



ESTABLISHED  
**1987**

**INTERNATIONAL REPORT**

# PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

## Belgium: GDPR implementing Act enters into force

Laura Brodahl, Laura De Boel and Cédric Burton of Wilson Sonsini Goodrich & Rosati analyse the specifics of the law.

Following the adoption of the General Data Protection Regulation (GDPR) the Belgian legislator has adopted a new data protection law.

The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (the 2018 Data Protection Act)

repeals the Privacy Act of 8 December 1992 (the 1992 Privacy Act) and its implementing legislation. It entered into force on 5 September 2018.

The 2018 Data Protection Act is a massive piece of legislation. It

*Continued on p.3*

## IAB revises its transparency and consent framework

As a result of feedback from DPAs and other stakeholders, a new version of this industry standard will be issued soon.

Laura Linkomies talked to IAB Europe in Brussels.

IAB (Interactive Advertising Bureau) Europe, the industry association for the digital advertising ecosystem in Europe, is working hard to make improvements to the “Transparency and Consent

Framework” which was launched in April 2018 just in time for the GDPR. The voluntary framework is based on publishers and tech vendors using an open source standard to

*Continued on p.4*

Issue 157 February 2019

### NEWS

- 2 - Comment  
GDPR: The global benchmark
- 9 - FEDMA voices its concerns about e-Privacy draft regulation
- 11 - CNIL fines Google €50 million

### ANALYSIS

- 6 - GDPR extraterritorial reach: Conflict with international law?

### LEGISLATION

- 12 - Japan to issue further data protection legislation
- 14 - Global data privacy laws 2019: 132 national laws and many bills
- 19 - Global data privacy laws: New eras for international standards
- 21 - New Zealand’s Privacy Bill
- 24 - Data protection bills in Kenya, Uganda, Tanzania and Zambia

### NEWS IN BRIEF

- 8 - 59,000 data breaches reported across Europe
- 18 - Mutual EU-Japan adequacy
- 18 - EU-US Privacy Shield continues
- 23 - Facebook accused of “exploitative abuse”
- 26 - EDPB adopts more DPIA lists
- 26 - Singapore’s DPA issues large fines
- 26 - Ireland advises on Brexit ‘no deal’ implications
- 27 - EU Advocate General: Right to be Forgotten is limited to EU
- 27 - Doctor has ‘Right to be Forgotten’
- 27 - EDPB advises on Brexit impact on data transfers and BCRs

## www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Materials from PL&B events
- Special Reports
- Videos and audio recordings

See the back page or [www.privacylaws.com/subscription\\_info](http://www.privacylaws.com/subscription_info)

To check your type of subscription, contact [kan@privacylaws.com](mailto:kan@privacylaws.com) or telephone +44 (0)20 8868 9200.

**Separate Supplement**  
Tables of 132 laws and 28 bills

**PL&B Services:** Publications • Conferences • Consulting • Recruitment  
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL  
**report**

ISSUE NO 157

FEBRUARY 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****Laura Brodahl, Laura De Boel and Cédric Burton**

Wilson Sonsini Goodrich &amp; Rosati, Belgium

**Kurt Wimmer**

Covington &amp; Burling LLP, US

**Mark Sherwood-Edwards**

This is DPO, UK

**Hiroshi Miyashita**

Chuo University, Japan

**Katrine Evans**

Hayman Lawyers, New Zealand

**Emma Anderson**

PL&amp;B Correspondent

**Published by**Privacy Laws & Business, 2nd Floor,  
Monument House, 215 Marsh Road, Pinner,  
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Fax: +44 (0)20 8868 5215****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

**Copyright:** No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2019 Privacy Laws &amp; Business

**comment****GDPR: The global benchmark**

According to the EU Commission, during the peak month of May 2018, GDPR was searched more often on Google than American superstars Beyoncé and Kim Kardashian. On a more serious note, GDPR is undoubtedly having a global effect, as shown in Professor Graham Greenleaf's articles and global tables of privacy laws issued here as a supplement.

Numerous countries have updated their data protection laws since 2017, invariably strengthening them in ways which reflect some aspects of the GDPR, and there are currently 28 bills for new privacy laws (p.14 and p.19). However, our US correspondents observe that "no law passed by one country, or even a political and economic union as powerful as the EU, can be global, regardless of ambition or breadth of terms" (p.6).

The key word for 2019 is adequacy – the countries which have it, such as Argentina, are being reviewed. Japan's newly acquired adequacy status is being supplemented in the form of some amendments to existing legislation (p.12) and the EU-US Privacy Shield has been given another lease of life (p.18). As key voices from US industry now support a federal privacy law, the US Senate is to hold a hearing on a federal privacy law on 27 February.

Within the EU, the GDPR's effect is felt in a most concrete way. According to the EU there have been 41,500 breach notifications, 255 cross border cases, and 95,000 complaints\*. The complaints mostly address telemarketing and promotional emails. For this issue, I interviewed FEDMA, the European umbrella organisation for direct marketers, about its concerns over the proposed EU e-Privacy Regulation (p.9) and IAB, the Interactive Advertising Bureau, about its Transparency & Consent Framework for GDPR compliance (p.1).

