

By František Nonnemann, CIPP/E, and Zuzana Radicova, CIPP/E

The GDPR implementing laws are the most expected pieces of legislation for privacy professionals in the Czech Republic.

The lower chamber of Czech Parliament adopted the new Act on Personal Data Processing and complementing acts changing other laws at the end of 2018. The upper chamber, Senate, is supposed to discuss the laws in the beginning of 2019.

These new acts do not introduce many of the derogations possible under GDPR. Main changes compared to the previous legal framework are:

- Legal age for online consent is set to 15 years.
- Possible fines for small municipalities are decreased to 15.000 CZK (app. 600 EUR).
- Personal data processing for journalistic purposes are exempted from some obligations.
- Changes in the supervisory body structure (strengthen the monocratic character).
- Exemption from the obligation to run data processing impact assessment and test of purpose compatibility when processing data on the basis of specific legal act.

As soon as the implementing acts are approved, further legislative changes will follow, e.g., in the area of health care registers, credit bureaus, etc. At this moment, no detailed draft of such further legislation is available.

Denmark

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

With The Danish Data Protection Act in place since May 2018, no new privacy legislation is expected before the ePrivacy Regulation will be passed in the EU system — which may result in amendments to the Danish Marketing Practices Act.

The focus in 2019 is on criminal legislation, which also raises privacy issues.

With effect from Jan. 1, the criminal code has been amended to raise sanctions for certain privacy violations — especially with focus on online offenses, e.g. sharing of nude pictures and video — and hacking. Further, tracking other people with GPS has now been criminalized — which was not the case before. Now only the police may track people by GPS when investigating serious crimes.

A new policy entity has been formed to handle airlines' passenger lists for all flights which will be kept by the police for five years.

Further legislation is expected in 2019 on the follow issues:

- Telcos' logging of tele- and internet traffic for investigation and prosecution purposes (as necessary to follow the ECJ rulings in cases C-203/15 and C-698/15).
- Strengthening the police's possibilities to investigate internet crimes, e.g. by using civil agents.
- Wider possibilities for both public and private organizations to use video surveillance and to give police access to surveillance files to investigate very serious crimes.

Germany

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

Germany delivered the first EU Data Protection Adaption and Implementation Act in mid-2017, and a draft of a second EU Data Protection Adaption and Implementation Act is now available that will enhance the new Federal Data Protection Act and align 153 more national laws with the EU Data Protection Standards. It is likely that the draft will undergo further changes in the legislative procedure during 2019.

Additional changes in the legal and regulatory framework in Germany may originate from the long term Data Protection Agenda of the German Government (stay tuned for an upcoming Privacy Tracker post with more on the government's agenda) including but not limited to the enhancement of the Online Access Act (Onlinezugangsgesetz) in the area of eGovernment and the Passenger Transport Act (Personenbeförderungsgesetz) in the area of autonomous driving. eHealth and ePrivacy, Employee data protection, data protection by design and by default, and ethics and innovation represent further areas of interest.

With regard to the latter, artificial intelligence in particular is considered a hot topic which is strongly reflected by the fact that the German government has adopted an Artificial Intelligence Strategy and established a Data Ethics Commission, which will begin public discussions in May.

Finally, the office of the Federal Data Protection Commissioner in Germany will be taken over beginning of 2019 by Ulrich Kelber who, most notably, is not a lawyer but a computer scientist, which may indicate a new way of coping with the challenges around digital transformation and data protection by design.

Greece

By Olga Tzortzatou

The Greek draft regulation (in Greek), which will transpose the GDPR into national law has been drafted and was open to public consultation until 05/03/2018. The proposed legislation favors EU-wide harmonization as much as possible and contains in total 72 articles which also implement the Directive (EU) 2016/680 "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data." In order to ensure the independence of its activities, the Greek data protection authority has requested for human and technical resources to be provided by the state, according the GDPR's Article 52(4), as stated at the annual DPA activity report, which was submitted on 03/01/2019. (Text in Greek can be found here.).

