ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

New era for US privacy laws: California and more

No US federal privacy law is in sight but keep a close eye on California and rapidly expanding enforcement and litigation risks. By **Laura Linkomies**.

The California Consumer Privacy Act (CCPA) will come into effect from 1 January 2020 and be enforceable by California's Attorney General from July 2020. The law, often compared somewhat erroneously with the GDPR, was amended in September and will be implemented through regulations that will be finalised in Spring 2020.

Latham & Watkins lawyers offered invaluable insights into the

Continued on p.3

DP is central to Germany's Facebook competition case

Stewart Dresner reports from Brussels on the rationale for the German competition authority's decision on Facebook's abuse of its dominant position.

Personal data plays a key role in data-driven services such as social networks, online search, or so called "digital assistants" which are part of our everyday lives. Global players acquire these data while offering their services at first glance for free. With regard to these strongly data-driven business models, there can be a close link between data protection law and competition law, says Andreas Mundt, President of the

Continued on p.5

Future PL&B Events

- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London. Speakers include Onfido on its use of biometric data and its experience of the ICO's sandbox.
- *Germany's data protection law: Trends, opportunities and conflicts,* 11 March 2020, Covington & Burling, London
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 162 **DECEMBER 2019**

INTERNATIONAL report

ISSUE NO 162 **DECEMBER 2019**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Caleb Skeath and Brooke Kahn
Covington & Burling LLP, US
Christopher Docksey
EDPS and Guernsey Data Protection Authority
Andin Aditya Rahman
Assegaf Hamzah & Partners, Indonesia
Merrill Dresner
Assistant Editor, *PL&B*

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Privacy developments around the world

We continuously monitor legislative developments globally. In this issue, Professor Greenleaf analyses the situation in Sri Lanka, which now has a GDPR-inspired bill, Pakistan and Nepal (p.22). There are also changes to Indonesia's law (p.17).

In the EU, Slovenia is the only country that has not yet transposed the GDPR into national law. The much-awaited new Greek data protection law entered into force at the end of August and we will publish an analysis of it in the next issue of *PL&B International*. The Greek law implements both the provisions of the EU Law Enforcement Directive and the GDPR.

In the US, the California Consumer Privacy Act (CCPA) will come into effect from 1 January 2020 (p.1) , and there are also changes to US state data breach notification laws (p.10).

How do we keep up with all these developments? Mainly with the help of our knowledgeable correspondents, but also by directly talking to regulators at events such as the DPA's International Conference in Albania (p.7 and p.12), where I met regulators from many countries including Malta's Information and Data Protection Commissioner to learn about Malta's new law (p.20). The host country, Albania, also granted us an interview, the results of which you can see on p.18.

Our own events also play a role. In March we will welcome authoritative speakers from Covington & Burling, Germany to our one-day conference in London on Germany's data protection law, as well as the Head of Department at Bavaria's Data Protection Authority (See programme at www.privacylaws.com/germany).

On p.14, read an analysis of accountability – it is a global standard with great advantages for organisations and regulators, says the author, Christopher Docksey, Honorary Director-General at the EDPS.

To help you in your own research, we have now updated our webpage www.privacylaws.com/links which includes links to 140 national/sub national DPAs, in 97 countries. Also available is online search by keyword to *PL&B's* previous publications and events.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

California... from p.1

CCPA and the current US data privacy regime at a *PL&B* conference on 14 November in London. Opening the conference, *Stewart Dresner*, CEO of *PL&B*, explained that we should not expect a federal privacy law any time soon but there are many state developments. Also, newly found support from US multinationals for a federal law puts more pressure on the legislature. *Gail Crawford*, Partner of Latham & Watkins' London office stressed the opportunity for private actions with high statutory penalties under the CCPA following data breaches – a real worry for organisations.

Michael Rubin and *Jennifer Archie*, Partners at Latham & Watkins San Francisco and Washington DC offices respectively explained the sectoral approach to United States privacy achieved through a patchwork of federal and state privacy laws; in addition to the well-known Children's Online Privacy Protection Act (COPPA) (dealing with collection or sharing of information from children under 13), and Health Insurance Portability and Accountability Act (HIPAA) (dealing only with healthcare providers and private payers such as insurers and their service providers). There are some others such as the Electronic Communications Privacy Act (ECPA) and The Gramm Leach Bliley Act (GLBA, dealing with the financial services sector).

The ECPA is a very broad act, also known as the Wiretap Act. It is very complicated as there is much case law, and also developments in technology affects this area. Similarly, the Video Privacy Protection Act (VPPA) which was originally passed to address the conduct of "videotape service providers," has not been amended in light of new technologies. Yet, through private class action litigation, many courts have been willing to extend the VPPA to companies like Netflix or YouTube.

Following many years of few or no filed enforcement cases, in response to pressure from Congress, the Federal Trade Commission (FTC) has aggressively stepped up enforcement of COPPA. The FTC enquired recently if this law should be amended again and this is likely to happen. The law is globally the first addressing children's privacy and introduced 13 as the age of consent. This area is very much the focus of the FTC, and there has recently been some significant enforcement action, including a $170 million settlement with YouTube for collecting personal information from viewers of child-directed channels without parental consent. Another fine imposed under COPPA recently was the $5.7m settlement with Musical.ly for failure to delete personal data at parents' request.

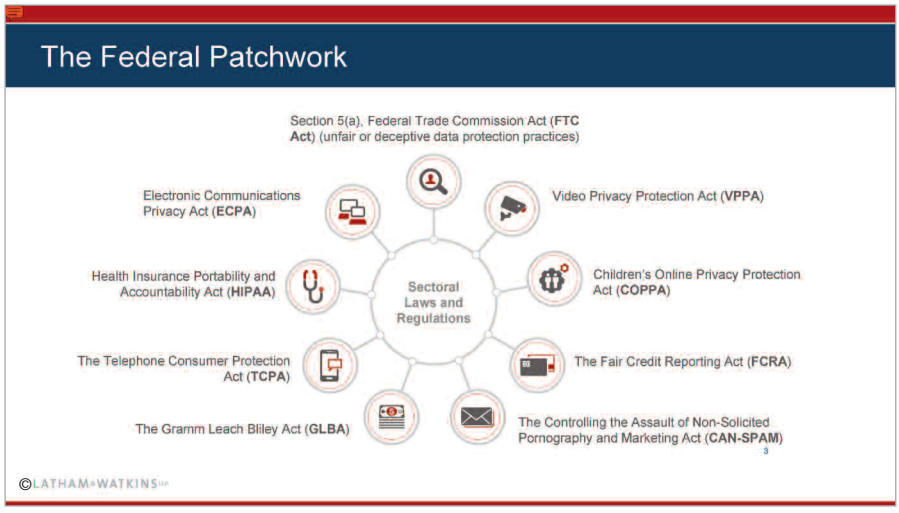
Michael Rubin noted with respect to the FTC, "It is a small agency, and for the first time in a very long time the FTC's five commissioners are all new. They try to reach unanimous decisions and make a real effort to stop scams. Many companies, especially smaller ones, choose not litigate with the FTC. And while FTC fines get all the attention, the consent orders are often where the real action is. If you are a first-time offender, the FTC cannot generally speaking impose a fine for violation of the unfair and deceptive trade practice laws which are the basis for data privacy or security enforcement cases. All big tech companies were therefore not fined in their first cases. There are efforts now trying to change that."

In addition to expanding enforcement of federal privacy laws, the states are a very important source of new legislation, expanding or experimenting with new privacy rights. In the US federal system of government, the states have great power to act, and the flexibility to move effectively and quickly to write and adopt new laws. As in other areas, the 50 states serve as a sort of laboratory to try out new ways of regulating information practices.

Nevada, for example, has adopted an Act prohibiting website operators, or anyone who runs an online service, from selling certain information on a consumer to data brokers without that consumer's permission, in force since 1 October. *Illinois* has a biometric statute that imposes strict consent requirements on the collection or processing of biometric information, including fingerprints, retina scans and facial scans. *Texas* and *Washington* have similar laws but no possibility for private action.

Jennifer Archie commented that the US states were the first globally to pass mandatory data breach notification, starting with California in 2002. Today, all 50 states have data breach laws, with overlapping and conflicting obligations around when to notify, whom to notify, how to notify, what, if any, benefits such as credit monitoring to offer, and many other variables which breached companies need to sort out with the help of counsel in the first hours or days after a breach. Fortunately, over time, insurance products and a large and expert service industry has developed to aid companies with their reporting and response obligations.

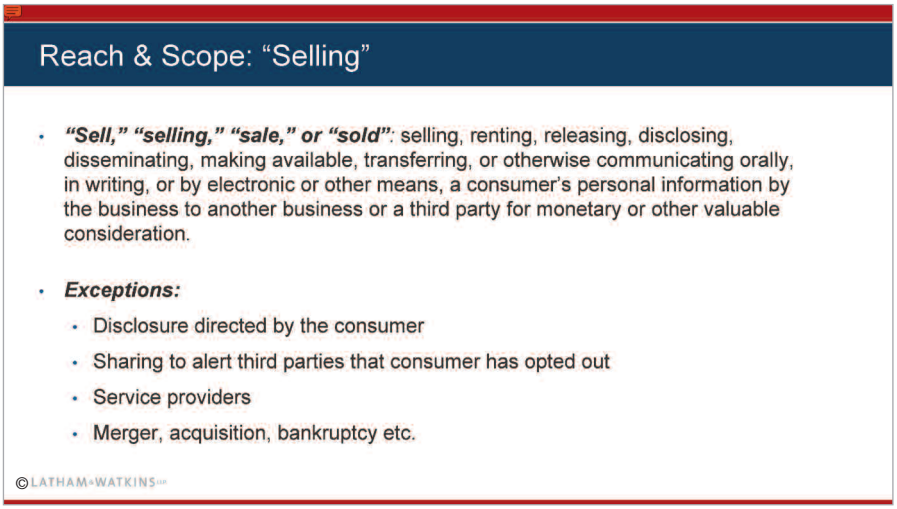
Another enduring feature of the US legal landscape post-breach, however, is the dominant role played by class action litigation. When a data breach occurs, affected consumers may be able to file a class action lawsuit against the company that failed to protect their information. Filing and settling these lawsuits is big business for a large, often highly professionalised, group of class action attorneys.



Watch out for the CCPA

Robert Blamires, Counsel at Latham & Watkins' San Francisco office explained that the CCPA is far reaching due to its broad scope and broad definitions. Whilst it only impacts covered "businesses", this includes a wide range of legal entities. A company is covered if they do business in California, collect personal information about consumers and determine the means of their processing, as well as fulfil one of the following requirements:

- Annual gross revenues over $25 million
- Exchanging personal information of 50, 000 or more consumers or
- 50% or more of annual revenue comes from selling personal information (see slide).



The Act creates a right for individuals to make enquiries about their personal information. However, the Act does not provide the same rights as the GDPR in terms of transparency, access, deletion and opt out from "sale" of personal information, Archie said. "It is a very limited 'show me' right."

The new obligations on businesses include specific requirements about responding to requests and providing information. Businesses must treat deletion requests as an opt-out request if a requestor cannot be verified. Also do-not-track requests, browser plug-ins or other privacy controls must be recognised as opt-out requests.

There are new data security implications as individuals have a private right of action to challenge an organisation in the case of a security breach due to failure to maintain reasonable security. There are some similarities with the GDPR, but the way in which the obligations work are quite specific and not always the same, Blamires said.

Archie stated that California's Attorney General (AG) has issued a fact sheet and draft regulations in stating very explicitly that compliance with the GDPR is not a "safe harbor" for demonstrating compliance with the CCPA. The AG has significant enforcement powers under the CCPA – he can request a business to correct their practices within 30 days. If the business fails to do that, the AG may bring a civil action for the violation. The current draft regulations add to this sanction to create more compliance burdens for business.

"The CCPA draft regulations will attract many comments – some areas are simply wrong. On the other hand, some aspects are so carefully construed that they are unlikely to change," Rubin said. "There is much industry lobbying but I doubt there will be major changes as a result."

There are exemptions for B2B and employees, for example, until 1 January 2021, personal data on employees, job applicants and contractors are excluded. But on the whole, businesses should be on their toes and not delay to ensure compliance, Latham & Watkins experts said. Covered businesses that have already put in an effort to comply with the CCPA may still need to implement important and significant changes in light of the draft regulations and should not wait until the final regulations are released to take action. GDPR compliance does not equal CCPA compliance. The laws have different definitions, scope and requirements, even though they address the same fundamental rights of transparency, choice, or access.

> Organisations should conduct a gap analysis to see where the CCPA and the GDPR differ in their impact and ensure that security measures are reasonable.

What to do next

Organisations should conduct a gap analysis to see where the CCPA and the GDPR differ in their impact and ensure that security measures are reasonable. Businesses should also analyse their "sale" position and prepare "do not sell" options.

In terms of responding to access requests, it is advisable to introduce a toll-free number and a form on the company website for making requests, as well as make sure there is a process in place for verifying the requestors' identity.

In addition, organisations will need external privacy policies which explain their verification process, and add notices for their California-specific workforce. Organisations that are found to have insufficient protections are liable for training employees on the CCPA and the draft regulations.

INFORMATION

See www.lw.com/thoughtLeadership/draft-california-consumer-privacy-act-implementing-regulations-what-is-new-what-is-next

Competition... from p.1

Bundeskartellamt, Germany's Federal Cartel Office.

Mundt explained that the business models of companies like Google, Amazon, Apple, Facebook, as well as Baidu, Alibaba and Tencent, are powered by consumers giving away their personal data. Much of their success is about the collection of personal data. The processing of this personal data can drive innovation and services, which people like and use, and Artificial Intelligence, which provides benefits to consumers in the form of new popular services.

But there are also pitfalls, as the companies use these huge volumes of named personal data and cluster it with other information in real time. For example, Mundt stated that according to a study done at Vanderbilt University, idle Android phones connect with Google 40 times an hour. Although Google disagrees, it has apparently declined to give its view of the correct figure. Tim Cook, Apple's Chief Executive, has described Facebook's methods as "military profiling".

This is worrying because it raises the question of who can compete with these companies, as consumers' personal data is not as easily available to other companies. As a result, for example, the algorithms of other search engines are worse than Google because they do not have so much data. "In the end, it is the consumer who pays the price, as the consumer is faced with a monopoly", said Mundt. He gave the example of Microsoft's Internet Explorer browser which was dominant in the early 2000s. It had no significant competitors, and therefore, introduced no innovations for five years until challenged by Firefox which introduced new features for users.

Strongly data-driven business models

Facebook is one example of a service whose members attract new members who in turn again attract new users, in effect a snowball system. Such network effects can lead to a lock-in effect for users, meaning that it is difficult for them to switch to another player. In particular in the interplay with these network effects, the access to data can be an important factor of market power.

Possible options to address this factor of market power could include:

1. To ensure data portability (Art. 20 GDPR) in order to enable consumers to take their data to another provider.
2. To enforce access to data – in certain situations and in line with the GDPR – to enable others to compete with the dominant companies.
3. To limit the gathering and use of personal data – this is what was done in the German Federal Cartel Office's Facebook decision in February 2019.

In Germany, there are currently around 23 million daily active users of Facebook and 32 million monthly active users. Based on monthly active users, Facebook holds 80% of the market, and it has no real competitors because services offered by other large tech companies, such as LinkedIn, serve a different purpose.

Facebook has superior access to personal data. This is reinforced by its terms and conditions which allow the limitless collection of personal data. This method of collecting personal data is extended to the personal data collected by other companies Facebook owns, such as WhatsApp and Instagram. Business tools such as Facebook Analytics collect data about the usage of millions of sites. The resulting personal data from various sources is combined to produce a perfect user profile. The Federal Cartel Office found that Facebook abuses its dominant position by imposing unfair and illegal business terms on its users, in particular limitless data processing terms. This amounts to a systematic infringement of the GDPR's rules on the legal basis for processing. The Federal Cartel Office has considered such conduct by a dominant company in a data-driven business to be a breach of competition law.