This issue introduces the new Belgian DP law (p.1). We aim to publish a report on each EU country's new GDPR adaptation law – if you would like to analyse your country's law please get in touch. An overview of GDPR implementation and the remaining issues will be provided at our 32nd Annual International Conference in Cambridge, 1-3 July 2019. See the 45 confirmed speakers and their sessions from 16 jurisdictions at [www.privacylaws.com/ac](http://www.privacylaws.com/ac)

**Laura Linkomies, Editor**

PRIVACY LAWS &amp; BUSINESS

\*EU statistics issued 28 January [ec.europa.eu/commission/sites/beta-political/files/190125\\_gdpr\\_infographics\\_v4.pdf](http://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf)**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](mailto:laura.linkomies@privacylaws.com).

*Belgium... from p.1*

implements and specifies the GDPR, but also implements the Law Enforcement Directive (EU Directive 2016/680) and includes privacy requirements in other areas (e.g. data processing by intelligence agencies and passengers' data). This article focuses on how the Act implements and supplements the GDPR. We set out below the key derogations and specifications.

#### TERRITORIAL SCOPE

The territorial scope of application of the Act is in line with Article 3 of the GDPR (i.e. the Act applies to the processing of personal data in the context of the activities of an organization's Belgian establishment as well as to processing by an organization that either offers goods or services to individuals in Belgium, or monitors their behaviour). The Act specifies that it does not apply to a Belgian processor acting on behalf of a controller established in another EU member state, when the processing takes place in that other member state. The data protection laws of that other member state would then apply.

#### AGE OF CONSENT FOR MINORS

Under the GDPR, online services that rely on consent must obtain parental consent when the service is offered directly to a child under the age of 16. The GDPR allows EU member states to lower the age threshold. Most EU member states have done so, including Belgium, that has lowered the age threshold to 13 years. The Belgian Data Protection Authority (DPA) has expressed its support for the Belgian legislator's choice. The DPA emphasizes that children remain vulnerable data subjects and special attention should be paid to the processing of their personal data. This position is in line with the Belgian DPA's past campaigns to raise awareness about children's online privacy, in particular in the context of smart devices and apps.

#### SENSITIVE DATA AND "SUBSTANTIAL PUBLIC INTEREST"

In principle, the processing of special categories of personal data (commonly referred to as "sensitive data") is

prohibited under the GDPR, unless an exemption as laid down in article 9 (2) GDPR applies. The 2018 Data Protection Act specifies one of those exemptions, namely, processing permitted when necessary for reasons of substantial public interest. It provides a list of such processing operations (e.g. processing by organizations fighting child abuse).

#### SAFEGUARDS FOR GENETIC, BIOMETRIC OR HEALTH DATA

The 2018 Data Protection Act imposes additional safeguards for the processing of genetic or biometric data or data concerning health. The controller and – where applicable – its processor must designate the categories of individuals who will have access to such sensitive data. This list should include a detailed description of their role in relation to the data processing. It should also be kept readily available for consultation by the DPA. The designated individuals must be bound by a statutory or contractual confidentiality obligation. An implementing act to the 1992 Privacy Act provided similar obligations, so the impact will be limited for companies that already complied with the previous Belgian data protection legal framework.

#### CRIMINAL CONVICTIONS AND OFFENCES

The GDPR provides that the processing of criminal convictions and offences or related security measures ("criminal data") can only be done under the control of an official authority or where it is authorized by Member State law, to the extent that the Member State law provides for appropriate safeguards. The 2018 Data Protection Act authorizes the processing of criminal data (i) to the extent necessary for the management of a natural or legal persons' own disputes; (ii) by legal counsel; (iii) insofar as necessary for important reasons of public interest laid down by law; (iv) insofar as necessary for scientific, historical or statistical research or archiving; (v) where the data subject has given explicit written permission for the processing for one or more well-defined purposes and the processing remains limited to those

purposes; or (vi) where the processing relates to data that were clearly made public by the data subject for one or more well-defined purposes and the processing remains limited to those purposes. A controller and – where applicable – its processor must implement the same safeguards as described under Section 4 of this article to the processing of criminal data.

The Act provides more exceptions for the processing of criminal data than the 1992 Privacy Act, while also narrowing the concept of "criminal data" to criminal convictions and offences or related security measures (e.g. the 1992 Privacy Act included suspicions in this concept). Businesses thus have more leeway to process criminal data compared to the 1992 Privacy Act.

#### ARCHIVING, RESEARCH AND STATISTICAL PURPOSES

The 2018 Data Protection Act provides derogations to the data subjects' rights in relation to processing for archiving, research and statistical purposes (e.g. the right of access to and rectification of data and the right to restrict and object to processing). In addition, the Act largely reiterates the requirements that applied to such processing under the 1992 Privacy Act. In particular, it provides the following steps for de-identification:

- First, the Act requires a controller to use anonymized data for research and statistical purposes.
- Only if the controller cannot achieve these purposes through anonymized data, it may use pseudonymised data.
- As a last resort, if the purposes cannot be achieved through pseudonymized data, a controller may use non-pseudonymized data.

Furthermore, the controller must include additional information in its internal records (i.e. a justification for using the data – whether in pseudonymous form or not, the reasons why data subjects' rights should be limited and a copy of the Data Protection Impact Assessment in case of sensitive data processing). A controller must also provide additional information to data subjects (i.e. the fact that the data is anonymized or not, and the reasons why data subjects' rights should be limited).

In case of further processing by another controller, the initial controller and subsequent controller must conclude a data processing agreement. This agreement must at least contain the contact details of the initial and subsequent controllers, and the reasons why allowing data subjects to exercise their rights would make it impossible to achieve the objectives or would seriously impede them. The agreement must be added to the internal records. The sharing and dissemination of data processed for archiving, research and statistical purposes is also subject to some other conditions (e.g. non-pseudonymised data can only be shared or disseminated in a limited number of cases).