Hong Kong

By Paolo Sbuttoni

There are no specific legislative changes to the privacy law tabled for Hong Kong. While there has been speculation and calls for a change given the recent high profile data breaches, nothing concrete has come about from them. We are currently in a period of watching the space for potential developments.

India

By Pranav Rai, CIPP/A

2019 is expected to be an exciting and important year for privacy in India, as the much-anticipated new data protection legislation may soon become a reality.

The existing data protection rules have severe deficiencies and also have a non-functional enforcement system. This lack of a robust data protection law not only affected the human rights of the residents of the most populous democracy but also impeded its trade with Europe. Thus, for some time now, efforts have been made by the government to develop a comprehensive data protection law.

While the draft law is a modern data protection legislation, it has its share of controversial issues. Many such issues were brought to the notice of the government. Submission from the EU, for example, was critical of certain provisions. Perhaps with a view to resolve these issues, the government intends to have a wider consultation on the draft law before introducing it in the Parliament.

On another front, Jan. 2, 2019, the government introduced in the Parliament the Aadhar amendment law. The goal of the Aadhaar project is to ensure targeted delivery of benefits, services and subsidies by the government through digital identification; howver, it was later made compulsory for many other purposes such as linkage to bank accounts and cellphone numbers. While the government claims that the amendments are being done keeping the Supreme Court's Aadhaar judgement in mind, critics and privacy advocates suggest that some of these amendments are in contravention of the Aadhaar judgement.

There is some uncertainty as to the timing for the passage of these laws in the Parliament since the current government has majority only in the lower house of Parliament, and to become a law the draft law has to be passed in both the houses. All that can be said for now is that, although it is theoretically possible that Parliament may pass these laws this month, the probability of them passing after general elections in March-April 2019 is much higher as the political dynamics will then change.

Ireland

By Kate Colleary, CIPP/E, & Natasha O'Reilly

GDPR implementation did not signal the end of legislative activity in the Irish data protection landscape in 2018. A number of subsequent pieces of legislation have either been enacted or are currently making their way through the legislative process and will be enacted in 2019.

The Minister for Health enacted the Health Research Regulations (The Data Protection Act 2018 (Section 36(2)) (Health Research Regulations 2018 (SI No.314/2018)) in August 2018. These regulations prescribe the "suitable and specific measures" that must be taken by data controllers to safeguard the rights of data subjects in the context of health research. Among the measures to be taken when processing personal data for the purpose of conducting health research is a requirement to obtain the explicit consent of the data subject in advance of commencing the health research (with a transition period to April 30, 2019, afforded to research commenced before the enactment of these regulations).

Draft legislation providing for the sharing and reuse of personal data between Irish government bodies is also currently

making its way through the Oireachtas. The Data Sharing and Governance Bill 2018 is currently at Report Stage which means it is nearing the end of the legislative process and will likely be enacted in early 2019. This legislation aims to provide a general legal basis (per GDPR requirements) for the sharing of information between public bodies where no other Irish or EU law provides a basis for such sharing. However, this draft legislation has been heavily criticized for issues around the use of a "public service identity" and for failing to implement principles of transparency, necessity and proportionality. It will therefore be interesting to see the final text of this legislation once enacted.

The Data Protection Commission is also likely to be busy in 2019 as the lead supervisory authority for many large social media and tech companies. There are currently 14 live cross-border investigations being conducted by the DPC which are likely to conclude in 2019. We also await the first administrative fines, which may also be levied in 2019.

Israel

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

The biggest question for 2019 is whether the Knesset (the Israeli Parliament) will enact a bill to amend the Protection of Privacy Act, which will increase dramatically the Protection of Privacy Authority's enforcement powers. The bill has already passed the first legislative procedure and awaits further hearings by the Constitutional Committee. If enacted, the PPA will have the power to impose fines up to NIS 6.4 million (approximately USD 1.8 million) including personal fines on company managements.