The decision

"In data-driven markets, data can be a key driver to dominance," declared Mundt.

One hundred of the 300 pages of the Federal Cartel Office's February 2019 decision in the Facebook case[2] directly relate to the GDPR, combined with arguments about harms to consumers. The Office also cooperated with different Data Protection Authorities. According to the decision, Facebook will be able to collect a person's data but not combine it with data from, among others, Instagram, WhatsApp or third-party sources. For the first time, consumers will have a real choice. They may use the social network of Facebook without also agreeing to such extensive data processing. Mundt described this as a "structural internal divestiture": Facebook would have to keep separate the personal data collected from different sources if the

> The Federal Cartel Office found that Facebook abuses its dominant position by imposing unfair and illegal business terms on its users.

EU'S COMPETITION COMMISSIONER WATCHING GERMANY'S FACEBOOK CASE

When meeting Margrethe Vestager, European Commissioner for Competition, in Brussels at the memorial meeting for Giovanni Buttarelli[1] in September, I asked her whether she is watching closely the investigation of Facebook and subsequent decision by Germany's Federal Cartel Office. She replied firmly "Yes" because of its significance for the tech sector across the EU. She has now been appointed Executive Vice-President of the European Commission with continuing responsibility for competition policy following the establishment of the new European Commission on 1 November.

Her attention to this Facebook case is relevant to all the leading technology companies.

Stewart Dresner

users do not give their consent to this kind of data processing and if there is no other legal justification.

As German competition law explicitly states that the Federal Cartel Office should assess access to and processing of data when evaluating market power, Mundt sees two possible approaches to satisfy this obligation:

1. Apply the existing parameters of the GDPR as the base of such an assessment, or
2. Develop a separate methodology to assess how data should be gathered and processed.

Since the latter approach would be hard, it seems strictly preferable to use the GDPR as an existing legal framework.

Fines?

Mundt explained his rationale for not imposing a fine on Facebook. He said "We have experience of fining, but we don't always impose fines because they are a price of doing business. Instead, we want to change Facebook's behaviour in the long run."

Future cooperation between different regulators

As to the future, Mundt said that the regulators must learn from each other. Joint investigations by competition, data protection and consumer regulators are difficult to organise because of the lack of a clear legal basis for such a step, stated *Ulrich Kelber*, Germany's Federal Data Protection Commissioner since January 2019. However, information can be exchanged between regulators. Mundt stressed that there could also be informal cooperation between competition and Data Protection Authorities. There could be a staff exchange between national competition and data protection authorities, as has occurred with the CNIL in France, explained *Marie-Laure Denis*, the President of the CNIL since February 2019.

Martin Selmayr, Secretary-General of the European Commission, when asked whether there are any plans for the European Commissioner for Competition Policy to take on a data protection case, replied that there was nothing to prevent it.

Giovanni Buttarelli, European Data Protection Supervisor, in one of his last public statements, said that three years ago he had established the EDPS Digital Clearing House which brought together the data protection, consumer and competition regulators from across the EU for regular coordination meetings.

In answer to the question whether there should be an EU supervisory authority for the digital sector, *Elizabeth Denham*, the UK's Information Commissioner, said "no because now nearly everything is digital" and Mundt added "We don't have a regulator for the offline world…Each regulator has to pursue its task". Selmayr agreed stating that each national regulator should not act like an EU-wide regulator both vertically and horizontally. If it works, we don't need centralisation."

Facebook's appeal against *Bundeskartellamt*

Facebook was given 12 months to discontinue the conduct objected to by the Federal Cartel Office. Facebook appealed the *Bundeskartellamt's* decision to the Düsseldorf Higher Regional Court. A person close to the case has provided *PL&B* with an update on Facebook's appeal.

The Higher Regional Court in Düsseldorf (OLG Düsseldorf) decided in an interim decision on 26 August 2019[3] that it had serious doubts whether the order of the Federal Cartel Office was lawful. Therefore, it decided that it should not be enforceable until a final decision in the main proceedings. The German Cartel Office has already appealed this interim decision to the Federal Court of Justice (*Bundesgerichtshof*).

The decision of the Higher Regional Court does not discuss the question whether Facebook's consent or terms and conditions breach the GDPR. It only mentions that Facebook has been fully transparent about data use and exchange and that the decision to use Facebook or not under these terms can be made by the users without undue pressure. The Court considered the question whether there might be a breach of the GDPR as not relevant, because a breach of the GDPR as such does not lead to a breach of competition law in Germany. There needs to be an impact on competition and the court was of the view that the Federal Cartel Office did not make this case as plausible. Therefore, it is a pure competition law decision.

The specific competition law clauses about misuse of market position by breach of law in Germany might not go as far as the Federal Cartel Office was hoping. We will see what the *Bundesgerichtshof* will in the end say about this case, but the decision of the Higher Regional Court in Düsseldorf already indicates that the idea of GDPR enforcement through competition authorities might not fly after all.

This is in line with the view of the EU Competition Commissioner, Margrethe Vestager, who advocates a clear separation between data protection and competition law.

INFORMATION

This report is based on *Data protection law and competitiveness in the digital age*, a panel discussion in Brussels on 9 July 2019, hosted by the late Giovanni Buttarelli, European Data Protection Supervisor, and Ulrich Kelber, Germany's Federal Commissioner for Data Protection and Freedom of Information.

REFERENCES

1 www.privacylaws.com/news/giovanni-buttarelli-a-personal-tribute/
2 The 12-page English language summary, published on 15 February 2019, and the 278-page English version of the *Bundeskartellamt's* decision, published on 11 July 2019, are at www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2019/11_07_2019_decisionFacebook.html
3 The 37-page German version of the decision by the Higher Regional Court in Düsseldorf, published on 28 August 2019 is at: www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf

Global data protection laws: Where will they converge?

Stakeholders discuss the role of the Council of Europe, the EU and the OECD in creating a global data protection standard. **Laura Linkomies** reports from Tirana, Albania.

The DPAs' 2019 international conference sought to find an answer to the hot topic of global convergence in privacy and data protection. First debated was the Council of Europe (CoE) Convention 108, which was first adopted in 1981 and was updated in 2018. Currently, Convention 108 has 54 signatory parties: all members of the Council of Europe, but also countries from Latin America and Africa. How is the modernised Council of Europe Convention 108+ different from other international frameworks? Its "human rights" flavour sets it aside from other instruments, but is this difference an asset or an obstacle? Does it have potential for global application?

Jan Kleijssen, Director of Information Society and Action against Crime, Council of Europe, spoke about the Convention's broad scope of application; Argentina and Morocco joined recently so the Convention has importance well beyond Europe. An accession request has been received by Costa Rica, and an assessment on it is being made now. Recent work on Artificial Intelligence includes new guidelines[1]. Codifying rules will soon be ready.

Joseph A. Cannataci, UN Special Rapporteur on the Right to Privacy, said that when the convention was first launched most of the focus was on government and companies, but much less so on law enforcement and national security. "The convention provides the countries with an obligation to meet minimum data protection standards in this field, but not enough countries have the political will to discuss these issues at a detailed level. It would be excellent if the CoE issued a detailed recommendation on this."

John Edwards, Privacy Commissioner, New Zealand, reflected that New Zealand obtained observer status in 2017. "We probably could have acceded earlier. It's important for us to do so – as a small, principled country we think it's important to engage internationally and find common solutions to transnational issues. The appeal of 108 is that is has a strong foundation in human rights, so it's not just about consumer rights."

Convention 108 has great promise to allow a nation like New Zealand to follow an international measure, Edwards said. Combined with ability to respond to emerging issues, for example, Artificial Intelligence, is important. CoE can tackle these issues without a treaty change required. "Each signatory adds strength to the international movement, where the EU GDPR is not really capable of doing that. CoE is a more welcoming instrument. I am yet to have to have this conversation with our government to see if we can meet all the obligations. There is a balance sheet of pros and cons but I see great opportunity."

Patricia Poku, Executive Director, Data Protection Commission, Ghana, said that Convention 108 has been very useful for Ghana. "I am personally a champion. We promoted it at the African data protection conference earlier this year, and many participants liked the idea and we got much positive feedback on it. Those who already use it, find it useful. As part of Africa's DPA network, we use it to promote best practice and as a basis to implement new laws. I hope it will create consistency, and engage countries with the same understanding, to sing from the same song sheet so to say.'

Omer Tene, Vice President, Chief Knowledge Officer, IAPP said that the US has acceded the cyber convention. The US has traditionally supported multinational frameworks such as APEC, and OECD guidelines he said. Until recently the US was an observer to 108. "This instrument was seen as a viable alternative instrument for data transfers. The US tried to persuade some of its non-EU allies to join. But it has limitations from the US perspective. We support open data flows but the convention tries to restrict that."

Tene said that while the convention is less bureaucratic than the GDPR, there are restrictions. "EU countries have become an island within the 108… The structure of DPAs still very much looks like the EU DPA structure. The US thinks it has a fairly robust DP Authority but it is not this model. For an international instrument, 108 has Europe in its name," Tene argued.

Future of convention 108?

Jean-Philippe Walter – Council of Europe Commissioner for Data Protection, said that 108 is certainly unique, as it is the only international legally binding instrument. It is also universal, because the Convention sets out the basic principles of data protection that are recognised worldwide and have this potential for universality. In addition, the Convention is not just a European convention, but a global convention. Any country with data protection legislation that complies with the requirements of the Convention may accede to it.

What do I think is vital for the future of the 108+ Convention? Walter said. "The first and most important and crucial step at the moment is the rapid entry into force of the text. We are dealing with an amending protocol which in itself requires the acceptance of all parties. The protocol has put in place a mechanism that allows for a faster entry into force but still requires the ratification of 38 States Parties. It is important to exert and maintain political pressure to accelerate the movement. The CoE's Convention Committee and Committee of Ministers have a responsibility and a role to play in this context. I also call on my colleagues in the data protection authorities of the countries party to the Convention to take active action and make a firm commitment to encourage their government and parliament to accept the amending protocol. Without a rapid entry into force, I fear that

Convention 108+ will lose its interest and become obsolete."

The future of the 108+ Convention truly depends on its recognition as a universal standard, Walter said. "There is no point in reinventing the wheel and wanting to develop new standards and instruments at all costs. We must build around the convention, make it grow and develop it. This is a task that the entire data protection community, starting with the International Conference, must address as a matter of priority."

Sophie Kwasny, Head of the Data Protection Unit, Council of Europe, chairing the session, posed the question to the panel: which model will win this "regulatory competition"?

Tene said that the underlying principles are pretty much recognised all over the world and are sound. The US has challenges with the European approach to adequacy, which means supremacy of certain framework over others. Other countries may not go with this idea, he said. Another challenge is the bureaucracy. Japan went for adequacy, that was a win for the EU but how many other economies will go this way?

Cannataci said that the US generally does not want binding agreements. Even when it does, it does not interpret the treaties etc. in the same way as others. For example, now the US claims that privacy is just for US citizens in America. There are certain questions about why US has not signed many international conventions. The importance of multinational conventions cannot be underestimated.

Kwasny said that in 108+, the modernized convention, there is now the limitation from the GDPR on data transfers. Recital 105 in GDPR says that CoE membership is favourable but not a precondition for adequacy, as we have seen with Japan which is not a party.

Edwards said that NZ has an EU adequacy decision. "I would think 108 would contribute to us being able to retain that status. Perhaps there is leeway – adequacy does not mean equivalence."

Tene said that the framework is European, and European law has been transformative in this area. On the other hand, a negative aspect is that Europe is a collection of democracies with structures that do not necessarily exist in other countries, that can't just copy paste European framework into their law. Japan or US do not necessarily provide less protection than, for example, Russia which is part of this framework.

Edwards said that the enforcement cooperation arrangement is enabling. 108+ promised mandatory cooperation. A DPA must do certain things at other DPAs' request. "This has given us a mandate to tell governments to request enough funds."

Cannataci said: "I rejoice in the human rights aspect. Some governments approach data protection by never mentioning privacy or human rights but only talk about consumer protection. It is a probability that CoE 108 will become truly global."

Latin American developments

Data privacy laws are developing fast in Latin America. The GDPR's influence can be seen and we may soon see new EU adequacy applications from this continent. Speaking at a conference session on Latin American data protection laws, *Eduardo Bertoni*, Director of Argentina's Data Protection Authority, said that Argentina became the 54th Party to the Convention 108 in June 2019. Argentina's government signed the convention and is now going forward with the ratification process. Argentina has "adequacy" but its position is being reviewed by the European Commission.

Brazil is moving forward and establishing its DPA. *José Ziebarth* from Brazil's Ministry of Economy explained that a Federal decree will soon establish the DPA. The next stage will be in April 2020. Enforcement of the law starts from August 2020.

Chile's data protection law was one of the first adopted in the region. *Marcelo Rago Aguirre*, President of the Chilean Transparency Council, said that the law had very little impact – it was implemented but not developed further. There are now efforts to make future improvements in the law of 1999. Convention 108 is a baseline we should refer to, he said.

Mexico acceded to Convention 108 in 2018. In the summer of 2019, Colombia had discussions about the possibilities of joining the Committee of Convention 108 as an observer, a first step towards Convention 108+.

More convergence?

Besnik Dervishi, Albania's Information and Data Protection Commissioner called for more convergence between data protection and competition laws. *Elizabeth Denham*, UK's Information Commissioner said that the DPAs are working towards an agreement on greater regulatory cooperation (see p.12 in this issue).

Chairing a panel on global convergence was *Professor Graham Greenleaf*, PL&B Asia Pacific Editor. Greenleaf, who has previously argued that the UN should adopt Data Protection Convention 108 as a global treaty, asked the panel what progress has been made toward common standards.

Chawki Gaddè, Head of the Tunisian DPA (INDPDP), and President of the Francophone Association of Personal Data Protection Authorities (AFAPDP), said that as a starting point, the ownership of personal data has been addressed by a declaration by the francophone association; it is human beings who own their data.

Bruno Gencarelli, Head of International Data Flows and Protection, European Commission, said: "Convergence is a reality. It is no longer just an interesting topic for conferences but in the past few years we have seen many developments; new opportunities facilitating trade and social interaction. At the European Union, we are committed to, and intensifying talks with third countries to develop convergence between systems."

He referred to the Japan adequacy finding, the negotiations with Korea, in addition to talks to be started soon with some Latin American countries. A broad toolbox is needed, he said. So where do we go from here? Horizontal convergence is needed as data breaches can affect a large number of jurisdictions but there are not many tools for joint enforcement.

Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong, said that his jurisdiction is proposing a legislative reform to converge or align with the global regulatory framework, prompted by the GDPR, and also recent data breaches.

Jan Kleijssen, Director of Information

Society and Action Against Crime from the Council of Europe, stated that the CoE stretches geographically to a wide area. The Committee brings together 70 countries as members and observers: about half of the countries that have a DP law.

Noboru Yamaji, Commissioner for International Cooperation, Japan PPC said that the Commission has taken initiatives, in addition to the EU adequacy decision, the promotion of APEC's cross border data transfer system in the Asia Pacific region. Based on these initiatives, we would like to work with all of you, he said.

Marc Rotenberg, President and Executive Director of EPIC, a public interest research centre in the US, commented that looking at the three global frameworks, the greatest challenge is enforcement regarding the GDPR. With the modernized CoE 108, the challenge is adoption. The OECD adopted a new policy framework for AI earlier this year, so implementation is the challenge there.

The way forward?

What is the most effective thing that could be done to raise data privacy standards? Is a global privacy agreement possible? Which international organisation would host it? These are clearly questions for the next few years and cannot be easily solved.

Gencarelli said that CoE also applies to national security and focuses on effective enforcement. There are parties from all over the world. He encouraged Asia Pacific countries to join. CoE is a Treaty so has to be ratified, but countries can also join as observers. So they can be part of the discussion, he said.

Wong thought that there is no pressing need to have another global agreement, but in terms of existing international agreements including the GDPR and its extraterritorial arm, we need an enforcement agreement or something similar, he said.