**COLLECTIVE ACTION**

The GDPR allows Member States to authorize a not-for-profit body to act without a mandate from the data subjects. Although the Belgian DPA supported including such representation

without mandate, this is not provided in the Act.

**CRIMINAL SANCTIONS**

In addition to the GDPR’s administrative sanctions, the Act provides for criminal sanctions that can be imposed by a Belgian court. However, the criminal fines are lower than the administrative fines (i.e. maximum €240,000 for criminal fines vs. maximum €20 million for administrative fines).

**CONCLUSION**

From a business perspective, the 2018 Data Protection Act does not significantly deviate from the GDPR. In practice, the main deviations deal with topics that were already specified under Belgian law (i.e. processing of genetic, biometric or health data, processing of criminal convictions and offences, processing of personal data for archiving, research and statistical purposes).

However, the Act allows for implementing legislation to further define safeguards and obligations. In the past, such powers were broadly used by the Belgian Government (e.g. many articles of the 1992 Privacy Act were supplemented by the Royal Decree of 13 February 2001), and it seems likely that these powers will also be used under the Belgian Data Protection Act. Businesses should continue to monitor these local developments.

**AUTHORS**

Laura Brodahl is a Privacy & Data Protection Lawyer, Laura De Boel is Of Counsel and Cédric Burton is Partner, Co-Chair Privacy and Cybersecurity Practice at Wilson Sonsini Goodrich & Rosati Brussels office.  
Emails: lbrodahl@wsgr.com  
ldeboel@wsgr.com  
cburton@wsgr.com

*IAB Europe... from p.1*

provide transparency, and share information about consumer consents across the advertising ecosystem.

Matthias Matthiesen, Director, Privacy and Public Policy at IAB Europe, told *PL&B* that they now have 176 registered Consent Management Providers (CMPs) and 472 registered vendors. This exceeds their expectations of 100-150 registrations in the first year.

**PL&B: The framework is based on publishers gaining consent on behalf of third-party vendors. What are the other benefits for GDPR compliance?**

Matthiesen: “The benefits for publishers are that they have a list of companies which they can use to make their own disclosures to users. In the past this has been more complicated – through static privacy policies for example – but if the information of the processing of their business partners changed, the details would not automatically have been updated in the privacy policy, and the disclosure to the users would no longer be accurate. With the Transparency and Consent Framework, transparency is about

publishers, advertiser or app providers being able to pull information and update it automatically, daily if they wish. In reality, this does not happen daily, but every time there are updates. Publishers can see what the differences are, and if significant enough, decide that they may need to go back to the consumers to refresh their consent. This is a communication channel that did not exist before.”

“We assume that companies only process personal data when they have a legal basis. Therefore, no third-party intermediary can process and collect personal data unless at some point, transparency has been provided or consent has been achieved. This puts publishers and advertisers in the driving seat. This is a much more sophisticated way of dealing with transparency and consent than previous mechanisms and is something that publishers have always wanted.”

“If you are a vendor, you now have an obligation to demonstrate data protection compliance. The framework allows vendors to have more confidence that transparency and/or consent have been established, for which purposes data can be collected and processed, and which com-

panies they can confidently share data with. The framework also provides an audit trail.”

**Has the framework been well received by publishers? Are they concerned about the legal risk to them – is there legal liability in the event of non-compliance by vendors?**

“We are asked this all the time. The Framework doesn’t change liabilities between participants in the advertising sector. If not using the framework, companies are still going to have to worry about liability. Publishers that are concerned about liability will find the framework helpful as they will be able to demonstrate all the steps they have taken to achieve compliance. Ultimately, controllers are responsible for compliance under the law. Most vendors are controllers in their own right and are therefore responsible for their data protection compliance. Many concerns stem from the desire of publishers wanting to be in control, but being ‘in control’ and being a ‘controller’ are not necessarily the same things.”

“Publishers have engaged with GDPR and consent obligations well from the start but had not thought as

much about who their partners are, and which companies form part of their supply chains. For publishers, the user experience has always been at the forefront but many publishers did not appreciate that once consent has been obtained, many other things need to happen. Now the framework provides that added functionality. Some publishers have taken a wait and see approach. But ultimately, this or another framework has to be used to allow all actors to demonstrate compliance with the law. Google is now publicly committed to joining once we have published version 2 of the framework, so the framework is well on the way to becoming the industry standard.”

“Version 2 will introduce a number of improvements, such as redefining purposes and adding new ones. We are unbundling some of the existing purposes into multiple purposes. In addition, we are adding some explicit signals for transparency. The signals we send are “yes” and “no” on a Purpose and Vendor basis. Think of it as a traffic light, it signals when it is OK to cross the street and when not. Red/Green. The Framework does the same. It tells you when it is OK to process data and when not.”

“Now there are signals for consent, which means there are implicit signals also for transparency but in situations where organisations rely on legitimate interest, we still need to convey information about transparency having been provided. Also, we are adding signals for user objections and we are adding certain publisher controls too so that they can, in essence, discriminate against vendors – to allow some to process for more or different purposes than others.”

#### FRAMEWORK DEFINITIONS

**CMP** – a company operating as a consent management platform that can read and/or set the user’s consent status for the vendors chosen by a website operator (either Publisher specific through a first-party cookie, or global through a third-party cookie).

**Purposes** – the purposes for which a Controller enabled by a website operator is using personal data collected from (or received by a third party) about an end user.