We also witness an increase in the number of privacy-related class actions, including against foreign companies who provide their services to Israeli consumers. Class-actions are currently, and will likely remain, the biggest risk for companies in terms of consumers' privacy. Cybersecurity continues to play a major role. Companies are gradually adapting to the onerous requirements under the newly enacted Protection of Privacy (Data Security) Regulations. Additionally, the new Cyber Law bill, which is likely to come in to effect in 2019, introduces new data sharing procedures for cyber defense purposes, which raise privacy concerns.

Italy

By Rocco Panetta

As May 25, 2018, slowly arrived and then suddenly passed, it appears that Italy and the rest of EU's member states have taken the final steps on national data protection regulations. Italy finally has its national law, approved Sept.19, 2018, with the aim to regulate the implementation of the GDPR in the Italian legal framework.

Will 2019 be a smooth year from a data protection perspective? Clear signals seem to suggest it will not. Concrete differences in national implementation laws could entail possible — and highly significant — divergences with regards to the protection of rights and freedoms of data subjects at EU level, potentially undermining the true spirit of uniformity, embodied in the regulation tool. In this sense, DPAs — and the Garante (the Italian DPA) is surely at the forefront in this respect — will have to assure a consistent implementation of data protection law in each member state, as well as at EU level.

Furthermore, the e-Privacy Regulation is expected to be approved in 2019. "GDPR's small sister" will require companies that operate on the Italian market as well as public institutions to further work in order to comply with this new set of rules, circumstance which might lead to a second disruptive wave of self-declaring privacy professionals and consultants.

Lithuania

By Natalija Bitiukova, CIPP/E

In July 2018, I wrote that Lithuania adopted the new Law on Legal Protection of Personal Data, and we were expecting the supervisory authorities to come up with the rules and guidelines for data controllers and processors. Some of the guidance (e.g., on the personal breach notification, the appointment of a DPO) was indeed released, and it is likely that we will see more in 2019. In particular, now, controllers should be on the outlook for a final list of processing operations requiring a DPIA.

The general trend for 2019 is likely toward increased enforcement of the new law, including ex officio investigations by the national DPA and the first GDPR-level fines. Some of the enforcement actions may be expected in the area of data processing in the electoral context as three different elections will be organized in Lithuania in the first half of 2019.

Outside the GDPR domain, the revised legislative package implementing the Cybersecurity Law and transposing the NIS Directive came into effect Jan. 1, and we can expect further actions in this area. There is also pending draft legislation related to AML and disclosure in state-owned enterprises, which imposes stricter transparency and data (including personal data) disclosure obligations. As we have already witnessed in 2018, this may lead to increased tensions between the right to data protection and a right to information in Lithuania.

Luxembourg

By Mélanie Gagnon, CIPP/E, CIPM, & Sarra Soltani, CIPP/E

In Luxembourg, several draft laws related to data protection have been tabled in the Chamber of Deputies in 2018. For example, the draft law on the limitation of the scope of certain rights and obligations under the GDPR in the financial and insurance sector.

There are also some draft laws in the public sector that will have an impact on data protection, such as the draft law on municipal administrative sanctions and the law on housing subsidies.

It should also be mentioned that several draft Grand Ducal Regulations on Health will certainly have some impact on the processing of health data (1,2,3).

In addition, the Luxembourg's data protection authority will publish the list of processing activities for which a DPIA is mandatory and the certification scheme for the processing of personal data "GDPR Certified Insurance-Based Processing Activities (GDPR-CARPA)." This certification scheme would be the first of this kind in Europe.

Mexico

By Rosa M. Franco Velázquez, CIPP/US

It seems that 2019 will be a year of continuous development of privacy and data protection matters in Mexico, and we hope for more recognition and commitment of our authorities, at all levels of government,

to the importance of privacy and data protection as a fundamental right. Example of the commitment of the data protection authority (INAI, for its Spanish acronym) is the adherence of Mexico to Convention 108, in June, 2018, and the amendments which will be required to be undertaken in particular regarding the private sector, as to comply with the recommendations of the Council of Europe. Another important fact that will keep our DPA busy for the coming year will be the preparation to host the International Conference of Data Protection and Privacy Commissioners in 2020, which has been known to be the "premier global forum for data protection authorities for nearly 4 decades."