Dr. Felipe Rotondo, President, Personal Data Regulatory and Control Unit (URCDP) (Uruguay) said that global agreement is possible but he did not see it happening in the near future.

INFORMATION

This article is based on presentations at the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC 2019) in Albania, 21-24 October 2019. See privacyconference2019.info/

REFERENCE

1 www.coe.int/en/web/artificial-intelligence/-/new-guidelines-on-artificial-intelligence-and-data-protection

ACCOUNTABILITY: A GLOBAL BRIDGE TO SUPPORT HIGH STANDARDS OF DP?

Peter Hustinx, former European Data Protection Supervisor, EDPS, said that accountability is a global bridge to support data protection, but it is not always well understood in all parts of the world, not even with regulators from different backgrounds. DPAs need to be accountable as well for the outcomes they show in dealing with the current challenges. The keynote speaker, *Christopher Docksey*, Honorary Director-General at the EDPS, said that accountability in transfers is still a very important element but was transformed to a self-standing general principle. In his view, accountability means actively developing compliance and being able to demonstrate compliance (see p.14).
Marty Abrams from the Information Accountability Foundation said that accountability takes us behind compliance. It is not self- regulation.
Caroline Louveaux, Chief Privacy Officer at MasterCard said that the lack of harmonisation is a challenge for business. The Mastercard privacy programme is built on accountability. Privacy by Design is a corporate objective, and there is a culture of privacy across the organization; in addition to the global team of privacy professionals, there are privacy champions. Binding Corporate Rules (BCRs) are in place for all activities whether the company is a controller or processor.
Daniel Therrien, Privacy Commissioner of Canada said that his position on accountability is guarded optimism. 'It is a helpful tool if done properly, but is not a panacea. It needs to be enhanced by enforcement. The Canadian law incudes the accountability principle. Regulators should proactively check companies' compliance.
Bertrand Du Marais, Commissioner at France's Data Protection Authority, CNIL, said that accountability is not a new concept, but has been widely used in the banking sector already. "Convergence can only succeed on common values. Accountability cannot be an interoperability factor, the transposition of law is important."
Ailidh Callander, Legal Officer, Privacy International, said that a lot remains to be done. DPAs need to be empowered and there needs to be opportunities for collective redress. Data controllers need to make accountability a reality or otherwise data protection is meaningless, she said.

Californian company settles with FTC over false EU-US Privacy Shield claim

A California company has agreed to settle Federal Trade Commission allegations that it falsely claimed participation in the EU-US Privacy Shield framework, the FTC says.

The FTC alleged that Medable, Inc.—which provides technology solutions to business customers operating in pharmaceutical, biotechnology, and research industries—falsely claimed in its privacy policy that it was a certified participant in the EU-US Privacy Shield framework and adhered to the program's principles. While the company initiated an application with the Department of Commerce in December 2017, it did not complete the steps necessary to participate in the framework.

The FTC says it has now brought a total of 17 enforcement actions related to the Privacy Shield framework since it was established in 2016.

• *See www.ftc.gov/news-events/press-releases/2019/11/california-company-settles-ftc-allegations-it-falsely-claimed*

Round-up of recent changes to US state data breach laws

While most US state data breach notification laws have similar aspects, there are also notable differences. By **Caleb Skeath** and **Brooke Kahn** of Covington & Burling LLP.

Over the past several months, many states, including Illinois, New York, Texas, and Washington, have passed significant amendments to their state data breach notification laws that will expand the scope of notification obligations under these laws in the event of a breach. Currently, most state data breach notification laws only require notification of residents (and possibly state regulators or others) following a "breach," usually defined as unauthorized access to or acquisition of personally identifiable information (PII). PII, in turn, is often defined by state law as a state resident's name along with a Social Security number, driver's license or state identification card number, or a financial account, debit, or credit card number with any required security code, access code, or password to access a financial account. The recent changes to state data breach notification laws expanded the categories of PII that may trigger notification obligations if breached, imposed new requirements to notify regulators (in addition to affected individuals) in the event of a breach, and implemented specific timing requirements for how soon after a breach individuals and regulators must be notified, among other changes. These changes are summarized in additional detail below, followed by a few additional thoughts on what these actions may mean for future legislative action regarding data breach notification at the state or federal level.

Summary of changes

Arkansas: Following the entry into force of H.B. 1943[1], the definition of PII under Arkansas' data breach notification law has expanded to include certain biometric data of Arkansas residents when disclosed along with a resident's name. As a result of this change, entities might now be required to provide notice in the event of a breach of this information. Entities will also now be required to notify the state Attorney General following certain breaches. Such notifications will need to occur within 45 days, but will only be required if a breach affects more than 1,000 individuals.

California: California recently enacted A.B. 1130[2], which will take effect on 1 January 2020. The bill will expand the definition of PII in the state's data breach notification law to include a resident's name along with certain biometric data, a tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify an individual's identity. For breaches involving biometric data, this bill will also permit – but will not require – businesses to provide instructions on how to notify other entities that may have used the same type of data as an authenticator, so that those entities will no longer rely on the data for authentication purposes.

Illinois: Once recently-passed S.B. 1624[3] enters into force on 1 January 2020, entities will be required to notify the Illinois Attorney General if the entity provides notice of a breach to more than 500 Illinois residents. This change will significantly expand regulatory notification obligations under the law, as the current version of the Illinois data breach notification law only requires notification to the Illinois Attorney General in limited circumstances for certain entities subject to and compliant with HIPAA.

Maine: L.D. 696[4] recently amended Maine's data breach notification law to require notification to affected residents within 30 days after an entity becomes aware of a breach of PII. The previous version of the law did not include a specific time frame for such notifications, although it did state that such notifications must be made as expediently as possible and without unreasonable delay.

New Jersey: Following the entry into force of S.B. 52[5], the definition of PII under New Jersey's data breach notification law has expanded to include a resident's name along with credentials for accessing an online account. Previously, the law only defined PII to include a resident's name along with a Social Security number, driver's license or state identification card number, or certain financial account or credit/debit card information.

New York: S.B. 5775B[6], which went into effect on 23 October 2019, included significant amendments to New York's data breach notification law. These amendments have expanded the law's definition of PII to also include online account credentials, as well as the following types of data when disclosed with an individual's name: (1) certain biometric data; or (2) a financial account, credit, or debit card number without a security code, access code, or password, if it could be used to access a financial account. In addition, while the previous New York law defined a "breach" to only include unauthorized acquisition of PII, the amendments broadened this definition to also include unauthorized access to PII, potentially expanding the types of breaches that may require notification. While these changes may broaden the scope of the law's applicability, the amendments have also introduced new safe harbors for entities that provide notice to affected individuals in accordance with the Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), the New York Department of Financial Services cybersecurity regulations (NYS DFS), or other federal or New York state data security rules or regulations.

Oregon: As of 1 January 2020, amendments to the state's data breach notification law pursuant to S.B. 684[7] will expand the types of PII covered by the law, and therefore potentially requiring notification in the event of a breach, to include a username or identifying information "for the purpose of permitting

access to the consumer's account, together with any other method necessary to authenticate." The amendments will also impose additional obligations on "vendors" who maintain, store, access, manage, or process PII on behalf of "covered entities," including obligations to notify the state Attorney General directly under certain circumstances. (Under the current version of the law, an entity that maintains or possesses PII on behalf of another entity is only required to notify that entity of the breach.)

Texas: The state's data breach notification law currently requires notification of individuals as expediently as possible and without unreasonable delay, but without a specific required time frame, and does not require notice to regulators following a breach. Amendments to the state's data breach notification law pursuant to H.B. 4390[8], which will enter into force on 1 January 2020, will require notification to affected individuals within 60 days. Entities will also be required to notify the state Attorney General within 60 days if a breach involves more than 250 residents.

Virginia: H.B. 2396[9] has expanded the definition of PII under the state's data breach notification law to include a passport number or military identification number when disclosed with an individual's name. As a result of these amendments, a breach involving these categories of PII may now require notification to individuals and the Virginia Attorney General.

Washington: H.B. 1071[10] will implement significant changes to the state's data breach notification law once it enters into force on 1 March 2020. The bill will expand the law's definition of PII – and, therefore, the types of information potentially requiring notice if breached – to include (1) online account credentials, as well as (2) other data elements when disclosed with an individual's name, such as dates of birth, private keys, certain biometric data, medical or health insurance information, or student, military, or passport identification numbers. While the current law requires notice to residents (and the state Attorney General, if more than 500 residents are notified) within 45 days after a breach is discovered, the amendments will shorten this time frame to 30 days.

In addition to changes to generally applicable state data breach notification laws, several states have also recently passed sector-specific breach notification laws. Building on recent trends, six additional jurisdictions (Alabama[11], Connecticut[12], Delaware[13], Maryland[14], Mississippi[15], and New Hampshire[16]) have recently passed breach notification laws aimed at state-licensed insurance entities that, in addition to other requirements, may require notification to certain state regulators within as little as three days. Illinois[17] and Nevada[18], meanwhile, have recently passed laws that will impose breach notification requirements on various providers of educational services, including operators of educational websites and applications.

The future of data breach legislation

As evidenced by the significant amount of legislative activity seen in recent months related to data breach notification laws, states are continuing to enhance their cybersecurity and breach notification laws in the absence of comprehensive federal legislation regulating these areas. All 50 US states have enacted their own generally-applicable data breach notification laws, and recent updates to these laws have indicated a desire among state legislatures to require quicker notifications for broader categories of PII to keep pace with the increasing risks posed by data breaches. For example, several recent amendments have updated state law definitions of PII to include information that can be used to authenticate or identify an individual, such as official identification numbers, online account credentials, or biometric data, which is increasingly used by businesses for authentication purposes. New requirements in several states regarding the timing of breach notices to impacted individuals indicates an interest in ensuring that consumers receive information about a breach in a timely manner, while new requirements to notify state regulators following a breach could facilitate increased oversight of data security and breach notification practices by these regulators.

Given the current patchwork of state data breach notification laws that can vary significantly from one state to the next, the prospect of federal legislation could provide greater certainty for businesses and remove burdens associated with complying with different state laws. However, efforts to pass a federal data breach notification bill have encountered differing perspectives on key issues among various stakeholders, including the degree to which it might preempt state law. While discussions continue at the federal level to identify an approach that could serve as the foundation for a federal data breach notification bill, more activity in this space at the state level appears to be likely, and businesses should continue to monitor for updates to state laws and ensure compliance with any applicable requirements.

AUTHORS

Caleb Skeath and Brooke Kahn are Associates at Covington & Burling LLP.
Emails: cskeath@cov.com
bkahn@cov.com

REFERENCES

1 www.arkleg.state.ar.us/assembly/2019/2019R/Acts/Act1030.pdf
2 leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130
3 www.ilga.gov/legislation/BillStatus.asp?DocTypeID=SB&DocNum=1624&GAID=15&SessionID=108&LegID=118713
4 legislature.maine.gov/legis/bills/display_ps.asp?LD=696&snum=129
5 www.njleg.state.nj.us/bills/BillView.asp?BillNumber=S52
6 www.nysenate.gov/legislation/bills/2019/s5575
7 olis.leg.state.or.us/liz/2019R1/Measures/Overview/SB684
8 capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=HB4390
9 lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB2396
10 app.leg.wa.gov/billsummary?BillNumber=1071&Year=2019
11 arc-sos.state.al.us/PAC/SOSACPDF.001/A0013015.PDF
12 www.cga.ct.gov/2019/ACT/pa/pdf/2019PA-00117-R00HB-07424-PA.pdf
13 legis.delaware.gov/BillDetail/47568
14 mgaleg.maryland.gov/webmga/frmMain.aspx?id=sb0030&stab=01&pid=billpage&tab=subject3&ys=2019rs
15 billstatus.ls.state.ms.us/2019/pdf/history/SB/SB2831.xml
16 gencourt.state.nh.us/bill_status/bill_status.aspx?lsr=923&sy=2019&sortoption=&txtsessionyear=2019&txtbillnumber=SB194
17 www.ilga.gov/legislation/BillStatus.asp?DocTypeID=HB&DocNum=3606&GAID=15&SessionID=108&LegID=120294
18 www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6732/Overview

International DPAs plan greater enforcement cooperation

Laura Linkomies reports from the DPA conference, organised in October in Tirana, Albania.

The 41st International Conference of Data Protection and Privacy Commissioners agreed on a framework that continues to strengthen the group's position as an effective international forum, and decided on greater enforcement cooperation. The conference will make its Enforcement Working Group a permanent body so that members are able to share lines of inquiry, analysis of issues and tactics, both in general and in concrete ongoing investigations.

Gathering 120 jurisdictions together in Tirana, Albania, the conference aims to strengthen relationships with other international bodies and networks. *Steve Wood*, UK ICO's Deputy Commissioner told *PL&B* that this will mean enhanced information exchange and focusing on key areas, as well as issuing template Memorandums of Understanding. The conference will help new and smaller members by making sure future conferences will also discuss practical data protection issues. The ICO will continue as the Conference Chair for the next two years.

Elizabeth Denham, UK's Information Commissioner said the conference will open up to engage more with external stakeholders, in particular civil society, in a new reference panel to be formed in 2020.

The members aim to further develop their information exchange and identify any legal impediments that relate to enforcement cooperation. A new permanent online public repository section on the ICDPPC website will be established that links to publicly available enforcement cooperation resources. To ensure that this repository remains up to date, the DPAs will create a small dedicated team or task force. The repository will have two distinct sections:

- One for members to share links to non-confidential, publicly available information, including, but not limited to, press-releases, publicised research, policy documents, court judgments, guidelines, relevant technology developments, decisions, enforcement tools and applicable laws. The information to be shared in this section is relevant to Enforcement Cooperation but may also be relevant to policy development, and does not necessarily have to be limited to documents created by ICDPPC members.
- The other is to be a place that provides links to resources and tools associated with various privacy and data protection related networks, such as – importantly – the Conference. One example of such resource could be the ICDPPC Enforcement Cooperation Handbook.

Resolutions

The conference passed several resolutions[1]:

- on the conference's strategic direction (2019-21);
- on privacy as a fundamental human right and precondition for exercising other fundamental rights;
- on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement;
- on social media and violent extremist content online;
- to support and facilitate regulatory co-operation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the digital economy;
- to address the role of human error in personal data breaches.

Enforcement panel

In a side event, organized by OneTrust Data Guidance, speakers addressed global enforcement trends. *Alexis Kateifides*, Global Privacy Director at OneTrust DataGuidance said that there are several current developments in privacy laws globally, for example Panama has a new law and Chile is considering a bill. Uganda has a new law since May and we expect to see a new law in Egypt soon. Bahrain has a new law since August but no authority has yet been appointed.

Alan Raul, Partner at Sidley Austin, said that in his personal view, the US poses a significant enforcement risk. "It has been said that the Facebook settlement was not adequate but it was nine per cent of its annual global revenue," Raul stressed. There are now 50 US state breach reporting laws, but they have different standards which makes it difficult for consumers. Greater harmonisation such as the GDPR is good for everyone, Raul said.

Brent Homan, Assistant Commissioner, Office of the Privacy Commissioner of Canada, said that Canada now has a federal law on data breach reporting. Since reporting became mandatory, the number of data breach notifications has skyrocketed. Some of those reports have involved well-known corporate names, but there are also significant volumes coming from small and medium-sized businesses.

Over 60% of the cases involve unauthorised access. There have been some serious breaches in the financial sector, Desjardins and Capital One, for example. The remedies offered are typically 1-2 years of credit monitoring.

Guilherme Roschke, Counsel for International Consumer Protection at Federal Trade Commission, offered his personal views on US enforcement. "This year has been incredibly significant. A fine of $5 billion was imposed on Facebook. Then there was the Equifax settlement. The FTC orders are much more detailed now than before, with an increasing recognition of accountability - it's being built into enforcement. This is an extension of traditional FTC practice," he said.