**Vendor** – a third party that a website operator is using in connection with surfacing content to its end users that either (1) accesses an end user’s device or browser (for setting cookies), or (2) collects personal data from the actions of the website operator’s end users.

**Signal** – The signals the framework sends tell when it is ok to process data and when not.

#### Consent Management Providers (CMPs) have to register with IAB. Do you monitor their compliance after that?

“While we currently do not have a comprehensive compliance programme, we are educating and engaging with CMPs. Ultimately, we want to systematically confirm compliance by CMPs with framework policies. When participating in the framework, companies enter into a contract with us. Under that contract, we can suspend framework participants who are not complying with its policies. However, in the first instance, we assume that everyone who joins the framework wants to do the right thing so that our priority is achieving compliance with our policies and by extension – hopefully – compliance with the law.”

#### Are vendors vetted in some way?

“At the moment we do not do any active vetting, but vendors have to warrant to us that they have a data protection compliance programme that covers the GDPR and e-Privacy Directive, and that they are a member of a trade body or organisation to verify there is no deception. In the future, we may start audits but at the moment there are no resources for that. We will first start checking CMPs as we have seen many issues with them. The ultimate goal is that every single vendor on the list will be regularly certified against the policies.”

#### What is the feedback from national DPAs on the framework?

“We have met with several DPAs. They are offering constructive criticism but also think this goes in the right direction overall.”

#### The CNIL decision on Vectaury says it failed to meet conditions for valid consent under data protection law. What is IAB’s view/reaction to CNIL’s order?

“The situation would have been rectified had we been able to enforce our policies more actively. What the Vectaury case showed is that our policies are correct. Had Vectaury followed our policies, the CNIL would probably have been satisfied, or had very little to complain about. We are forced to be reactive because of resource constraints, but wish to enforce the policies more actively in the future. We only found out about their issues due to the very public enforcement by the CNIL. As a result, Vectaury CMP has been suspended from our framework. Once they can demonstrate they comply with our

#### HOW DOES THE TRANSPARENCY AND CONSENT FRAMEWORK FUNCTION – IN A NUTSHELL

IAB Europe’s Transparency & Consent Framework is an open-source, not-for-profit industry standard that helps all parties in the digital advertising chain ensure that they comply with the GDPR when processing personal data or accessing and/or storing information on a user’s device, such as cookies, advertising identifiers, device identifiers and other tracking technologies.

The IAB Europe Transparency & Consent Framework is designed to enable

publishers to (i) disclose the vendors who will be processing personal data when a user accesses the site; (ii) disclose the data processing purposes and associated legal bases for which and under which the vendors are processing personal data; (iii) request consent on behalf of those vendors who are relying on consent as their legal ground for processing for one or more data processing purposes; (iv) store the user’s consent choices; and (v) transmit the user’s consent choices to upstream vendors.

IAB Europe’s Transparency & Consent Framework leaves some freedom for publishers and their Consent Management Platforms (CMPs) to interpret how best to adapt their interface to their relevant market(s).

Publishers select which ad tech vendors they wish to work with. Vendors pay a nominal fee to participate. Publishers then get consent from the consumer on those vendors’ behalf.

policies, they will be reinstated.”

“The decision covers several moments in time. The company was under investigation already before the IAB Europe framework was announced. If anything, the CNIL recognised that their compliance improved once they started to implement the framework. The CNIL criticised one of our purposes and I think that was a fair criticism – it is too complicated for users to understand.”

**Did IAB Europe suffer negative publicity as a result of the CNIL decision?**

“It is the exact opposite. There has been some bad misinformation on Twitter initially by a commentator who did not understand the framework or the decision. But on the whole, *Vectuary* is proof of why the framework is needed. We are not

perfect yet, but what else is there? With regard to the recent €50 million fine on Google by CNIL, Google is not implementing the IAB Europe framework at the moment so there is no immediate connection, though of course any enforcement action is instructive as to what DPAs consider requirements to be.”

**When will version 2 of the framework be launched?**

“We need to reach consensus with many stakeholders which takes time. We have been working on it since last May and are now in the final stages. Once we have agreed on everything, we will need to finalise the technical details.

There will be a public consultation – maybe in a few months’ time, and then a transitional period.”

**How will the e-Privacy Regs affect the IAB Transparency & Consent Framework?**

“The e-Privacy Regulation will not dramatically change what Member States are doing now, apart from Germany that has not implemented the cookie provision in the e-Privacy Directive. The regulation introduces some new features such as browser settings. The big question for us is what ‘freely given consent’ means and whether ad-funded services will continue to be allowed to restrict access to their offerings if users do not agree to their data being processed for advertising purposes.”

<b>INFORMATION</b>
See <a href="http://www.iabeurope.eu/category/policy/tcf-updates/">www.iabeurope.eu/category/policy/tcf-updates/</a>

# GDPR extraterritorial reach: Conflict with international law?

Do the principles of territoriality and nationality override the GDPR’s territorial reach?

**Kurt Wimmer** of Covington & Burling LLP analyses the issues at stake.

It has become commonplace for commentators and others to refer to the General Data Protection Regulation (GDPR) as a “global” law, or a “global” standard.<sup>1</sup> To be sure, the GDPR is having a significant impact on the privacy landscape around the world. And users around the world have had to deal with a hailstorm of new requests for consent and cookie banners based on widespread assumption of GDPR requirements even far outside the EU.

But no law passed by one country, or even a political and economic union as powerful as the EU, can be “global,” regardless of ambition or breadth of terms. Even international treaties require countries to assent to their applicability.