During 2018, and in compliance with its responsibility to issue opinions and recommendations in accordance with the applicable provisions of the Federal Law on the Protection of Personal Data held by Private Parties, the INAI published, among others, "The Minimum Criteria suggested for the Contracting of Cloud Computing Services when involving the processing of personal data"; "Recommendations for the handling of Personal Data Security Incidents" and "The Guide for processing Biometric Data," this type of guidance shall be expected to continue in 2019.

The Netherlands

By Abraham Mouritz, CIPP/E, CIPM, FIP

The Dutch bill implementing the GDPR into Dutch national law, the UAVG, became effective on the same date as the GDPR. The Dutch deviations from the GDPR can be found as part of the IAPP's "EU Member State GDPR Derogation Implementation Tracker."

Per Jan. 1, EC Directive 2016/680 has been implemented in various Dutch laws and royal decrees with regard to the processing of personal data by Dutch investigation and prosecuting authorities. New Dutch legislation is also expected as a result of the ePrivacy Regulation taking effect and the implementation of the European Electronic Communications Code down the road.

New or more stringent legislation may also follow as a result of some of the recent decisions made by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). The AP has clearly become more active, and it is interesting to see that the AP has become very critical particularly of government organizations as illustrated by below examples:

- The AP found the National Police does not protect police information well enough against unauthorized disclosure and use. If the National Police has not implemented appropriate improvements to its security measures by 4 Feb. 4 it may forfeit fines of up to €320,000.

- The AP has ordered the Dutch Employee Insurance Agency to implement more appropriate security measures, most notably with regard to its employer portal.

- Furthermore, the AP has determined that the Dutch Tax Authorities may no longer use social security numbers (BSN nummers) of Dutch residents as part of the VAT identification numbers (BTW nummers).

Worth mentioning while on the subject: In line with comparable investigations and decisions made by other supervisory authorities, the AP has imposed a fine of €600.000 on Uber as a result of the late notification by Uber of its 2016 large-scale personal data breach.

On a personal note, I expect there to be a call at some point for legislation with regard to director's liability (bestuurdersaansprakelijkheid) to also extend to situations where organizations are found liable or are imposed fines for data protection violations.

New Zealand

By Jaqueline Peace

At the end of my 2018 prediction, I asked the question, "should I cross my fingers again?" This question was in reference to the never-ending hope that privacy law reform will materialize in New Zealand in 2018 (some seven+ years after the Law Commission review was undertaken), and we would finally see the 1993 Privacy Act updated. Well it seems, that despite all digits being crossed, as we head into 2019 we still did not manage to achieve privacy law reform in 2018. There has been progress though, of a kind.

The Minister of Justice introduced the Privacy Bill, intended to overhaul the 25-year-old Privacy Act currently in place. While the bill included increasing the commissioner's powers and mandatory data breach reporting, among other provisions, none of the above reflects the overhaul of the current Privacy law that New Zealander's were expecting or wanting. The bill currently fails to address the need for increased individual's rights to control or delete their personal information, nor does it address fines for organizations that fail to comply with their privacy obligations. Privacy Commissioner John Edwards often notes at speaking events, that whilst he welcomes the reform, the current form of the Privacy Bill, "will mean New Zealand will have a Privacy Act fit for 2012."

We now patiently await the Review Report of the Bill Select Committee, which was due in November but has been pushed to March 2019. Here's hoping the delay means that the submissions calling for our out-of-date bill to give increased consideration to international privacy law developments and provide New Zealanders the privacy protections they deserve are being heard. We are currently privileged in that we have EU "adequacy status," but within four years of the EU GDPR coming in to effect, that status is required to be reviewed. The future looks challenging if the current draft of the Privacy Bill isn't truly overhauled to go beyond what is currently set out in the proposed reform.