The FTC has worked to develop the Global Privacy Enforcement Network's soft cooperation. Regular conference

calls take place to discuss enforcement trends, there is an annual workshop, and the GPEN alert network – a confidential area to discuss investigations.

When might we see a US federal privacy law? (p.11) Intense work is going on, and we have seen EU stakeholders such as European Data Protection Board Chair, Andrea Jelinek, and Ireland's Data Protection Commissioner, Helen Dixon, testify in Congress. However, Congress can wipe out state laws in the area if they would be conflicting. The new California law will take effect before any federal law will be ready, and some other state proposals also look similar to GDPR.

Laura Flannery, International Affairs and OSS Operations at Data Protection Commissioner Ireland, spoke about the EU GDPR One-Stop-Shop. The GDPR has had a huge impact. We have seen an increase in complaints and 4,000 breach notifications. In Ireland, we need to handle all complaints as this is required by our law, she said.

The EU-level regulatory cooperation in cross-border cases involves a steep learning curve. There are huge advantages to learn from others and Ireland wants to take advantage of these models. "Having said that, there are challenges. We have a common law system and some other countries have a civil law system. Our system has the right to be heard and some other countries do not provide this, or it is not a standard practice."

The expert meetings in Brussels are very helpful, she said. The consistency mechanism has not really been tested yet. So there are opportunities and challenges.

The EU will review the working of the GDPR in 2020. The Commission has invited jurisdictions to provide feedback. Further aspects to consider are the EU e-Privacy Regulation which is still to come, and Brexit.

INFORMATION

See privacyconference2019.info/ and privacyconference2019.info/conference/side-events/

REFERENCE

1 privacyconference2019.info/closed-session-documents/

DPAs adopt guidelines on the EU GDPR's territorial scope

The European Data Protection Board has now finalised its guidance on the somewhat controversial topic of territorial scope under the GDPR's Article 3 and the concepts of "targeting" and "establishment". The DPAs say that simply having an employee in the EU does not mean that the processing falls under the GDPR; it must be carried out in the context of the activities of the EU-based employee. Although the notion of establishment is broad, it is not without limits. It is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking's website is accessible in the Union, the DPAs say.

Also, the inadvertent or incidental offering of goods or services to individuals in the EU, for example to non-EU individuals travelling in the EU, does not trigger the GDPR.

There are other useful clarifications. The guidelines also include 25 real-life scenarios, and have been modified in light of the feedback received from stakeholders.

- *The guidelines, adopted on 14 November are at edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf See edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf*

Spain adopts new cookie guidelines

The AEPD, Spain's Data Protection Authority, has, on 8 November, published new Guidelines on the Use of Cookies. The Guidelines, prepared together with the marketing and online advertising industries, state that the definition of personal data also includes data processing when "unique identifiers are used that allow for the differentiation of certain users from the others, and to track them individually (for example, an advertising ID)." This consideration is particularly important for online business activities, law firm Hogan Lovells reports.

Some important aspects to note, Hogan Lovells lawyers write, include identifying types of cookies and which ones are exempt. "The exempt cookies are mainly cookies that are required for services requested by the user to operate, and technical cookies allowing the communication between users' terminals and networks. These are the cookies that do not trigger information duties or an obligation to obtain the user's consent. That said, and for transparency purposes, the AEPD recommends informing users about the use of these cookies at least in general terms."

The Guidelines advise on how to divide cookies into different categories and how to manage cookies. They also indicate the minimum information that must be provided to users about cookies Where information on cookies is not fully displayed to users on a Cookie Policy (which is less user-friendly), webmasters can divide the information to be displayed into two layers, with the second layer intended to provide more information to users.

- *See www.hldataprotection.com/2019/11/articles/international-eu-privacy/spanish-dpa-on-use-of-cookies-continued-browsing-is-consent/*

Accountability is crucial for effective protection of privacy

We need to understand and apply accountability – it is a global standard with great advantages for organisations and regulators. By **Christopher Docksey**, Honorary Director-General at the EDPS.

The principle of accountability means much more than simple compliance with legal requirements. Its key elements can be described as actively developing, demonstrating, and being able to demonstrate, compliance.

The recognition of accountability as a key concept has developed over many years in national and international law. It has been enshrined in the OECD Guidelines, the Madrid Resolution, the GDPR and Modernised Convention 108. It has also been the subject of influential guidelines by regulators across the world.

As a result, accountability is now a global standard. But it needs both legislation and explanation to be fully effective. It must be in the law - accountability is not self-regulation - and it has to be backed up by effective guidance.

The road to accountability

One pragmatic way of understanding accountability is to see it as a toolbox, full of useful tools. If we take the GDPR as an example, we can see a number of these accountability mechanisms. They are not merely legal requirements, they also represent best practice:

- privacy by design and privacy by default
- records of processing activities
- security measures and data breach notification procedures
- DPO/CPO
- DPIA /PIA
- codes of conduct
- certification

Too many people think that accountability, and these accountability mechanisms in the tool box, represent yet more legal obligations. However, we should see them as helpful tools rather than as extra obligations, as part of the solution rather than the problem. And the accountable organisation that uses these tools will find that it has carried out the core of its various legal obligations.

Another way of looking at accountability is as a philosophy: of being a responsible and ethical steward of personal information. There are various roads to enlightenment, to saying "Aha! I understand!" It can come to top management if they receive an effective message. Many senior managers realise that privacy, although it is an extra burden, is something that has to be done. It can also come from team members, sometimes by reminding managers that they are processing the personal information of fellow human beings. In Acxiom, the analytics team developed a model of "10,000 audience propensities", which included scores for sensitive personal information such as "erectile dysfunction" and "vaginal itch". The leadership team was discussing whether the use of such scores would be too invasive, when one member of the team announced that she would be able to read out the actual scores on these sensitive topics for each of the individuals in the room. Once confronted with this very personal information, the leadership team had their "Aha!" moment. They understood that these types of scores were too sensitive to be made available as a product to customers.

This story shows how important colleagues can be for raising awareness, and it reminds us that modern data processing can be very, very personal, and that managers need to take it very, very personally.

How to implement the principle of accountability

I would like to concentrate on four key elements of accountability.

First and foremost, organisations must take responsibility for the personal data that they handle. This starts with ensuring top management commitment, taking data protection seriously, being honest, and managing risks. Top management must then ensure that managers and colleagues at all levels have to give their support - otherwise a fine-sounding privacy policy will be a hollow shell.

Second, once there is that commitment, it is time to adopt a Privacy Management Program (PMP). It is not necessary to do everything at once, one can prioritise and handle the issues step by step. Accountability is a process, a responsibility that requires constant care and attention.

Third, the organisation has to have a privacy professional, the DPO or CPO, the person or the team who will assure internal implementation of the PMP. In its 2010 Opinion on Accountability, the Article 29 Working Party stressed that the DPO is the "cornerstone of accountability". This year, in the Stockholm Declaration, the Nordic data protection authorities recognised the importance of accountability and committed themselves to help ensure GDPR compliance by supporting DPOs in their important tasks.

Finally, I would stress the need to ensure the transparency of the measures in the PMP, for data subjects, regulators and the public. Transparency goes to the heart of the concept of accountability. Sometimes it is not the processing that is the problem so much as the lack of transparency to users. For example, if Google, Amazon, Apple and Facebook had announced they wanted to make recordings of their smart assistants, and to use human beings to check those recordings for quality purposes; if they had set out a clear framework of what they wanted to do, surrounded by safeguards, and had called for volunteers: then we would not have had the scandals this summer, with newspaper articles on 'Why are you snooping on me?' and 'Alexa, are you invading my privacy?'

The advantages of accountability

Accountability offers clear benefits to both organisations processing personal information and to their regulators.

For regulators, I would underline three reasons to encourage organisations to be accountable.

First, demonstrated accountability can satisfy the due diligence obligation of the regulator. Under accountability laws, the first thing the regulator can do is ask to see the accountability records. These records, or their absence, make it possible to distinguish between accountable organisations and organisations that have no clear overview of their processing activities, thus enabling the regulator to prioritise its investigatory work on the latter.

Second, accountability minimises over-reporting of data breaches. An accountable organisation will know when to notify and, more important, when not to notify. There is a huge difference between the percentage of data breaches that people assume should be notified (100%), and the percentage that actually have to be notified after good incident risk preparation and assessment (10%). Such knowledge represents a huge saving of effort for both regulators and organisations.

Third, accountability can work as a bridge between jurisdictions. Andrea Jelinek, the Chair of the European Data Protection Board, has noted that accountability can help bridge jurisdictional and legal differences by creating interoperability. It can facilitate transnational investigations by providing a more uniform environment, based on mutually agreed or commonly accepted privacy and implementation standards.

However, as many regulators already know, this means a new type of work for regulators. They have to invest resources in accountability, be creative, and think how to help controllers understand. Many regulators of all sizes have already identified where support is needed. For example, in Guernsey the regulator organises popular "drop-in" sessions for controllers every other Wednesday morning. In Madrid the Spanish regulator has developed the 'Facilita' software tool to help small and medium size enterprises deliver an adequate level of data protection.

So regulators have a lot of accountability work to do, to provide leadership, support and guidance.

For organisations, I would underline four reasons to be accountable.

First, accountability prepares for the known unknowns – Subject Access Requests, data breaches, complaints and investigations. The GPEN Data Sweep in 2018 shows that there is a real need here, because a number of organisations had no processes in place to deal with the complaints and queries by data subjects, nor were they equipped to handle data security incidents appropriately.

Second, accountability helps when the regulator calls, because there will be a documented privacy policy to show the regulator. Regulators will take demonstrated accountability into account when carrying out investigations and enforcement. For example, the Singapore regulator's Model AI Governance Framework states that adopting the voluntary Framework will help to demonstrate that an organisation has implemented the necessary accountability-based practices. Indeed, legislation could even provide a Safe Harbor one day, as can be seen in the IAF model accountability law[1], which states that an accountable organisation that has satisfied the requirements of a privacy impact assessment or a code of conduct should not be subject to civil penalties.

Third, accountability can provide a competitive advantage. A strong privacy policy on the website means consumer trust and a strong reputation. The EDPS has argued strongly that accountable firms should gain a competitive advantage from being fully accountable.

Fourth, accountability provides a methodology for dealing with the game-changer of Artificial Intelligence. The accountability toolbox is already available, it provides the tools to respect privacy and to develop AI at the same time. For example, risk assessment (an automated decision-making with legal or significant effects on data subjects will always trigger a DPIA under the GDPR), privacy by design and privacy by default (ensuring that meaningful human review will be designed in from the outset), and transparency (to provide information on the values that underpin automated decisions).

Accountability when things go wrong

Finally I should mention the disadvantages of not being accountable when things go wrong.

For most controllers, who want to do the right thing, accountability means preparing in advance, organising security, and putting all the necessary procedures into place. An accountable organisation, which has put in place robust programmes, is in a good place when things go wrong and the regulator calls.

However, if you fail to plan, you plan to fail, and when something goes wrong, you will be sanctioned, even fined: as Marriott and British Airways have found out in 2019, courtesy of the ICO.

Indeed, administrative fines should and will be used to support accountability. For example, the GDPR uses the same risk-based approach for both accountability and for fines, referring to "risks of varying likelihood and severity for the rights and freedoms of natural persons." An accountable organisation will have taken these risks into account; if not, it risks being fined.

Moreover, the GDPR specifies that fines may be imposed for failure to implement the accountability mechanisms in the Toolbox. It is a mistake to assume that accountability tools are too abstract for fines: on 27 June 2019 the Romanian regulator fined UniCredit Bank the equivalent of 130,000 for failure to implement Privacy by Design.

Fines have a particular significance for organisations that resist compliance or that merely pretend to be accountable. An organisation is not accountable if it hides behind consent, and says one thing in its PR and its privacy policy, but does something else in the research lab and on the website. Accountability is not about treating the risk of noncompliance as a business risk to be factored into turnover forecasts. Such organisations can be faced with three consequences in particular.

First, fines have been calibrated for these organisations to be horizontal in scope and potentially very high. For example in the EU the GDPR has powerful, competition-level fines, first imposed by the CNIL against Google

in January 2019 (€50 million). Regulators in Germany have recently developed a new model for calculating fines, set on the high side so as to be particularly dissuasive.

Second, in addition to fines, such organisations can be subjected to enforced accountability. For example, the FTC has recently imposed significant fines on Equifax ($575 million) and Facebook ($5 billion). There is disagreement whether even these high fines are sufficient and whether other remedies should have been imposed to address incentives and the business model itself. However it should be noted that in these two cases the FTC also imposed accountability mechanisms: the Equifax Board must obtain annual certification that it is complying with the FTC order, and the Facebook settlement imposes independent accountability mechanisms at all levels - a new independent Privacy Committee at Board level and Compliance Officers at operational level.

Third, research on corporate psychology has shown that even high fines are not as persuasive as damage to the business. Companies can absorb even high fines as costs of doing business, but they do care about making profits, and if their reputation suffers, it can harm their sales.

Finally, if an organisation ends up in court, it is increasingly likely that it will be held to account. Courts across the world are becoming more sensitive to enforcing privacy and data protection.

In *Riley v California*, 2014, the US Supreme Court warned that "privacy comes at a cost." In *Puttaswamy v India*, 2017, the Indian Supreme Court emphasized that "Privacy is the constitutional core of human dignity". In this ruling the Supreme Court insisted that India should develop a "robust regime" of data protection, including, specifically, accountability, and indeed accountability can be found in Section 11 of the ensuing Indian Data Protection Bill.

In the EU, the case law of the Court of Justice since *Google Spain*, 2013 has deliberately applied the data protection rules as broadly as possible in order to ensure "effective and complete protection of the persons concerned." This time last year, at the 40th International Conference in Brussels, the President of the Court of Justice of the European Union, Koen Lenaerts, said that the Court is attached to "high levels of accountability" of individuals that process personal data, in light of the "central theme" of accountability in the GDPR. It is worth looking at the recent EU rulings on transparency, tracking and consent in *Wirtschaftsakademie*, *Fashion ID* and *Planet 49*. These rulings may well signal a tipping point for the present economic model of private surveillance.

A lot has been achieved, but there is still much work ahead. Accountability has been established as a world-wide principle, developing across the globe. I hope we will see more and more legislation on accountability and on increased powers for regulators, who, once empowered, have to breathe life into what it means.

Accountability is crucial for protecting personal data in the digital age. It requires organisations to understand and mitigate the risks their data processing creates, and it weaves data protection into their cultural and business fabric.

Finally, an accountable organisation will develop naturally towards "Accountability 2.0". This is about more than avoiding risk to customers. It is responsive, creating value for individuals and society as well as for organisations; it is transparent about what it is doing, and why, and it is ethical, because data controllers are aware they are processing the personal information of fellow human beings.

As former European Data Protection Supervisor, Giovanni Buttarelli said: "Not everything that is legally compliant and technically feasible is morally sustainable".

INFORMATION

This is an edited version of Christopher Docksey's keynote speech at the 41st International Conference of Data Protection and Privacy Commissioners in Albania in October. The full speech and slides can be seen at privacyconference2019.info/closed-session-documents/

AUTHOR

Christopher Docksey is Honorary Director-General at the EDPS, a member of the Guernsey Data Protection Authority, the Advisory Board of the Maastricht European Centre on Privacy and Cybersecurity, and an editor of the OUP Commentary on the GDPR.

REFERENCES

1 informationaccountability.org/category/iaf-model-legislation/

DP code of practice for digital identities in Africa

With the increasing deployment of digital IDs by governments in African countries, there has been an increase of complaints about perceived privacy violations. *The Data Protection Code of Practice for Digital Identity Schemes in Africa* aims to apply across all identity schemes from passport applications to national ID card schemes such as those introduced in Ghana and Kenya.

The authors stress Privacy by Design and Default, and the code can be used to check that privacy considerations have been taken into account from the start. Privacy Impact Assessments, and consultation with privacy authorities are additional recommendations. Ultimately, the lack of knowledge and information has been in the way of implementing effective privacy standards and the code is a step in the right direction, the authors say.