The question of whether and to what extent a law can have extraterritorial effect is one that did not start with the GDPR and will not end with it. Over decades of global interpretation and scholarship, settled principles of

public international law have been established to govern when it is appropriate for a law passed by one country to apply in the territory of another country that may have very different laws. These principles should be taken into account in determining whether it is, in fact, legal for European data protection authorities (DPAs) to enforce principles of the GDPR against companies with no presence in the EU.

This article analyzes those principles and concludes that companies with no EU presence may have colorable arguments against the jurisdiction of EU regulatory authorities and courts to enter orders against them.

**THE JURISDICTIONAL ASPIRATIONS OF THE GDPR**

The GDPR was developed with the goal of providing consistent privacy protections for individuals across the EU.<sup>2</sup> Prior to the adoption of the GDPR, each EU member country implemented its own data privacy laws

under the guidance of the 1995 EU Data Protection Directive (the Directive). The Directive provided that where parties not established in the EU use “equipment” in the EU to collect personal information, they are subject to the law.

The GDPR employs an entirely different approach to jurisdiction. Article 3(2) of the GDPR applies specifically to entities not established in the EU and provides as follows:

“This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.”

The GDPR thus contains two criteria

to establish its applicability to parties outside the EU. It applies to (1) parties offering services in the EU or (2) that monitor the behavior of EU users.

**Offering goods or services:** It is important to note that the recitals of the GDPR and long-standing European common law are extremely important in interpreting the terms of the GDPR. In terms of “goods or services” jurisdiction, recital 23 of the GDPR contains a useful clarification:

“In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.”<sup>3</sup>

Accordingly, the mere accessibility from the EU of a non-EU company’s website or the use of English on a US website are not sufficient to trigger the applicability of the GDPR. The targeting of EU users must be more obvious and “envisioned,” for example, by allowing them to order goods and having them shipped to the EU, by using the euro as a currency option, or by offering content in languages adapted to EU users.

This first criterion of targeting a service is clearly inspired by existing European case law. The key authority in this area is the *Pammer* case.<sup>4</sup> In this case, the Court of Justice of the EU (CJEU) was asked to clarify when an Internet service can be considered to target data subjects in a Member State. The CJEU held that mere accessibility of a website does not suffice. Similarly, the indication of the trader’s address,

email address or phone number (without international code) cannot be construed as targeting. To the contrary, the CJEU highlighted the following examples of activities that can demonstrate an intention to target:

- the express mentioning that the service is provided to users in a Member State;
- paying search engines to have its website favorably indexed in order to facilitate access by consumers in particular Member States;
- the international nature of the services;
- the provision of international telephone numbers;
- the use of Internet domain levels other than those of where the service provider is established (or general ones, such as .eu, or .com); and
- the mentioning of international clientele, and accounts written by such customers.

In the *Pammer* case, the service at issue, a travel package, was advertised on a third-party website. The CJEU did not consider whether the third-party website was a service targeting another Member State. The court only considered if the advertised service was targeting the Member State.

**Monitoring behavior:** The second trigger for the applicability of the GDPR is whether the party outside the EU “monitors the behavior” of users in the EU. On this prong, recital 24 of the GDPR provides an important interpretative principle:

“In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviors and attitudes.”

The recital assumes tracking of behavior that is quite extensive. The tracking should occur with the intention of influencing the user based on an analysis and prediction of personal preferences. The profiling required to trigger jurisdiction on this point is quite extensive. Longstanding online

advertising strategies rely on data that does not contain contact or identifying information of “natural persons,” but might rely on device identifiers, Internet Protocol (IP) addresses, cookies and other proxies for identifying a particular advertising subject on the Internet. One could reasonably argue that “monitoring” that focuses on serving targeted advertising to a user based solely on device identifier, IP address or other identifier that cannot be used to identify a “natural person” should not fall under the definition.

### INTERNATIONAL PRINCIPLES OF JURISDICTION AND THE GDPR

The GDPR contains a broad jurisdictional test. There are, however, specific principles under international law to assess when the extraterritorial reach of a state is permissible under international law. These recognized bases for asserting jurisdiction include the territoriality principle, the nationality principle, the passive personality principle, and the protective principle.<sup>5</sup> Especially with regard to online conduct, states have also increasingly exercised jurisdiction under variations of these principles such as the objective territoriality test and the effects doctrine.

**Territoriality and nationality:** The most commonly invoked principles are territoriality and nationality, which permit states to assert jurisdiction over what happens within their borders<sup>6</sup> as well as over acts committed by individuals and organizations of the state’s nationality (even if those acts take place outside of the state’s physical territory).<sup>7</sup>

**Passive personality and the protective principle:** In addition to asserting jurisdiction over acts committed abroad by their own nationals, states can sometimes assert jurisdiction for acts committed against their own nationals by foreigners. The passive personality principle permits states to exercise authority based on their connection to the victim of illegal conduct.

**The effects doctrine:** Finally, under the so-called “effects doctrine,” states can assert jurisdiction based on the fact that conduct taking place entirely outside of the state has substantial effects within the state.<sup>8</sup>

### REASONABLENESS ANALYSIS IN INTERNATIONAL JURISDICTION

Under any of the preceding three theories, the party seeking to assert jurisdiction must prove why it is reasonable to exercise extraterritorial jurisdiction under any one of the bases described above.<sup>9</sup> The factors to be considered include (1) the link of the activity to the territory of the regulating state, including whether it has a “substantial, direct, and foreseeable effect,” (2) the connections between the regulating state and the person who is responsible for the activity; (3) the nature of the activity, its importance to the regulating state, and the extent to which other states regulate it, (4) the “existence of justified expectations that might be protected or hurt by the regulation,” (5) the extent to which another state may have an interest in regulating the activity, and (6) the likelihood of conflict with regulation of another state.<sup>10</sup>

If an evaluation of these factors suggests that the extraterritorial application of the law in question would be unreasonable, courts are likely to find that there is no jurisdiction.