So, once again we kick off the new year crossing our fingers in the hope that by the end of 2019, we will have a newly reformed Privacy Act in place, but who knows what year it will be "fit" for.

Nigeria

By Ridwan Oloyede, CIPP/E

Nigeria currently has a fragmented privacy framework, with largely sector-specific driven regulations and laws.

We expect to see the enactment of the Digital Rights and Freedom Bill. The bill has provisions on privacy and has been passed by the Nigerian Parliament but has yet to be transmitted to the president for assent.

A new Data Protection Bill will be initiated before the Senate this year. The bill is largely influenced by the EU GDPR and the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+) of the Council of Europe.

The Federal Ministry of Health pursuant to its power under the National Health Act 2014 is working on a national e-health policy which is expected to have provisions on privacy.

We expect to see significant progress and clarification on the position of the Electronic Transaction Bill and the National Information Technology Development Agency 2017 draft guidelines on data protection. The Consumer Protection Council in the past year released a set of guiding principles. It is expected that the CPC will issue a formal guideline to steer the enforcement.

Lastly, there are also other bills with privacy implications pending before the Nigerian Parliament at different legislative phases such as the Computer Security and Critical Information Infrastructure Protection Bill 2005, the Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008, the Electronic Fraud Prohibition Bill 2008, and Computer Misuse Bill 2009.

Poland

By Marcin Lewoszewski & Anna Kobylanska

It is expected that 2019 will be busy as to the data privacy legislation and regulatory guidelines. As to the new legal acts, we expect the package of about 160 currently binding legal acts will be enacted and binding in first quarter of the year. Within the package we will find crucial acts as banking or insurance law. The changes will reflect requirements of the GDPR in relation to, e.g., right of access or profiling and automated decision making in some of the business sectors. On the other hand, we expect that the Ministry of Digital Affairs will issue its guidelines in relation to GDPR and the derogation acts. It is planned that the "general GDPR guideline" will be issued in early February, and will be followed by other guidelines focused on Brexit and processing of personal data within the public sector.

Russia

By Maria Elterman, CIPP/E, CIPP/US

The Russian Data Localization Law, Federal Law No. 242-FZ, is actually enforced in Russia. Sanctions are given on a regular basis to infringing companies, and the trend for 2019 is toward increasing enforcement aiming at companies which are not complaint with the Localization Law.

During 2019, expect two draft amendments to the Russian Law "On Personal Data" as of 27.07.2006 No. 152-FZ. The first is regarding the human genome to be qualified as personal data in Russia. The draft is in the process of preparation by Roskomnadzor (the Russian data protection authority), and will come into effect in 2019. The second draft (in Russian only) is regarding data anonymization techniques that can allow processing of the data without any restrictions or users' consent. Also, it removes the requirement to obtain users' consent before sharing the data with third parties if the sharing is safe. The process of obtaining users' consent is going to be simpler without the need to make it in writing.

The overall trend for data protection in Russia is toward further enforcement and development of the data protection legal framework.

Serbia

By Aleksa Andjekovic

A new era for data protection and privacy is expected to emerge in 2019 in Serbia. In November 2018, the long-awaited and much-debated new Law on protection of personal data (Official Gazette of the Republic of Serbia, no. 87/2018) has been adopted. The Commissioner for Protection of Personal Data and some privacy professionals have

criticized first the draft and, following its adoption, the new law, finding it hardly comprehensible and expressing doubt regarding the implementation and application of it.

The new law implements to the Serbian legal framework the GDPR and transposes the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The full implementation of the new law on protection of personal data is scheduled for Aug. 21. The period until the end of August 2019 is expected to be quite hectic and challenging both for business and for privacy professionals having in mind new obligations the law imposes regarding processing of personal data and potential fines for breaches of it. Companies headquartered in the EU and companies dealing with the GDPR will have slightly less challenging tasks.