• *The code is published by Africa Digital Rights Hub ISBN: 978 - 9988 - 54 - 744 see t.co/E5zMU3JTrW*

Indonesia clarifies data localization, right to be forgotten

Andin Aditya Rahman of Assegaf Hamzah & Partners assesses the changes made recently to the legislative framework in Indonesia.

Nearing the end of the previous term of President Joko Widodo's Indonesian government, in October 2019, the government issued Government Regulation No. 71 of 2019 on Organization of Electronic Systems and Transactions (GR 71/2019), which repeals and replaces Government Regulation No. 82 of 2012 on the same matter (GR 82/2012). As had been anticipated, GR 71/2019 was issued to change provisions previously under GR 82/2012 to conform to the latest amendment to Law No. 11 of 2008 on Electronic Information and Transactions under Law No. 19 of 2016 (EIT Law). Government Regulations are the second-highest form of Indonesian legislation, after Laws made by the legislature.

However, GR 71/2019 does not repeal any existing implementing regulations of GR 82/2012. It is expected that the Minister of Communication and Information Technology (MCIT) will update these existing implementing regulations to conform with GR 71/2019.

Data localization

Prior to GR 71/2019, electronic system providers for public services under GR 82/2012 were subject to data localization obligation for their data centres and disaster recovery centres, meaning that they must store all their data in Indonesia. Although the definition of public service is made clear in other legislation, there were different views on what is considered as providing public service because GR 82/2012 does not provide a definition of what is considered as public services stipulated by the MCIT contrasted with the definition in other legislation. GR 71/2019 no longer uses the term 'public service' for data localization.

GR 71/2019 removes this ambiguity by using the term "public electronic system provider", defined as the operation of electronic systems by any government institution, whether legislative, executive, or judicial, at the central and regional level, as well as other government institutions established by law. Public electronic system providers must manage, process, and store their electronic systems and electronic data in Indonesia. They may only conduct such activities overseas if the technology is not available locally.

On the other hand, private electronic system providers may manage, process, and store their electronic systems and data overseas, provided that they can be effectively supervised by the relevant government authority and law enforcement agency, as well as provide access to their electronic systems and data overseas.

Right to be Forgotten

GR 71/2019 elaborates further the Right to be Forgotten framework in the EIT Law. Pursuant to the EIT Law, electronic system providers are required to erase any irrelevant electronic information and documents if requested by the relevant person. GR 71/2019 provides two different right to be forgotten measures that may be requested: right to erasure and right to delisting.

Right to Erasure: Unless otherwise specified by law, a person may request deletion of the following data:

1. Data acquired and processed unlawfully or without the prior consent of the relevant person;
2. When consent relating to this data has been revoked;
3. Data no longer consistent with their original purposes (purpose limitation);
4. When the retention period has elapsed; or
5. Data has been disclosed in a way that has caused damages to the relevant person.

Right to Delisting: The right to delisting is for data to be removed from search engines based on a court determination. The relevant persons may apply for the right to delisting to their local district court, which must be accompanied with the following information:

1. Identity of the relevant persons, electronic system providers, and electronic systems;
2. Data requested to be delisted; and
3. Reasons for the removal of the data from the search engine.

Draft Bill

The Indonesian House of Representatives (House) has agreed with the MCIT to include the draft Bill on Personal Data Protection in the priority legislation list for next year, which is certainly an encouraging sign since the Bill has not been included in any of the priority legislation lists in the last four years.[1]

Furthermore, the newly appointed head of MCIT has shown commitment in expediting the discussion on the Draft Bill in the legislature, (the House) which he hopes to be enacted in 2020. This is following the Indonesian president's speech to the House back in August 2019, in which he asserted the importance of data protection and quoting from the film The Great Hack that data is "now much more valuable than oil".[2]

However, whether the Draft Bill is included in next year's priority legislation list remains to be seen, as the list has not yet been issued by the House.

AUTHOR

Andin Aditya Rahman is Associate at Assegaf Hamzah & Partners, Jakarta, Indonesia.
Email: andin.rahman@ahp.co.id

REFERENCES

1 Indonesia House of Representatives, "RUU Penyiaran dan RUU PDP Disepakati Masuk Prolegnas 2020," 5 November 2019, dpr.go.id/berita/detail/id/26349/t/RUU+Penyiaran+dan+RUU+PDP+Disepakati+Masuk+Prolegnas+2020 .

2 Kompas.com, "Draft RUU Perlindungan Data Pribadi Akan Diajukan ke DPR December 2019," 5 November 2019, https://tekno.kompas.com/read/2019/11/05/15270097/draft-ruu-perlindungan-data-pribadi-akan-diajukan-ke-dpr-desember-2019

Albania updates its data protection framework

Host country to the DPAs' international conference 2019, and striving to become an EU member, Albania looks into adopting GDPR requirements. By **Laura Linkomies**.

Albania's data protection law, applicable both to the private and public sectors, dates back to 2008. Amendments are now being prepared to introduce GDPR-style provisions.

Albania is a member of the Council of Europe, and has ratified the Council of Europe Convention 108, which entered into force in Albania on 1st June 2005[1]. "As regards the ratification of Convention 108+, we are ultimately committed to making all possible efforts in this respect," Besnik Dervishi, Albania's Information and Data Protection Commissioner told *PL&B* in an interview.

"Both Convention 108+ and the EU General Data Protection Regulation (GDPR) are key aspects in the short-term strategy of the Commissioner's activity." Albania has applied for technical assistance with the European Commission's Instrument for Pre-Accession Assistance (IPA), in order to receive assistance to draft or amend the current law, and to integrate all the innovations contained in the GDPR. We have anticipated, in our National Plan for European Integration, the adoption of the new aligned law in 2020; hence we expect to complete the process in the next couple of months, Dervishi said.

Albania's data protection law has followed the EU Data Protection Directive 95/46 since 2012. "We have since identified the novelties introduced by the GDPR, such as the right to be forgotten, data breach notification, territorial scope and its outreach to third countries with respect to European data subjects, just to mention a few. In relation to some of these new principles, we have attempted to address them by introducing by-laws adopted by the Commissioner."

For example, to level the playing field for data controllers which are subsidiaries to international companies, and already applying the GDPR, Albania has partially implemented the data breach notification provision.

Awareness raising a priority

The Commissioner's Office is responsible for enforcing both data protection and freedom of information laws. Last year, the Commissioner's Office celebrated its 10th anniversary. "Over the first years of its activity, the authority strived to establish itself and raise awareness regarding the activity of the Commissioner's Office; hence the number of complaints received was quite limited, ranging from 25-36 complaints per year. As of 2014, our awareness efforts have increased significantly, and as a result, a tenfold increase in the number of complaints has occurred", Dervishi said. "It is worth noting that the figures relating to complaints should be understood as complaints handled at the procedural level, as opposed to the very high number of different requests for legal assistance or other types of requests by data subjects or data controllers that the office processes in the course of the year."

> We have anticipated, in our National Plan for European Integration, the adoption of the new aligned law in 2020.

"Public awareness campaigns are among our key priorities. We have conducted several successful campaigns that have been widely recognized. Last year, at the 40th International Conference of Data Protection and Privacy Commissioners, we were the winner of the 'Education and Public Awareness' category. We organise campaigns targeting elementary and secondary schools, as well as large parts of private and public universities. Alongside the education sector, we've carried out campaigns in the healthcare sector, as it is another sensitive area requiring enhanced awareness. This campaign was quite broad and it was ultimately finalized with training for all public and private controllers operating in the domain. Beside these areas, our focus has been the financial sector, as well as telecommunications and insurance companies. In addition to building on our close co-operation with various justice sector stakeholders, we have conducted joint awareness activities with the National Chamber of Notaries, the National Chamber of Advocacy, and the National Chamber of Mediators. So we have sought to include all the key sectors within our awareness efforts."

In October, the office organised the International Data Protection Commissioners' Conference in Albania. Commissioner Dervishi told *PL&B* that the Conference was a landmark event for Tirana, not only in terms of size and scale, but also as regards its content, ultimately attracting attention from all over the country, with press and media being particularly interested in this event. Some 36 representatives from international media followed the conference, and many local ones too such as *Albanian Daily News* which is among the only press outlets in Albania providing daily news translated into English, and Scan TV, a television station based in Albania, specialising in economic and financial news.

"The 41st ICDPPC Closed and Open Sessions welcome speeches were broadcast live by all the major TV channels in Albania, including the keynote addresses of some of our prominent speakers, most notably the presentation delivered by Microsoft's

Brad Smith, which attracted a lot of interest. News reports were also published during the conference week in several newspapers."

Enforcement

"I believe that no data protection authority's end purpose is to impose sanctions, and building on this, we strive to find a solution acceptable for the parties within the requirements of the law. The Commissioner has the power to seek information from data controllers, and they are required to comply in a timely manner and provide all the requested information. The Commissioner also has other legal instruments at his disposal, such as blocking the unlawful processing of personal data, or imposing administrative sanctions, which vary from 10,000 Albanian lek up to two million lek (up to €16,000). The Commissioner may also issue recommendations when he does not identify a violation, or encounters minor infractions which are not subject to administrative sanctions. Controllers must, however, observe these recommendations and report to the Commissioner about their implementation."

Administrative investigations totalled 190 in 2018. So far this year, 126 have been launched. The administrative process is triggered and concluded by the Office of the Commissioner with the decision made by the Commissioner. The decision-making of the Commissioner is subject to a judicial review, and the competent court is the Administrative Court which reviews the actions taken by the Commissioner if challenged by the parties, Dervishi said.

The Commission performs sector-specific inspections especially in the education sector, healthcare, banking, telecommunications, and issues sanctions and sector-wide recommendations based on these audits. "For example, following the administrative inspections that we have conducted with the banking sector, we issued a recommendation for this sector."

The Commission has so far issued guidance for the banking sector, healthcare system, education, CCTV, etc. Speaking about the work programme for Albania's Data Protection Commission for 2019-2020, Dervishi said that in 2019 the ICDPPC was amongst the key priorities. Now many post-event tasks follow.

"As far as the other priorities in our 2019-2020 work programme are concerned, they are ratification of Convention 108+ and the transposition of the GDPR into our legislation and practices."

EU membership application postponed so far

In October, the EU Council of Ministers decided not to start negotiations with Albania about Albania's accession to the EU.

"I am obviously not entitled to provide a political view. Nevertheless, I would like to state that this is certainly not good news. The opening of negotiations with the EU would definitely have a positive impact on the activity of all the institutions in Albania, including the Commissioner's Office, as our work is closely tied with international developments, particularly with regard to the global convergence of data protection and privacy rights. We have close relations with the Data Protection Unit of the European Union, and our office is a permanent observer to the European Data Protection Board. Based on the ambitious plan made in 2016-2017 that Albania would ideally accede to the EU by 2025, we had discussions with the EU Data Protection Unit on a possible adequacy decision for our country. Following negotiations with the EU Data Protection Unit, we submitted a full and extensive report."

"The EU's decision to not open negotiations compels us to rethink our position and probably to contact the EU Data Protection Unit again, in order to prevent this handicap from hindering the activity of our institutions, specifically *vis-à-vis* local and foreign data controllers and processors. It is also important to stress that the Commissioner's Office is strongly engaged in the European integration process of our country, partaking in Chapter 23 of the country's annual progress report "Judiciary and Fundamental Rights", as well as Chapter 24 "Justice, Freedom and Security" and Chapter 10 "Information Society and Media", the latter regarding the interplay between the information society and the protection of personal data, and the access or re-use of public sector documents. Moreover, in our capacity as the national data protection regulatory body, we are regularly consulted on legislative proposals or other data protection aspects by national institutions involved in the integration process."

International cooperation

Albania's main references, when drafting, implementing and modernising the Albanian data protection law have been Convention 108 and the EU GDPR. Albania has close co-operation in place with several counterparts formalised through co-operation memoranda, the latest having been signed with the Italian Data Protection Authority (*Garante*). "I consider it successful in terms of exchange of know-how, information and joint handling of cases," Dervishi said.

"The Commissioner's Office is closely involved in international data protection co-operation networks. To date, there is not a Balkan group of data protection authorities. However, we have close ties of partnership and collaboration especially with the Western Balkans authorities of Montenegro, North Macedonia, Kosovo, and Bosnia and Herzegovina not excluding the fruitful cooperation we have with Italy, Croatia, Slovenia, and Greece."

INFORMATION

See www.idp.al/?lang=en
and www.idp.al/annual-reports/?lang=en

REFERENCE

1 www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cW4vw16P

Malta applies its new GDPR style law in a pragmatic way

PL&B talked to Malta's Information and Data Protection Commissioner, Saviour Cachia, about changes in their legislative framework. By **Laura Linkomies**.

Malta's new GDPR-style law, Data Protection Act 2018 (Chapter 586 of the Laws of Malta), took effect on 28 May 2018. It follows and implements the GDPR and includes derogations for processing for archiving purposes in the public interest, scientific or historical research or statistical purposes, and journalistic purposes.

The law lowers the age at which a child can consent to online services, and is currently 13. Other new aspects include data breach notification, and a fines regime for public entities. Depending on the type of infringement, public sector bodies can be fined up to €25,000 or up to €50,000, and may incur a daily fine of €25 or €50 for each day the violation persists. In addition to the GDPR-style fines, the law stipulates that any person who knowingly provides false information to the DP Authority's (DPA) investigations or does not comply with a request for an investigation, can be subject to a fine between €1,250 and €50,000 and/or imprisonment for six months.

On special categories of data, there are special rules regarding processing of personal data for health insurance purposes in the Maltese Subsidiary Legislation 586.10, prompted by the fact that consent is not considered to be freely given in this area.

Enforcement

Previously, the Commissioner's Office had mostly conducted enforcement in the style of education and awareness-building rather than issuing large fines. Whilst the fining power was already there, the new law and the strengthened enforcement powers have also affected Malta's style of enforcing the law. Cachia said that his decisions on fines are influenced by various factors, e.g. the kind of data which has been breached, whether the act was repetitive, whether there was true negligence in the organisation's compliance or whether it was a one-off human error. Fines are issued on a case-by-case basis. Since the new law entered into force, 21 fines have been issued, the highest amount being €15,000 for infringements relating to the sending of unsolicited marketing communications, the right of information to data subjects, and the data controllers'/processors' obligations.

When asked about a uniform EU fining regime, Cachia said that this is a very difficult area in which to achieve harmonisation as countries and situations are different. In Malta most controllers are SMEs and, any fine imposed will be effective, proportionate and dissuasive. The DPA will take into account certain considerations when determining the amount of the fine, including but not limited to, the general conditions set out under Article 83 of the GDPR.

> Fines are issued on a case-by-case basis. Since the new law entered into force, 21 fines have been issued, the highest amount being €15,000.

Malta's Information and Data Protection Commissioner, Saviour Cachia, told *PL&B* that other subsidiary legislation is now under review due to the new data protection provisions. The government consults the office with regard to data protection matters and there is a good working relationship.

Data breach notification has really taken off. Controllers in the financial services sector were making breach notifications even before the GDPR entered into force, Cachia told *PL&B*. At first, there was some over-notification, but this has now settled down. The office has posted a breach notification template on its website, which organisations can use to deliver the first details of the breach to the regulator, who will then follow up with more questions if need be. If there is no risk to individuals' rights and freedoms, a breach does not need to be notified.

Organisations in Malta are now getting better at conducting risk assessments. Malta's authority investigates all complaints, including individual cases – data subjects expect that, Cachia said. Audits will be on the cards but no particular sectors have been identified. "Trends in complaints and investigations will drive the audit activity."

One of the sectors where there have been many complaints is the gaming industry which is an important area for the Maltese economy. In 2018, the authority received in total 76 complaints, a marginal increase when compared with pre-GDPR times.