The concept of reasonableness is also closely aligned with the principle of comity, which is often characterized as the “golden rule” among nations — that is, that each state should respect the laws, policies, and interests of other states just as it would have others respect its own in similar circumstances. Comity dictates that states should generally avoid extraterritorial application of their laws against foreign citizens where those laws conflict.<sup>11</sup> Where two states have concurrent jurisdiction over an individual or a particular act, states should do a balancing test and defer to the state whose interests are clearly greater.<sup>12</sup>

### PRACTICAL CONSEQUENCES AND POLICY CONSIDERATIONS

Based on the triggers for the applicability of the GDPR discussed above, non-EU companies could consider specific measures to mitigate the risk that they may be found to be targeting EU audiences with digital advertising that might be claimed to be “monitoring the behavior” of EU data subjects. In particular, companies may consider the following strategies:

- Avoiding the use of EU languages other than English in the content displayed by the website;
- Not providing international dialing codes when providing telephone numbers for contact information;
- Not delivering products to the EU or permitting registration by users known to reside in the EU (for example, eliminating any EU-country selection option on a drop-down menu for registration information); and
- Not using the Euro or other EU currencies as currency for products or services sold.

Companies may take additional steps to further distance themselves from the EU market. For example, they could insert a sentence clearly indicating that the website is not intended for EU users, as many non-EU companies do today in their privacy policies. Of course, such statements can only be useful if the website itself does not undermine the statement.

In making these multifaceted decisions, however, it may be useful to consider that the jurisdictional reach of the GDPR should be tempered by the application of longstanding international principles that govern jurisdiction. For a purely non-EU entity, a realistic view of public international law would be a

useful complement to a clear-eyed look at the business realities of working within Europe.

#### REFERENCES

- 1 See, e.g. S. Greengard, Weighing the Impact of GDPR, *Communications of the ACM*, Vol. 61, p. 16 (November 2018), available at <https://cacm.acm.org/magazines/2018/11/232192-weighing-the-impact-of-gdpr/fulltext>.
- 2 See Council of the European Union, Draft Statement of the Council's Reasons 3 (Mar. 31, 2016).
- 3 GDPR, Recital 24.
- 4 *Peter Pammer v. Reederei Karl Schlüter GmbH & Co.*, KG (C-585/08) and *Hotel Alpenhof GesmbH v. Oliver Heller*, (C-144/09) (December 7, 2010), available at [curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08](http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08).
- 5 See Restatement (Third) of Foreign Relations Law § 402 (Am. Law Inst. 1987) [hereinafter Rest. (Third)].
- 6 *Id.* § 402(1)(a)-(b).
- 7 *Id.* § 402(2).
- 8 Rest. (Third) § 402(1)(c). See also *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 796 (1993).
- 9 Rest. (Third) § 403(1).
- 10 *Id.* § 403(2)(a)-(h).
- 11 See, e.g. *Hartford Fire Ins. v. California*, 509 U.S. 764 (1993).
- 12 Rest. (Third) § 403 cmt. e.

#### AUTHOR

Kurt Wimmer is Partner and U.S. Chair, Data Privacy and Cybersecurity Practice, Covington & Burling LLP, Washington D.C.

#### INFORMATION

A more extensive treatment is available at K. Wimmer, Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?, 68 *Syr. L. Rev.* 547 (2018).

## 59,000 data breaches reported across Europe

Since the GDPR entered into force on 25 May 2018, over 59,000 cases of personal data breaches have been reported to EU and EEA DPAs, a DLA Piper survey reveals.

Most notifications have been made in the Netherlands, Germany and the UK. DPA Piper survey suggests that the figures released by the EU Commission are conservative (41,500 breach notifications

by end of January), and that there are disparities in levels of reporting across EU Member States. The lowest numbers of reported breaches were made in Liechtenstein, Iceland and Cyprus with 15, 25 and 35 reported breaches respectively.

The Netherlands, with 89.8 reported breaches per 100,000 people topped the list when the number of notifications were weighted against country popula-

tions, followed by Ireland and Denmark. Of the 26 EEA countries where breach notification data is available, the UK, Germany and France ranked tenth, 11th and 21st respectively on a reported breach per capita basis.

• See *DLA Piper GDPR data breach survey*, at [bit.ly/2GIWaZ3](http://bit.ly/2GIWaZ3) and *EU data* at [bit.ly/2Rdeyef](http://bit.ly/2Rdeyef)

# FEDMA voices its concerns about e-Privacy draft regulation

The organisation wants to reopen the negotiations on unsolicited communications. **Laura Linkomies** talked to FEDMA's Director General, Mathilde Fiquet, in Brussels to find out why.

The Romanian presidency of the EU Council, which hopes to reach agreement on the e-Privacy file at Council within the next few months, faces many unresolved issues in the draft e-Privacy Regulation<sup>1</sup>. While there have already been two meetings dedicated to e-Privacy in January, the forthcoming elections for the European Parliament 23-26 May 2019 in the 27 EU Member States may cause delay, and the stakeholders are still some way off starting Trilogue which involves the Council of Ministers, the European Parliament and the European Commission negotiating to reach a consensus.