Also in 2019, the new Commissioner for protection of personal data is expected to be elected by the National Assembly.

Spain

By Miguel Recio

The year begins with a bill in the Congress to comply with Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016, on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Spain should have brought into force the law by May 25, 2018, as stated in Article 18 of the directive.

Furthermore, Spain has not yet adopted the law to bring into force the Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016, protecting personal data when being used by police and criminal justice authorities.

During 2019, it is expected that the bill on security of network and information systems will be passed, to adopt the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. Currently, the Royal Decree-Law 12/2018, of September 7, is in force.

Finally, as the current director of the Spanish DPA was appointed in July 2015, it is expected that the government shall appoint a new director this summer.

Switzerland

By Stéphane Droxler, CIPP/E, CIPM

Swiss politicians have no reputation for being fast. On data protection, there is no exception to that rule. Back in 2015, the Federal Council passed its project for a new data protection law to the Parliament. For whatever reasons, it has not been processed so far. After having decided in 2018 to split the project in two, and spent the whole year on the easiest part, Parliament should finally tackle the next hunk during its spring session.

However, the complete revision of the current data protection law could not come at a worse time. The relationship with the EU is very tense, due to sterile negotiations on a global framework aimed to replace the multiple bilateral agreements. Switzerland does not want it. The EU is getting impatient and will not offer to the Swiss what it refuses to the English in the Brexit context. In addition to that, 2019 is a year of federal elections in Switzerland. Therefore, parliamentarians will likely be more

concerned with their re-election than with the progress of a complex topic, moreover closely linked to the EU relationship.

Turkey

By Begüm Yavuzdoğan Okumuş, CIPP/E

Apart from an economic slow-down, one can say that 2018 has been productive and looked promising for Turkey from a privacy perspective. We have seen considerable efforts and attempts from the data protection authority, as it has been active in meeting with the practitioners, academics, organizing trainings and seminars, and issuing new guidelines, and regulations. We have seen more data breach decisions rendered by the DPA and these shed a light to the practice and claims made at level of DPA has also increased dramatically as stated by the DPA experts.

The Data Protection Law in Turkey became fully effective as of April 2018 and privacy has been on the top list of agenda of privacy practitioners.

The most debated issues in data privacy in Turkey, (i) data transfers outside of Turkey in the absence of safe country list and (ii) processing health data (a requirement to get explicit consent in almost any and all situations – one exception reserved from medical purposes) have not yet been resolved. However, the DPA has acknowledged the legal needs for a revision on these matters and added that it is currently working on the safe country list. The DPA has also prepared undertaking templates for data transfers abroad.

The obligation to be registered with the Data Controllers' Registry started as of Oct. 01, 2018 for those who are held within the obligation to get registered. Registry obligation will also include those who are not based in Turkey but process personal data in Turkey, the deadline set for registration is Sept. 30, 2019.

We anticipate that the DPA will continue to be active and cooperate with privacy professionals in 2019, and this will help establishing and developing the privacy practice in a concrete manner. The DPA is required to release data breach decisions in more details (without anonymization) so that it can provide more insight to the practice. There are still various issues that need clarification and guidance from the DPA.

It is worth saying that the public sector is not as diligent as the private sector about data privacy, although there is no difference in their obligations. Further, the Turkish courts that are capable of resolving privacy disputes from criminal law perspective must be also fully informed about the new regulations. We see that there is lack of knowledge and interest in the public sector and Turkish courts (especially criminal courts) in privacy matters and expect to overcome these in coming years.