The focus on awareness-building continues and the office has applied for EU funds, issued under a restricted call for data protection authorities, for this purpose of raising awareness and assisting SMEs in complying with the requirements of the Regulation. Cachia said that much work is needed to inform organisations about cyber security threats, particularly as SMEs do not have sufficient knowledge in this field, or funds to put extra security in place.

Malta's authority has so far issued guidelines in the sectors of banking, gaming, political campaigning and credit referencing.

International cooperation

Despite its small size – Malta's authority is EU's smallest with eight technical members of staff working both on data protection and freedom of information matters – the office actively participates in the work of the European Data

Protection Board. "We have to be very selective. However, we currently take part in the technology and law enforcement subgroups, and the fining taskforce. We also chair a SiS II[1] Supervision Coordination Group," Cachia said.

The Commission has found the EU DPAs' new IT platform for the implementation of the consistency and cooperation requirements between EU Data Protection Authorities very useful, as it saves time not having to duplicate investigations. There have already been some cross-border cases. These are sometimes difficult to investigate, Cachia said, in terms of identifying the controller's and data subject's true location. Malta has been the Lead Supervisory Authority in several cases.

"The consistency mechanism saves us time and has been a successful development for cross-border cases. But the results depend on the level of complexity – with the tech giants this is a lengthy process," Cachia said.

The office has been involved in one application for Binding Corporate rules for an organisation in the health sector. In this case, the Maltese DPA was acting as a lead authority and approved the BCR of Cardinal Health Inc.

Going forward

The number one priority in terms of advising Maltese companies (in addition to cyber security) is now individual rights, dealing with Subject Access Requests, and providing the information required for transparency purposes, as well as, data protection by design and default.

The office is also actively looking into data protection issues in connection with Artificial Intelligence. The government recently published a national strategy for AI, and it is proposed that the DPA will set up a regulatory sandbox environment to support organisations that need to use personal data in the process of developing or testing innovative products and services in the specific area of Artificial Intelligence. Participants will be guided and assisted by professionals on how to apply data protection rules and requirements to their projects and be given assurances, to the extent possible, that such projects do not infringe the provisions of the GDPR. The scope of the sandbox is to give a certain level of comfort from enforcement action. Projects will be assessed on the degree of demonstrable benefit that they will potentially deliver to the public.

INFORMATION

Malta joined the European Union in 2004, and the Eurozone in 2008.
See Malta's DPA at:
idpc.org.mt/en/Pages/Home.aspx
The law is available at justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12839&l=1

REFERENCE

1 Schengen Information System edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en

Russia introduces fines for infringing data localization rules with amendments to DP Act

The Federal Law No. 405 of 2 December, which establishes new administrative sanctions, is now in force.

The law, "On amendments of certain laws of the Russian Federation", sets fines for failure to localize personal data of Russian citizens on the territory of Russia and for repeated failures of certain provisions of information legislation. In particular, these administrative sanctions concern two laws:

- Federal Law No.149 "On information, information technologies and protection of information" of 27 July 2006
- Federal Law No. 152 "On personal data" of 27 July 2006

This is the first law to set administrative sanctions for failure to comply with the localization rule. However, the obligation of personal data operators to localize personal data of Russian citizens on the territory of Russia appeared in Federal Law No. 152 "On personal data" of July 27, 2006, almost 15 years ago.

The table below shows the new fines included in the Russian Code of Administrative Offenses (the Code).

The law also sets high fines for repeated violation of certain provisions of Federal Law No. 149 "On information, information technologies and protection of information" of July 27, 2006 committed by: Owners of organizers of information dissemination (e.g., social media, email services, cloud services) up to 6 million roubles (€85,000); Messenger owners up to 2 million roubles (€25,000); Search engine providers up to 5 million roubles (€70,000); Owners of audiovisual services up to 5 million roubles.

• *By Victor Naumov, Office Managing Partner and Vladislav Arkhipov Counsel, Dentons, Russia*
Emails: victor.naumov@dentons.com
Vladislav.Arkhipov@dentons.com

Part of Article 13.11 of the Code	Description	Liability of legal entity (in roubles)	Liability of officer in roubles
New Part 7	Failure to comply with the localization requirement	2,000,000 to 6,000,000 (up to €85,000)	200,000–500,000 (up to €7,000)
New Part 8	Repeated failure to comply with the localization requirement	6,000,000 to 18,000,000 (up to € 254,000)	500,000–1,000,000 (up to €14,000)

Advances in South Asian DP laws: Sri Lanka, Pakistan and Nepal

South Asia is slowly catching up with the rest of Asia in privacy law developments.

By **Graham Greenleaf**.

Five years ago, the only significant data privacy laws in South Asia (or SAARC, the South Asia Area of Regional Cooperation) were India's new and extremely limited private sector law, and Nepal's public sector law. The region's data privacy protections were far more limited than in North-east Asia or the ASEAN countries.[1] India continues to prevaricate, but is expected to introduce a modernising Bill in the 2019 winter Congress sessions. Meanwhile, in addition to the Sri Lankan Bill which is the focus of this article, Bhutan and Nepal have enacted privacy laws, and Pakistan has a private sector Bill. Bangladesh, Afghanistan and the Maldives continue to be the states in the SAARC region where there are no significant developments.

Sri Lanka's GDPR-inspired Bill

What is said to be the final draft of Sri Lanka's Personal Data Protection Bill[2] was released on 24 September 2019 by the Ministry of Digital Infrastructure and Information Technology (MDIIT). The previous "Data Protection Framework",[3] released in June 2019, has been modified after government consultations with stakeholders.[4] Once enacted, its various provisions must be brought into force within three years, or 18 months for the formation of the DPA (s. 1).

Scope and exceptions: The Bill is comprehensive in that it covers both the public and private sectors (s. 3, s. 4). It appears to have extra-territorial effect in similar terms to the GDPR art. 3 (offers to or monitoring of persons in Sri Lanka: s. 3(1)(iv) and (v)), but is actually much more limited because it only applies where the processing of the data "takes place wholly or partly within Sri Lanka" (s. 3(1)(a)).

Although the Bill reserves significant powers to make delegated legislation to the Data Protection Authority (DPA) (ss. 19(1)(B), 22(2), 28(q), 29(h), 31(1)(b) etc), the Minister of MDIIT (s. 25(2)), or the Secretary of MDIIT (ss. 31(6), 43(1), 43(2) etc), there are no outright exceptions to its provisions for either public or private sector entities. In addition, any "exceptions, restrictions or derogations" to its provisions are not allowed unless provided by law and "respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society" for protection of various public interests (listed (a)-(f)) (s. 35). However, s. 35 does not specify the sources of legitimate "exceptions, restrictions or derogations", creating the risk that it might authorise unspecified exceptions other than those legitimated by existing statutory provisions (in this Bill or other laws), so this needs to be clarified. The broad regulation-making powers in s. 43 are particularly dangerous unless it is clarified that such regulations may not derogate from the right and protection of data subjects in the Bill. This is particularly so when the "fundamental rights and freedoms" referred to in s. 35 do not include privacy rights in Sri Lanka.

The Bill is also comprehensive in that it defines "personal data" by a conventional definition in terms of identifiability, but over-inclusive in that "data subject" includes persons "alive or deceased" (definitions, s. 46) with no time limit based date of death. "Special categories of personal data" are defined by an extensive list including genetic and biometric data (definitions, s. 46).

The only exceptions to the data covered are for the usual "personal, domestic, or household" use exception, and for anonymous data ("irreversibly anonymized in such a manner that causes the individual to be unidentifiable") (s. 3(2)). The use of "irreversibly" makes this a more strict standard of anonymisation than the GDPR, which allows "all the means reasonably likely to be used" to re-identify data, taking into account current technology, to determine whether data has been anonymized (GDPR, recital 26), rather than imposing an absolute requirement which may be impossible to meet.

Principles with strong GDPR influence: The Bill does require lawful grounds for processing to take place at all (s. 5). Schedules I, II and III set out many similar grounds to those in the GDPR (including for special/'sensitive' data). The ground of consent (Schedule 1(a)) makes it appear that blanket consent to processing (i.e. not only for a specified purpose) is allowed, but s. 6 requires processors to ensure that processing is only for "specified" and "explicit" purposes, and that further processing is not incompatible with such purposes. The Minister, with the concurrence of the DPA, may expand any of these Schedules, by disallowable regulations (s. 43).

Obligations of controllers and processors: Among many aspects of the Bill reflecting the influence of the GDPR are the requirements on controllers of proportionality in processing (s. 7(c)); minimality of processing, but only in the very weak form of 'not excessive' (s. 7(d)); and limited retention (but the word 'only' is missing) (s. 9). There is no absolute obligation to provide an appropriate level of security, but only an obligation to follow prescribed security measures (s. 10), defined by the Minister or the DPA. Data breaches must be reported, and the DPA is to specify when such reports must be made to it, and to the data subject (s. 22).

The previous draft included mandatory registration of controllers, but in the latest draft this has been replaced with a version of demonstrable accountability (s. 12), described as a "Data Protection Management Program", and including numerous elements. Controllers must appoint Data Protection Officers (DPOs) (s. 20(1)),

where they are in the public sector, or in such private sector categories as the DPA decides requires a DPO, or processing involving monitoring, large scale special categories of data, or high risk processing is involved (s. 31). Private sector entities aggrieved by a DPA requirement to appoint a DPO may appeal to the Secretary of the Minister's department (s. 31(6)).

They must carry out a data protection impact assessment (DPIA) prior to carrying out any processing 'likely to result in a high risk to the rights and freedoms of a data subject as guaranteed under any written law' (s. 23(1)). Sri Lanka's Constitution provides in Chapter III various "Fundamental Rights" which could be relevant, but this would be infrequent, as they do not include a right of privacy, or a general protection of liberty (as in s. 21 of India's Constitution). The rights most likely to be relevant are the protections against numerous forms of discriminations (Constitution, art. 12(2) and (3)). Such DPIAs are required (and possibly only required) where processing involves large scale or systematic evaluation of personal data such as by profiling, monitoring of public spaces or telecommunications networks, special categories of personal data, or other circumstances prescribed by the DPA (s. 23(3)). The DPIA results must be given to the DPA irrespective of the outcome, for the purpose of the DPA assessing compliance with the law (s. 23(5)). If the DPIA indicates that processing will involve high risks despite any mitigation, the controller must consult with the DPA before proceeding (s. 24).

Unsolicited messages using personal data in any medium are prohibited, with prior consent, and a right to opt out, being required (s. 26).

Processors are required to only carry out processing on the instructions of a controller, and in accordance with the same obligations as controllers (or they will be deemed to be controllers), and must erase or return data after processing (s. 21).

Rights of data subjects: The rights of data subjects (Part II) expressed in terms familiar from the GDPR include, in addition to the rights of access and correction, the right to withdraw consent to continued processing (s. 13); "right to erasure" including the "right to be forgotten" where data is "no longer necessary" (s. 16). Where controllers refuse data subject requests they must (in this draft) inform them of their right of appeal. Appeals are initially to the DPA, and either the data subject or the controller may then appeal to the Court of Appeal (s. 18). There is no right of data portability.

The rights of the data subject to request a review of automated decision-making (s. 19) only apply if it "affects rights and freedoms … guaranteed under any written law" (a condition not found in GDPR art. 22). Unless such rights can be inferred from this Bill, this condition means that these rights will very rarely apply to the private sector, in areas such as employment, insurance etc, unless some other statutory rights are likely to be infringed, or the abovementioned constitutional protections against discrimination are infringed. This uncertain scope makes it difficult to evaluate the rest of the section. The application of the section to "special categories" (sensitive data) is also unclear.

Data localisation and export restrictions: Public authorities may only process personal data within Sri Lanka, unless the DPA and any relevant supervisory body classifies the data as permitted to be processed overseas (s. 25(1)). There is no such data localisation requirement applying to the private sector.

Private sector bodies may transfer personal data to a third country (or territory/sector within it) prescribed by the Minister (s. 25(2)). Otherwise, they are only permitted to process personal data outside Sri Lanka if they ensure compliance with specified sections of the Act (s. 25(3)), through a legally binding and enforceable instrument with the recipient, or one determined by the DPA (s. 25(4)). Such instruments will only allow enforcement by the exporting data controller, not the data subject, because the common law doctrine of privity of contract applies in Sri Lanka (even though its contract law is largely based on Roman-Dutch law). It is not clear that the section covers both transfers to another controller overseas, as well as to a controller processing data outside Sri Lanka.

A DPA without apparent independence: The Minister is empowered to "designate a Public Corporation, Statutory Body or any other public institution controlled by the government or established by or under any written law, as the 'Data Protection Authority of Sri Lanka'" (the DPA) (s. 27(1)). While this section would not preclude the Minister from designating a statutory body with guaranteed independence as the DPA, or prevent such an independent body being established by separate legislation, it also clearly enables the Minister to so designate a body with no such independence as the DPA.

This apparently intended lack of independence is underlined by s. 41, which provides that the Minister may convey relevant directions by the Cabinet to the DPA "in connection with the exercise, performance or discharge of its powers, duties and functions". Furthermore, there are no provisions in the Bill indicating that the DPA is to exercise its powers independent of the views of the Minister or the government. In similar vein, responsibility for the Act and its implementation is given to both the DPA (s. 27(3)) and the relevant Ministry (s. 2). This contradiction needs to be resolved.

Appeals against decisions of the DPA generally go to the Court of Appeal (s. 18(4)). However, appeals against DPA decisions on whether a DPO must be appointed go to Secretary to the Minister (s. 31(6)), which could also be considered to reduce DPA independence.

Broad enforcement powers, but financial risks limited: The DPA has broad powers of investigation (s. 28(b)-(d)), and powers to 'receive complaints, hold enquiries and to make determinations or orders (s. 28(f)). It can direct controllers or processors to comply with their obligations (s. 28(c)), including by issuing both negative and positive "directives" (injunctions) (s. 30(1)), enforceable by court orders if necessary (s. 30(4)).

The DPA may suspend a controller "from the carrying on of a business or profession or the cancellation of a licence or authority" for such purposes, to the extent the law allows (s. 32(5)). It remains to be seen whether this sanction will be used. The DPA is

not explicitly empowered to take the more direct approach of ordering suspension of particular forms of processing, but that could be implied by its injunctive powers.

The DPA also has powers "to establish standards in relation to data protection" (s. 28(q)) (except in relation to what constitutes "adequacy" for data exports: s 25(1)). It can enter into agreements with foreign states (s. 28(l)), and "recognize certification and certifying bodies" (s. 28(k)).

The Bill empowers the DPA to levy maximum fines for breach of 10 million rupees (US$55,000), to be doubled on subsequent breaches (s. 32). Factors to be taken into account are set out (s. 33), somewhat similar to GDPR art. 83(2). This is a considerable reduction from the previous draft, which included fines up to 2% of global turnover of companies in breach, or 25 million rupees (US$122,500), whichever is the larger. The two other GDPR-influenced laws in Asia vary on this point, with Korea having fines with maxima based on global turnover (like the GDPR, and with one example reaching US$5,400,000), but Thailand having a maximum fine equivalent to only US$160,000. Singapore already has maximum fines of S$1 million (US$730,000), and has levied one fine approaching that. Fines in the new Sri Lankan Bill therefore have relatively little bite.

The Bill does not include other common means of enforcement: there are no provisions for compensation to aggrieved data subjects (comparing adversely with GDPR art. 82, or the laws of Korea, Singapore or Hong Kong); nor are suitably qualified NGOs given the ability to take representative actions on behalf of data subjects (comparing adversely with GDPR art. 80, and laws in Korea, Thailand and elsewhere), except to exercise user rights if authorised in writing (s. 17(6)(c)).

Comparative analysis: To put the Sri Lankan Bill in perspective, it is useful to compare it with other data privacy laws in Asia, and to consider what prospects, if enacted, it might have to assist Sri Lanka to obtain a finding of "adequacy", or for it to accede to data protection Convention 108+.

If enacted, this would be the second "post-GDPR" law in Asia, following Thailand, but it is (as yet) not as strong an implementation as that law. With Korea's law, it would be one of the three strongest data privacy laws in Asia, at least until India or Indonesia enact their proposed Bills.