The previous Presidency of the Council, Austria, proposed deleting Article 10 that would make “do not track” settings legally enforceable, but some Member States do not support that. Other issues still to be resolved include confidentiality of communications, browser settings and cookie walls.

FEDMA, the Federation of European Direct and Interactive Marketing, states that the e-Privacy proposal is not just about cookies. B2B marketing and unsolicited communications are a major issue but have not received nearly as much attention.

communications. The article prescribes that natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons who have given their consent.

“Article 16 is not talked about that much. Yet there is some misunderstanding about it – unsolicited communications are not necessarily always direct marketing. So we have tried to raise the profile of Article 16. Member States tend to think it is not a topic that needs further discussion – however Article 16 needs to be reopened to assess the actual impact that it will have on the industry in terms of being able to contact existing customers and prospects.”

Article 16, as proposed in the current draft text by the Council<sup>2</sup>, now states that natural or legal persons shall be prohibited from using electronic communications services for the purposes of sending or presenting direct marketing communications to end-users who are natural persons, unless they have given their consent.

The e-Privacy regulation also includes some flexibility to this general rule of consent, such as for marketing to existing clients as long as certain

raise two issues regarding this point:

1. For the first time, there is a definition of direct marketing at EU level; the FEDMA code of conduct includes one but the European Commission has taken a very different approach. The proposed definition seems to include online display advertising. From FEDMA's point of view these are two separate activities which have different definitions.
2. The rules that apply to direct marketing mean that the users can at any time decline further direct marketing whether it is a phone call, email or mail. With regard to display advertising, consumers cannot object to its presence on websites – the decision is with the publisher whether to display the ad or not. There is confusion between the control that the user should have over their privacy when the ad is targeted, and the control the user should have over the presence of the ad. So in FEDMA's view, digital advertising is separate from direct marketing.

Fiquet explained that the problem with the current approach, to solve the challenge of privacy with digital advertising, is that it is dealt with in Article 16 about unsolicited communication, while in fact it is now addressed in Article 8 which is about cookies and tracking. Users are already asked for consent to tracking for advertising purposes. Having both articles apply to digital advertising would cause confusion for consumers and the industry, Fiquet said.

---

## Article 16 needs to be reopened to assess the actual impact that it will have on the industry.

---

FEDMA's Director General, Mathilde Fiquet, explained in an interview that FEDMA follows a number of issues with regard to e-Privacy; obviously Article 8 on tracking and cookies, and Article 10 on information and options for privacy settings to be provided. However, lately, most of FEDMA's work has been focused on Article 16, unsolicited

safeguards are in place, voice to voice telemarketing and B2B marketing communications when decided by Member States. However, while the e-Privacy regulation does not fundamentally change the rules for direct marketing, these rules are likely to have a much broader scope due to a new definition of direct marketing.

Fiquet said that FEDMA wants to

### BUSINESS-TO-BUSINESS MARKETING

“B2B marketing currently benefits from a more flexible regime – the former e-Privacy Directive does not regulate B2B marketing – it refers to Member States to decide on the level of protection needed. The draft regulation keeps the same wording –

the problem is that now the GDPR is in place, widening the concept of personal data, it is not clear whether companies can continue to communicate with their business partners if the contact details include personal data.”

This is potentially a huge issue, as most work email addresses now include a name attached to the organisation, rather than a more generic info@email-address. As the email addresses including names of persons would be regarded as personal data, there is no clarity yet whether these types of marketing messages would benefit from an exemption or not.

“This is a huge concern. We want to keep the flexibility – we think it is working well. Member States have not requested this area to be further regulated but on the other hand this is now a loophole that has not been addressed. Otherwise there will be different interpretations at Member State level which would have an impact on business practices.”

Fiquet said FEDMA is not against the proposal as such – just that businesses need clarity. There has been positive feedback from Member States on FEDMA’s view, she said.

### TELEMARKETING

“Telemarketing is still a significant activity in many markets such as in the UK, Poland and Finland. It is mostly smaller businesses and charities that use telemarketing. E-Privacy proposals leave it up to the Member States whether to apply an opt-in or opt-out regime.”

Now, roughly 70% of European countries operate an opt-out system, and 30% opt-in. Most countries that demand opt-out, use the so-called Robinson list, which is a central register. The problem is the definition of automated calls and connecting systems.

“Pre-recorded calls require a consent. Definition of automated calls, however, now also include technology we call predictive diallers. It enables voice-to-voice calls and would require, according to the current proposal, an opt-in. So even if the e-Privacy proposal gives the impression in Article 16 that there is some flexibility with opt-in and opt-out for telemarketing, in fact in practice the vast majority of the

### PROPOSED E-PRIVACY REGULATION

**Article 6:** Permitted processing of electronic communications data.

**Article 8:** Protection of information stored on end users’ terminal equipment, such as cookies. Requires browsers and other software enabling access to the Internet to offer privacy settings to users.

**Article 10:** Information and options for privacy settings to be provided.

**Article 16:** Unsolicited communications.

telemarketing industry is moving to opt-in simply because of the technology that is being used. So far, no one wants to address this problematic issue. For example, in the UK which operates an opt-out regime, any company conducting telemarketing using a predictive dialler would have to switch to an opt-in system. This would have a major impact on business.”

### PRIVACY SETTINGS

Article 10 on providing information and options for privacy settings, and especially browser settings, is another controversial area. Some Member States have mentioned the need for a new impact assessment, and questions have been sent to the European Commission.