UK

By John Bowman, CIPP/E, CIPM

Once again, privacy law in the U.K. is likely to be dominated by Brexit. As things stand, the U.K. is due to leave the European Union March 29. However, the political situation remains unpredictable. U.K. members of Parliament are due to have what is described as a "meaningful vote" on the draft withdrawal agreement during the week of Jan. 7. If MPs vote in favor of the agreement, this will lead to a status quo transition period where the free flow of personal data between the EU and the U.K. will be maintained until at least December 2020. However, if Parliament votes down the agreement and the U.K. heads for a "no-deal" exit, then data transfers from the

EU to the U.K. will be prohibited unless appropriate measures as set out in the GDPR are put in place. Dec. 19, 2018, the European Commission published its no-deal contingency plans across a range of thematic areas, but there was no mention of data protection. Therefore, as things stand at the beginning of 2019, there will be no contingency for data transfers in a no-deal situation beyond what is set out in the GDPR unless the withdrawal agreement is approved. Businesses and practitioners should note this situation and make plans accordingly.

US—Federal Law

By Emily Leach, CIPP/E, CIPP/US

There has been lots of movement toward a federal privacy law in the U.S., with industry, advocacy and government parties weighing in and drafting bills. It's certainly looking more likely than ever before that we may see a federal law this year. What that law would look like, however, is anyone's guess. Some say the standard set by the California Consumer Privacy Act may become the new baseline, meanwhile others are looking to preempt it. To keep up with the latest developments, check the US Federal Privacy Watch page in the IAPP Resource Center.

US—Health Care

By Kirk Nahra, CIPP/US

The current hot ticket is the Request for Information issued by the Department of Health and Human Services' Office for Civil Rights, which seeks stakeholder input on a smorgasbord of HIPAA privacy issues. These range from the old (the HITECH holdover accounting rule) to the new (a broad range of issues related to expanding information disclosures for "coordinated care" and related activities, many linked to the opioid crisis). While I don't expect a proposed rule (and then a final regulation) any time soon, this is an opportunity to the broadly-defined health care community to state its positions on this variety of issues.

At the national legislative level, the big issue is how health care will fare in the current debate over national privacy legislation. Will the health care industry — at least the part covered by HIPAA— be "carved out" of national law? Or will it face a new set of requirements on top of HIPAA? And how will this national proposal deal with the biggest health care "gap" today — the broad range of health information being created and gathered outside of the scope of the HIPAA rules, through wearables, mobile aps and the like. We also will be watching how the national debate will deal with the growing concerns about how "non-health" information (such as incomes, voting records, purchasing habits) are being applied and evaluated in critical health care contexts. All of this while health care technology explodes and a growing array of technology companies begin entering health care markets.

US—FTC/FCC

By Yaron Dori

In December 2018, the FCC issued a Declaratory Ruling classifying text message services as "information services," effectively subjecting them to the jurisdiction of the Federal Trade Commission in much the same way that broadband internet access services were reclassified and effectively subjected to the FTC's jurisdiction in the Federal Communications Commission's "net neutrality" decision a year earlier. Expect to see the FCC continue to resolve regulatory ambiguities through deregulation when it comes to technology, and for parties with concerns over those deregulated technologies to take those concerns to the FTC. At the same time, expect to see

Congress work through these issues as it considers comprehensive privacy reform legislation, and for Congress to rethink the FTC's rule-making and fining authority so as to provide the agency with greater resources to develop and enforce privacy protections.

Zimbabwe

By Kuda Hove

Over the past year, the Zimbabwean government has stepped up efforts to use technology to maintain law and public order. This led to the acquisition of facial recognition technology from China and the launch of a smart cities initiative. So far, traffic surveillance cameras have been installed in parts of the capital city as part of these complementary initiatives. Japan and Zimbabwe have also entered into an agreement that will see Japan give or sell cybersecurity equipment to Zimbabwe.

Despite this increase in the acquisition and use of surveillance technologies that have a huge potential to affect individuals' right to privacy, the government is still yet to introduce any adequate privacy legislation. Zimbabwe still lacks any laws and policies that regulate the handling, processing and disposal of data collected by government agencies.

In late December 2018, government approved the drafting principles for the proposed Cyber Protection, Data Protection, and Electronic Transaction Bill. The proposed merged bill has gone through various draft versions over the past five years and it remains to be seen whether the Zimbabwean government will finalize and gazette the bill during the course of 2019. Currently, government has not given timelines within which it will finalize the bill.