Adequate in GDPR terms? Whether Sri Lanka would wish to seek a finding of adequacy under the GDPR is not known. If it did so, the independence of the DPA would be the most obvious impediment. The ability of the Minister to allow data exports to selected countries would need to be restricted. Following Japan's adequacy assessment, it is not clear what other aspects of the GDPR are necessary in a third country's law.

Potential for Convention 108 accession: It is not known whether Sri Lanka wishes to accede to Convention 108+. If it does, the Convention requires acceding countries to meet all its substantive provisions (art. 4), which is not the case with 'adequacy' under the GDPR. Rights included in Convention 108+ which are not fully addressed in the Bill include the right to know the reasons underlying processing applied to the data subject (art. 9(1)(c)), including because of deficiencies in s. 19; and the right to object (art. 9(1)(d)), because s. 13(2) is too limited.

An unusual function of the DPA is to 'ensure domestic compliance of data protection obligations under international conventions' (s. 19(h)). The recitals to the Bill include references to its purposes being to "improve interoperability among personal data protection frameworks" and "respecting … applicable international legal instruments". These provisions might enable the DPA to impose additional obligations needed for 108+ accession.

Otherwise, the principal problems that Sri Lanka is likely to face in an accession application are the lack of independence of the DPA, and the extent of the discretionary powers of both the DPA and the Minister. Provided there is effective enforcement, the limited extent to DPA enforcement powers is unlikely to pose a problem.

Other South Asian developments

Bhutan enacted the Information, Communications and Media Act of Bhutan 2018[5] in 2017, in force from mid-2018. Although the data protection principles in the Act are stated briefly, they do more than give Bhutan a minimal data privacy law, because they include seven of the ten "second generation" principles found in the 1995 EU Data Protection Directive, and are thus a moderately strong law for the Asian region.

Nepal's idiosyncratic privacy law: Nepal enacted The Privacy Act 2018,[6] but it is not a data privacy law because it does not include most of the set of basic principles shared by all such laws since 1980. In addition, most of the twelve chapters only have a significant effect on information held by public bodies,[7] the definition of "personal information" only covers specific (although extensive) categories of information about a person, and not whatever information can identify a person, and there is no DPA created or designated, just enforcement through the District Court.

However, there are many provisions in the Act to which private sector bodies operating in Nepal should pay careful attention in order to avoid prosecutions or compensation claims. For example, personal data collected by bodies corporate may only be used 'for the purpose for which such data have been collected', or with consent, and some personal data cannot be disclosed without consent. This wide-ranging Act cannot be ignored, but Nepal still does not have a data privacy law covering its private sector.

Pakistan: e-Commerce Policy, and data protection Bill(s): Pakistan's Ministry of Commerce published a revised version of the country's e-commerce policy[8] on 13 November 2019. The Policy focuses on nine areas, including data protection, and ranging from fintech, to telecoms to consumer protection. It includes plans to establish a national e-commerce council to provide strategic direction. It states that "the Data Protection Bill 2018 is … at an advanced stage of consultations", but does not clarify whether this is a revised version of the Personal Data Protection Bill, 2018 (discussed below), or possibly will be more aligned with the GDPR. "Regions such as EU do not allow their enterprises to transact with companies of such countries

which do not offer same level of data protection which is available under the EU Regulations", the Policy notes. "Such disclosure will also include disclosure about the country/legal jurisdiction where such data will be stored and the purpose for which it may be used".

The Policy says that it "is essential to have effective data protection laws and enable the local digital industry to make proper use of the data generated in Pakistan", and that "Pakistan Data Protection Act & Cloud/Data Policy (under consideration) [are] to provide for data sovereignty, data localization and address issues relating to e-Commerce." There is no doubt some forms of data localization are on Pakistan's agenda, as they are in India and Sri Lanka.

The Policy also includes separate plans for 'a code of conduct applicable to all e-commerce businesses, which would require all e-commerce platforms to make full disclosures regarding data protection provisions on their websites and apps'.[9]

Personal Data Protection Bill 2018: This Bill[10] only covers the private sector ('information in respect of commercial transactions'). It is legislation which, at best might meet most of the requirements of a 'second generation' law (based on the 1995 EU Data Protection Directive), but relatively little from the additional "'third generation" requirements of the GDPR and Convention 108+. Of these, it includes a requirement of lawful ground for processing; some requirements of minimal processing ("necessary", "not excessive"); rights to withdraw consent to process personal data; rights to prevent processing likely to cause damage or distress; and a right to erasure. Sensitive data is covered, but not including biometric or genetic data. The Bill would establish a National Commission for Personal Data Protection (NCPDP) with independence ('shall enjoy operational and administrative autonomy'). Since this is a Bill which is not certain to indicate Pakistan's legislative direction, further analysis is not justified here.

Conclusions: SAARC is slowly catching up

The most important developments in South Asia are still incomplete (India, Sri Lanka, Pakistan), and where legislation has been completed it is of minor importance (Nepal, Bhutan). There are no regional (SAARC) initiatives. Nevertheless, the situation is a considerable improvement on five years ago, and negotiations between the countries with Bills, and Brussels and/or Strasbourg could possibly see South Asia emerge with a number of laws closer to current international standards.

INFORMATION

Thanks to Angela Potter for information concerning Nepal, and to various anonymous commentators concerning Sri Lanka. Responsibility for all content remains with the author.

REFERENCES

1 G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 435-6.
2 Draft Personal Data Protection Blll (Sri Lanka) www.mdiit.gov.lk/images/news/Data_Protection_bill/Data_Protection_Bill_3-10-2019_-_Amended_Draft_FINAL_-_LD_Release.pdf
3 Summary of Data Protection Framework (July 2019) www.medianama.com/2019/07/223-summary-sri-lanka-personal-data-protection-bill/
4 For a summary of changes, see Aryan Babele 'Sri Lanka introduces final draft of Personal Data Protection Bill' *Medianama* 10 October 2019 www.medianama.com/2019/10/223-sri-lanka-final-draft-of-data-protection-legislation/
5 Information, Communications and Media Act of Bhutan, 2018 www.dit.gov.bt/information-communications-and-media-act-bhutan-2018
6 The Privacy Act 2018 (Nepal) www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/statutes-acts/the-privacy-act-2075-2018
7 Nepal has had a basic data privacy law for the public sector since the Right to Information Act 2007: Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 440-445.
8 e-Commerce Policy of Pakistan, October 2019 www.commerce.gov.pk/wp-content/uploads/2019/11/e-Commerce_Policy_of_Pakistan_Web.pdf
9 'Pakistan: MOC publishes e-commerce policy' *Data Guidance* 26 November 2019.
10 The Data Protection Bill 2018 (Pakistan) moitt.gov.pk/userfiles1/file/PERSONAL-DATA-PROTECTIONBILL October18Draft.pdf

events diary

Computers, Privacy & Data Protection (CPDP) 2020: Data Protection and Artificial Intelligence

22–24 January 2020
Brussels, Belgium

CPDP gathers academics, lawyers, practitioners, policy-makers, computer scientists and civil society from all over the world to exchange ideas and discuss the latest trends and emerging issues. CPDP2020 has the theme: "Data Protection and Artificial Intelligence" to pave the way for a timely and thorough discussion over a broad range of ethical, legal and policy issues related to new technologies and data analytics. CPDP2020 will offer more than 80 panels addressing current debates in the area of information technology, privacy and data protection. Already lined-up for the programme are panels on AI and healthcare, autonomous vehicles, digital evidence, AI for crime prevention, GDPR compliance for SMEs and much more.

Stewart Dresner, Publisher, *PL&B International*, will be the Moderator for a session taking place at 11.45h. on Thursday, 23 January organised by the African Network of Data Protection Authorities.

See www.cpdpconferences.org/

Where trade goes, so does data

Michael McEvoy, the Information and Privacy Commissioner for British Columbia, Canada, has a unique regulatory perspective relating to the other provinces and the federal Privacy Commissioner, but also facing Asia. **Stewart and Merrill Dresner** report from Victoria.

Canada gained EU adequacy status in 2001 which was confirmed in 2006. Canada's Federal government reports every two years to the European Commission on developments, most recently in June 2019. The European Commission will assess Canada again in 2020 and the European Data Protection Board will give its Opinion.

As the standard Canada needs to reach is "essential equivalence" rather than an identical law, Canada's current law is evolving rather than copying the GDPR, Michael McEvoy, the Information and Privacy Commissioner for British Columbia, Canada, told *PL&B* in an interview. Canada's private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies in all the provinces except those which have their own "substantially similar" laws, Alberta, British Columbia (BC) and Quebec. These provinces together make up around 50% of Canada's population. There are some differences between the provinces. For example, BC's law is more wide-ranging than those in the other provinces, as its Personal Information Protection Act (PIPA), applies to over 500,000 private sector organizations including businesses, charities, associations, trade unions, trusts and political parties.

Discussion about adequacy, with the European Commission, is a government responsibility. But the Privacy Commissioner of Canada (OPC) and the Provincial Privacy Commissioners are consulted, co-ordinate their policies, and give their views to the government, McEvoy said. There is no discussion in Canada about a mutual adequacy agreement with the EU following the EU-Japan model.

Reform on the way

The federal government has this year published a white paper with proposals to modernise PIPEDA[1]. It states that "changes are required to Canada's federal private-sector privacy regime to ensure that rules for the use of personal information in a commercial context are clear and enforceable and will support the level of privacy protection that Canadians expect." Canada's new government under Prime Minister Justin Trudeau has not yet announced its plans on reforms of Canada's privacy laws.

Mandatory breach notification was added to PIPEDA on 1 November 2018. This is also a requirement in Alberta's private sector and health information legislation.[2] BC's Office of the Information and Privacy Commissioner (OIPC) formally recommended adding mandatory breach notification to its private-sector statute in 2014[3] in harmony with the Alberta and federal model – but this has not yet occurred. Clearly, regulating data breaches is covered unevenly across Canada.

Privacy commissioners in Canada do not have the power to administer fines but have asked legislators for the ability to do so.[4] At present, fines can be administered by the courts in very limited situations.

Other aspects of the GDPR, such as data portability, do not exist as a privacy right in Canada. However, there may be steps in this direction in some sectors, such as banking driven by the Canadian Competition Bureau rather than privacy advocates. Anthony Durocher, Deputy Commissioner, Monopolistic Practices, Competition Bureau Canada, stated on 13 June 2019: "Consumer switching, or the threat of it, lies at the heart of the competitive process." [5]

GDPR has more importance than APEC

Government and companies realise the importance of data for international trade. Large Canada-based companies are certainly aware of the GDPR but the APEC Cross-Border Privacy Rules (CBPRs) have not gained traction. McEvoy is not aware that Canada has an Accountability Agent, nor that any Canada-based companies have signed up to the CBPRs, nor that any company has consulted his office on the perceived benefits of doing so. The demands on any prospective Accountability Agent are detailed in a 68-page document.[6]

McEvoy pointed out that whatever rules companies bind themselves with, they still have to deal with the existing laws and regulations. He stated: "The APEC framework may assist them with their compliance process. As a regulator, I may or may not look at the way a company is following these rules. The key question remains – have they abided by our laws?"

Data localisation on the way?

The federal government has a policy, not a law, with respect to processing and storage of the federal government's personal data in Canada, McEvoy said. *The Direction for Electronic Data Residence*, issued by the Treasury Board of Canada Secretariat[7] states "… when the data physically resides in Canada, it is subject to the protections afforded by Canadian privacy laws and Canada will be better situated to take prompt action, for example, in the event that access to data is compromised. Keeping data resident in Canada is also important for safeguarding sensitive information in the interest of national security." There are some exceptions for temporary measures when necessary.

There is a provision in Sec. 30.1 of BC's Freedom of Information and Protection of Privacy Act (FOIPPA) regarding data localisation which is covered at length in the 2004 report *Privacy and the US Patriot Act Implications for British Columbia Public Sector Outsourcing* (pp. 97-129). [8]

McEvoy explained that there are challenges with restricting the use of outsourcing outside Canada. He gave examples:

- the health care sector where diagnostic data for health conditions is processed abroad because that is where the data centre is located, and

- the education sector where advanced cloud-based services, on which teachers depend, are located in the US.

On the other hand, Microsoft, Amazon and Adobe have set up servers in Canada to operate within Canadian jurisdiction demonstrating their compliance with Canada's data localization policies. However, there is no appetite to require data localization for the private sector, McEvoy said.

Government proposals on revising PIPEDA

The proposals include "the protection of online reputation", which could be understood to be the equivalent to the right to be forgotten in the GDPR. McEvoy explained that the federal government wants a "Made in Canada" solution to build on existing provisions, for example, the right to correct and delete data with additional provisions for minors. Adding to the complexity of this issue are provisions enshrined in Section 2 of Canada's Charter of Rights and Freedoms to protect freedom of expression.[9] This issue involves a proportionate balancing of rights which is why such cases sometimes need to be resolved by the courts.

Codes of practice

When asked about the role of codes of practice on Canada's privacy scene, McEvoy said: "Codes are uncommon in terms of our privacy regime in Canada. Our provincial public sector privacy law makes a single reference to an information sharing code of practice (which has not been developed) and the word "code" does not appear in our provincial private-sector law. There are also few references to codes in PIPEDA. It is true that PIPEDA is based on the Canadian Standard Association's Model Code for Privacy Protection, but codes of practice are not something we see referred to in our work. It is the case that the federal government's white paper (cited above) raises the possibility of using codes and refers to this a number of times – see the section on *Incentivize the use of standards and codes*. The Privacy Commissioner of Canada is currently researching the efficacy of this approach in other jurisdictions."

Different sectors may introduce industry codes, McEvoy explained. "Together with BC's Chief Electoral Officer, we have recommended and are currently working with BC's political parties to develop a voluntary code of practice. The parties have cooperated in this initiative and we hope to finalise such a code in 2020."

The proposals would enhance the federal Privacy Commissioner's powers. Currently, McEvoy has order-making power in BC and strongly supports enhanced powers for his federal colleague. "Enhanced powers for the Privacy Commissioner of Canada are absolutely necessary, in particular, order-making and fining powers. The Federal Commissioner currently has to go to court to use these sanctions, for example, against Facebook in the current micro-targeting case."[10]

"He can utilise a Voluntary Compliance Agreement but this is not sufficient. The Federal Commissioner needs both deterrence and incentives. Fines get people's attention and are an incentive to do the right thing. It was quite a revelation to me when I was working at the UK's Information Commissioner's Office, and spent half a day listening in to the phone helpline. Everyone was talking about the GDPR level of fines. Those fines certainly made everyone aware they had significant legal responsibilities to abide by privacy law."

Cooperation with colleagues

"The federal and provincial Privacy Commissioners have complementary roles. We have an annual meeting in different provinces and territories in rotation and mostly coordinate by conference calls."[11]

BC works closest with the other Canadian jurisdictions that have private sector privacy laws. These are the Federal Privacy Commissioner and the Commissioners of neighbouring Alberta and distant Quebec. This frequently means joint approaches and investigations to matters that cross provincial boundaries such as privacy breaches. This ensures, in part, that companies do not play one regulator against another. Ontario's provincial privacy law does not cover the private sector except in the field of health care where it applies to both public and private sectors, Mc Evoy said.

McEvoy believes that given the relentless flow of personal information across borders, privacy regulators must cooperate internationally to properly protect their citizens. So inevitably, the BC regulator's attention is drawn to the Pacific rim where much of BC's trade happens. "Where trade goes, so does the data", McEvoy says, and to that end his office has taken a leading role in the Asia Pacific Privacy Authorities (APPA).

APPA has 19 member authorities from 13 countries and held their 52nd APPA Forum in the Philippines 2-4 December. McEvoy's office serves as the APPA Secretariat and McEvoy himself chairs APPA's Governance Committee.[12] He requested additional financial resources from the BC legislature to support this Asia-facing mission and they agreed. Clearly in this province of 5 million people, Asia is regarded as a strategic trading partner.

An example of cooperation via the APPA network was the data breach at Hong Kong-based VTech, which was investigated and worked on by several APPA members including the Privacy Commissioner of Canada, the BC Commissioner (where the company's Canadian HQ is located), the Federal Trade Commission in the US and Hong Kong's Privacy Commissioner for Personal Data. An investigation into a global data breach at VTech found the connected toymaker had failed to adopt adequate security measures to protect sensitive personal information of children.[13]

Role of GPEN

McEvoy says the 50-country GPEN (Global Privacy Enforcement Network) is an invaluable tool for encouraging cooperation among regulators. [14] His office plays an active role in GPEN, hosting and coordinating monthly teleconferences phone call for the Asia Pacific region. The members exchange experience on policy matters, investigations and good practice. The FTC in Washington DC hosts a similar GPEN phone call for the European and Americas regions. The calls are recorded so any GPEN member can catch up with developments in either region at a convenient time. The Federal Trade Commission (FTC) also

manages a secure alert service which is helpful when mounting investigations.

Future work

"With my 40 staff, responsible for 2,900 public bodies, and more than 500,000 private sector organizations, we must choose carefully our priority areas for investigations, both in response to complaints and those taken on our own initiative. We look for systemic investigations that will maximise our impact both to ensure legal compliance but also to educate on best privacy practices. I expect the health care field is an area which will get special attention in 2020 given the technologies employed in the sector and the very sensitive nature of personal information they handle. We have just finished an extensive audit of medical clinics in BC which will soon receive follow-up," McEvoy said.

"Even though breach reporting is not mandatory in BC we still receive an increasing number of breach notifications and complaints. That said, I believe this is the tip of the iceberg and that mandatory reporting of breaches must be made the law in BC."

According to the latest annual report (2017-2018):

- In 2017-18, the office received 186 privacy breach notifications and 273 privacy complaints.
- In 2018-19, the office received 194 breach notifications (a 4% increase from the previous year) and 332 privacy complaints (a 22% increase from the previous year).

"My office has launched a very significant campaign to educate the private sector about its privacy obligations. The PrivacyRight program went online in March of this year and has been very well received. Its objective is to help small businesses and organizations in BC understand their privacy obligations using webinars, videos, and podcasts."[15]

Some commentators have argued that privacy laws are a constraint on the development of Canada's digital economy. McEvoy does not share that view: "In fact, it is precisely the opposite because if innovative technology using people's information is not properly protected, citizens, customers and clients will rapidly lose trust and confidence in it. You need to build in privacy protection from the outset. The message I give businesses in BC, including small start-up tech companies is that they can come in and feel comfortable talking with my staff about privacy related issues. It's not a 'gotcha' exercise and my office is here to help facilitate some of the dynamic interesting technologies that are developing. Business has a right to use personal data when its collected and used fairly. It's fair to say that often small and medium enterprises (SMEs) generally have a lower awareness of privacy laws but they realise that people need to have confidence in their company if they are to be successful. Again, our office is here to help."

REFERENCES

1 www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html – government white paper
2 www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx
3 www.oipc.bc.ca/media/17271/fpt-resolution_-pei_-effective-privacy-and-access-to-information-legislation-in-a-data-driven-society.pdf
4 www.oipc.bc.ca/special-reports/1717
5 www.canada.ca/en/competition-bureau/news/2019/06/competition-in-the-age-of-the-digital-giant.html
6 cbprs.blob.core.windows.net/files/APEC%20Canada%20Enforcement%20Map.pdf
7 www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html
8 www.oipc.bc.ca/special-reports/1271
9 www.canada.ca/en/canadian-heritage/services/how-rights-protected/guide-canadian-charter-rights-freedoms.html
10 Links to OIPC investigation reports, including the joint investigation – www.oipc.bc.ca/reports/investigation-reports/
11 Resolutions from the October 2019 conference – www.oipc.bc.ca/media/17271/fpt-resolution_-pei_-effective-privacy-and-access-to-information-legislation-in-a-data-driven-society.pdf
12 www.appaforum.org/forums/communiques/52nd-appa-forum-communique/
13 www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180108/
14 www.privacyenforcement.net/authorities-listings
15 www.oipc.bc.ca/privacyright/

EU DPAs: EU-US Privacy Shield improved but not perfect

The European Data Protection Board (EDPB) says that while it welcomes the appointment of a "permanent" Ombudsperson in the US to deal with complaints, it is not certain that the Ombudsperson has sufficient powers to access information and to remedy non-compliance. Also, there remains a certain lack of oversight in substance.

"The Department of Commerce (DoC) as well as the Federal Trade Commission (FTC) also undertook new *ex officio* oversight and enforcement actions as regards the compliance of Privacy Shield certified organisations with its safeguarding requirements. The EDPB particularly welcomes that the DoC has increased the number of 'random spot checks' to 30 organisations per month."

However, compliance with the substance of the Privacy Shield's principles remains unchecked for the majority of companies, the DPAs say. For example, more substantive checks are needed on onward transfers. The DoC could make use of its right to ask organisations to produce the contracts they have put in place with partners in third countries in order to assess whether they provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed, they say.

• *Eight representatives of the EDPB participated in the third joint review conducted by the European Commission in the autumn of 2019. See edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf*

Wojciech Wiewiórowski appointed new EDPS

Wojciech Wiewiórowski's appointment as the new European Data Protection Supervisor (EDPS) was confirmed on 5 December by a joint decision of the European Parliament and the Council, following a rigorous selection process launched earlier this year.

Wiewiórowski's appointment does not come as a surprise. He has been Assistant Supervisor at the EDPS since 2014, and prior to that Inspector General for the Protection of Personal Data at the Polish Data Protection Authority. He was also Vice Chair of the Article 29 Data Protection Working Party.

Questioned by the European Parliament's Civil Liberties, Justice and Home affairs, Wiewiórowski said that in early 2015, in the first 100 days of their mandate, he and the late EDPS Giovanni Buttarelli developed a three-pronged strategy of taking data protection into the digital age, forging global partnerships and opening a new chapter for EU data protection. "This has been ideal preparation for me to now take our authority to a new level of leadership, building smart and innovative public administration. I intend to lead by example and harness the synergies available to EDPS with its unique place at the heart of the EU institutional architecture as well as the data protection community. European law – not only classic data protection acts but all *acquis communautaire* – should be a benchmark for all new regulations around the world. At the moment the EU holds considerable influence in the regulation of the digital economy, but we cannot take this position for granted. If we allow our standards to slip, then countries in the world will increasingly look to other models, such as China's or the models that are likely to emerge in India and the United States over the next five years," he said.

"I will do everything within my competence to help the EDPB succeed in delivering consistent and robust enforcement of the GDPR throughout the EU."

Wiewiórowski started his five-year mandate on 6 December.

• *See www.europarl.europa.eu/cms-data/189189/1192318EN-original.pdf and edps.europa.eu/about-edps/members-mission/supervisors/wojciech-wiewi%C3%B3rowski_en*

EU Guidelines on Data Protection by Design and by Default open for consultation

The European Data Protection Board (EDPB) Guidelines on Data Protection by Design and by Default encourage organisations to implement these measures to gain a competitive advantage in the market.

The Guidelines cover elements that controllers must take into account when designing the processing. The GDPR Art 32 requires: 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate.'

The criteria of "state of the art" requires controllers to stay up to date with technological progress in order to secure continued effective implementation of the data protection principles, the DPAs say. In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. This means that controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape, the guidance says.

"The 'state of the art' is a dynamic concept that cannot be statically defined at a fixed point in time, but must be assessed continuously in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could result in a lack of compliance with Article 25."

• *The guidelines, which are open to consultation until 16 January 2020 are at edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en*

Senate to debate a US federal privacy law

Senator Maria Cantwell has proposed a new federal privacy bill, Consumer Online Privacy Act or COPRA.

COPRA would "provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."

The bill would establish explicit consent, access and deletion rights, and make the FTC the enforcement body.

• *See www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf*

New proposal expected on e-Privacy Regulation

The e-Privacy compromise proposal by the Finnish Presidency of the EU Council has stalled as too many Member State representatives have rejected the proposal. The Presidency was hoping that the TTE (Transport, Telecoms and Energy) Council would adopt a general approach at its meeting on 3 December.

The European Commission may now present a revised e-Privacy proposal during the Croatian Presidency of the EU Council (from January 2020), *Covington & Burling* report. Internal Market Commissioner Thierry Breton said however, that all options remain on the table, including continuing work with the current text.

The progress note on e-Privacy from the Permanent Representatives Committee (COREPER) says there have been differing views on the issue of processing of electronic communications data for the purposes of prevention of child abuse imagery.

It says that the Presidency made "considerable effort on clarifying the scope of the Regulation." The Presidency has also included recital text clarifying the concept of third parties.

"In this connection, when it comes to processing of electronic communications data by the providers of electronic communications networks and services, the Presidency proposed a change that would allow such processing when necessary to provide an electronic communications service."

Delegations have also raised concerns about the way the e-Privacy proposal would interact with Machine-to-Machine and Internet of Things services.

• *See www.insideprivacy.com/data-privacy/new-e-privacy-proposal-on-the-horizon/*

e-Privacy regulation in conflict with GDPR

The law firm Hogan Lovells says that the proposed EU e-Privacy Regulation, rather than complementing the GDPR as originally intended, is in some fundamental respects in conflict with it.

The proposed e-Privacy Regulation seeks to limit the processing of a broad spectrum of information, including both personal and non-personal data, irrespective of the actual impact of such processing on people's privacy, the firm says. In summary, the essence of flexibility in the application of the GDPR created by focusing on risk is fundamentally missing from the proposed e-Privacy Regulation.

The firm's policy recommendations to improve the current text include the following:

- The e-Privacy Regulation should move away from setting out narrow legal bases for the processing of specific types of data.
- The risk-based approach of the GDPR should be applied to e-Privacy.
- Data processing that poses no risks to individuals, particularly where data that is or is made anonymous, should be explicitly excluded.

Eduardo Ustaran, Global Co-Head of the Privacy and Cybersecurity practice at Hogan Lovells, said: "There is clearly a need for the protection of privacy in the digital economy, but to be effective, any e-Privacy legal framework must be compatible with technological development and human progress. The European Union has the opportunity to get this balance right by applying a more flexible risk-based approach."

• *See www.hoganlovells.com/en/news/hogan-lovells-calls-for-an-alternative-approach-to-regulating-privacy-in-the-digital-economy*

Recommendation on health-related data at UN

In October, the United Nations Special Rapporteur on the Right to Privacy (UNSRP), Professor Joseph Cannataci, presented to the United Nations General Assembly his 'Recommendation on the Management of Health Related Data'. The Recommendation provides principles for the processing of health-related data and to serve as an international baseline for minimum data protection standards. It was developed through extensive international consultation.

The premise of the recommendation is that quality healthcare protects the right to privacy. Everyone has the right to the highest attainable standard of physical and mental health, and, to the highest attainable protection for their health-related data regardless of indigeneity, disability, gender, age, or social background, for example.

The recommendation is concerned about the very sensitive nature of health-related data, its high commercial value, and the largely hidden industry of collecting, using and securing health data.

Capturing the benefits of innovative digital health technologies depends on patients' and citizens' trust in the use of these technologies. This trust is generated by the management of their health data within a human rights framework and according to established data protection and privacy standards. The right to health has been recognized in the Universal Declaration of Human Rights (Art. 25) and in core international human rights instruments such as the Convention of the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women, the Convention of the Rights of Persons with Disabilities, amongst others.

Operational and frequently overlooked matters such as data use in Electronic Health Records, healthcare record keeping, IT systems, and research amongst other matters undermine the confidence of the patient and their families in healthcare systems. The recommendation is applicable to the data processing of health-related data in both public and private sectors.

Reported for PL&B by Dr Elizabeth Coombs, University of Malta

• *See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/FINALHRDDOCUMENT.pdf and www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf*

Privacy 2030: Giovanni Buttarelli's 'New Vision for Europe'

A manifesto from former European Data Protection Supervisor, Giovanni Buttarelli, advocates that the large amounts of personal data now being collected globally should be used for the common good. By **Stewart Dresner**.

The late Giovanni Buttarelli, European Data Protection Supervisor, drafted a Privacy Manifesto with Christian D'Cunha, the Head of his Private Office who, following Buttarelli's death in August, prepared it for publication.[1] The following extracts, selected from the document, give a flavour of his wide-ranging ambitions to strengthen privacy rights.

"Democracy and the rule of law are threatened. Data protection authorities, along with other enforcers, face enormous challenges in uncovering opaque business practices to uphold the rights of individuals."

"Vast amounts of data have been collected — however lawfully or ethically … The question for society is whether this data can be now used for the benefit of individuals and wider society. A 'Europe fit for the Digital Age' must be oriented toward the common good and sustainable solutions."

"Clerical workers have to work on smart desks monitoring their movements that one described as 'an umbilical cord to the computer.' AI systems are deployed to replace human caseworkers in mediating between the state and people dependent on welfare support."

"The rule of law implies legitimacy, fairness and impartiality of a legal process, regardless of outcome. Corporate secrecy and intellectual property rights seem to enjoy stronger protections in practice than individual privacy and personal data. Individual plaintiffs need to spend tens of thousands of euros in legal fees just to get to court and contest violations of the EU General Data Protection Regulation. We shouldn't have to beg, plead and become technical wizards to exercise our fundamental rights."

"Privacy policies protect the controller rather than the user of the service; they are rarely consulted and almost never open to negotiation."

"Although companies offer a veneer of transparency, actually accessing data about yourself seems to become more difficult the larger the company…. Increasingly, private platforms intermediate the relationship between citizen and state. Data defines individuals and determines how they can be treated. The terms of service therefore become, in effect, the law."

"The religion of data maximisation, notwithstanding its questionable compatibility with EU law, now appears unsustainable also from an environmental perspective. Tens of thousands of entities use hundreds of techniques to track people across the web. Tracking and sensors are so pervasive that each of us leaves digital traces …. wherever we have been. The enthusiasm for video, AI, facial recognition, wearables and smart devices indicates an inexorable drift to ever more personal data collection and storage — estimated to double energy consumption every four years."

Although companies offer a veneer of transparency, actually accessing data about yourself seems to become more difficult the larger the company.

"The right to human dignity demands limits to the degree to which an individual can be scanned, monitored and monetised — irrespective of any claims to putative 'consent.'"

"We do not, in the name of 'innovation,' allow products onto the market where there is risk of harm; no one criticises such precautions as 'strangling' innovation."

"The EU is ideally placed to lead this conversation, even at the price of calling a moratorium on certain invasive and dangerous technologies – like facial recognition."

"The GDPR does not systematically address the massive imbalances in power between, on the one hand, major tech companies and governments and, on the other, small competitors, individuals and workers – not to mention vulnerable groups, like children, the socially disadvantaged and migrants. …Many novelties of the GDPR, such as data portability, certifications and privacy by design, have not been implemented or tested."

"Data protection authorities should not simply demand additional resources — they need to have courage to exercise their full powers."

"There are regular calls for more convergence in the regulation of digital services. The *Bundeskartellamt* decision on Facebook [p.1] is an early demonstration of the possibility that certain behaviour violates more than one set of legal obligations. Article 5 of the GDPR requires data processing to be lawful — that means not only compliant with the GDPR itself, but also with other applicable laws, including those governing e-commerce, e-government, competition, consumer and environmental protection. There is no good reason why competition and data protection authorities should not pursue cases jointly where there is a common interest. If there are legal barriers to such cooperation, national and EU legislators should remove them."

REFERENCE

1 *Privacy 2030: A New Vision for Europe* t.co/P4NByPrbF1?amp=1

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> "*Privacy Laws & Business* is my go-to for the latest international thought leadership on hot topics in data protection law and policy."
>
> **Giles Pratt, Partner, Freshfields Bruckhaus Deringer LLP**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report*, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.