### CONSENT

The GDPR and the e-Privacy Regulations should complement each other. However, consent is one of the issues where there will be challenges.

“e-Privacy relies largely on consent whereas the GDPR provides many other legal bases for processing. There are many questions whether websites can refuse access for individuals who are seeking a service but do not consent to advertising.”

“We have interpretations by national DPAs and the European Data Protection Board about what freely given consent means, and there are complaints in parallel. The GDPR is being implemented. The e-Privacy Regulation could bring some clarity for publishers but but whatever the way forward, it risks being in conflict with the GDPR.”

Fiquet says FEDMA is not advising members as yet about e-Privacy compliance as there is still so much uncertainty about fundamental issues. She says the starting point would be to be

compliant with the GDPR and its consent requirement, as well as ensuring that companies have a procedure to object to direct marketing.

“The main message from FEDMA is to do what is right by the consumer. Think ethically what is fair and try to empower consumers.”

### POSSIBLE TIMEFRAME

Fiquet thinks that the Member States are looking to establish their position as soon as possible as they are under much pressure by the European Parliament and the European Commission. However, she thinks the Trilogue will not start before the European elections.

The Council discussion last summer indicated that Member States regard the current text as a good basis for discussion, but there are also some fundamental differences especially with regard to browser settings and Article 10. Article 8 is close to being agreed.

“The file could be adopted by the end of the year but will also depend a lot on the new Parliament. Birgit Sippel, the rapporteur at the Parliament for this file is likely to be re-elected so we can assume she will fight for this file to remain high on the agenda.”

If the Romanian Presidency reaches a common position by June 2019, then the file would move to the Finnish presidency after the election. Originally, when the Commission aimed at matching the GDPR timetable, the implementation period was proposed to be just six months, at the time when they were hoping to match the GDPR timetable. Now, it is more realistic than the implementation period will be close to two years, Fiquet said.

### REFERENCES

- 1 [ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications](https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications)
- 2 [www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU\\_39172/imfname\\_10848802.pdf](https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf)

# CNIL fines Google €50 million – the biggest GDPR fine so far

Google says it will appeal. **Mark Sherwood-Edwards** of This is DPO explains the decision, and why the “one-stop-shop mechanism” could not be used.

On 21 January, the CNIL (France’s DPA) fined Google €50 million for breaches of the GDPR. The amount of the fine is unlikely to worry Google unduly (it was fined €4.3 billion by the EU Commission in July 2018 for abuse of its dominant position in relation to the Android system – Google is appealing.) but the fine shows that things are hotting up for companies that use mobile phones as platforms from which to gather and exploit personal data.

How many users were affected in total? The CNIL’s notice doesn’t say, but a quick calculation suggests that approximately 20 million users were affected, which works out as a fine of €2.5 per affected user – not exactly heavy stuff.

The Google fine was not the CNIL’s first foray into privacy breaches relating to data collected via mobile phones. It has previously taken action against four French companies that collected (primarily) user location data. The last of these, Vectaury (see p.6 in this issue), had been ordered to destroy its database of 67 million records on the basis that the consents obtained were not valid and therefore the data was not properly obtained. Why the CNIL did not also take the same action against Google is unclear. A possible reason is that the GDPR breaches the CNIL was aware of (the CNIL’s investigation was carried out largely online) related to an Android operating system that was used by only 7% of Android users, and it would have been difficult to separate this 7% from the remaining 93%.

## WHAT HAPPENED?

So, what did Google get wrong? The CNIL started from the position that Google was a huge user of very detailed personal data (*massifs et intrusifs* is the phrase used by the CNIL) – a position that no-one was likely to argue with. If you are

collecting this amount of personal data to this amount of granularity (and the CNIL made the point that Google has over 20 different services collecting personal data, and a virtually unlimited ability to combine this data) then, according to the CNIL, you are under an obligation to make sure that you are really upfront and clear about how you are planning to use the data you collect: there will be little tolerance for error. Equally, you have to make sure you are rigorous in your compliance with the GDPR’s obligations.

Against this background, the CNIL found the following failures:

1. It was hard for users to find out how their data was going to be used. The CNIL gave a number of examples where a user would have to click five or six hyperlinks before it could find the relevant information. From the user’s perspective, the information was not provided in a clear and easy-to-access manner. On the contrary, it was fragmented and hard to navigate.
2. Some of the Google uses were described in vague marketing-speak: again, it was difficult for an ordinary user to understand what the data was really going to be used for.
3. There were some basic GDPR failures. For example, some uses (which required consent) were pre-ticked and, for some types of data neither a specific retention period, nor criteria on which the retention period would be decided, were set out (ie. a breach of Article 13).
4. Some parts of the privacy documentation referred to the lawful basis as being consent, others parts referred to the lawful basis as being legitimate interest. Google had subsequently confirmed to the CNIL that it was all intended to be based on consent.
5. Given that consent was the basis, valid consent could not be given by a user. The poor quality of the

documentation meant that the consent was, by definition, not informed.

6. The nature of consent as a lawful basis meant that it had to be specific to the purpose the data was going to be used for, and therefore each purpose required its own dedicated consents (ie. if there are ten purposes, then ten consents are required). Google had obtained the consents *en bloc*: therefore, by definition, they were not specific and therefore not valid.

On the facts, none of the CNIL’s conclusions are particularly surprising. Whether a disclosure is clear or not clear to an average user is something which, failing any objective evidence, is always likely to be subjective. However, it is noteworthy that Google did not put forward any evidence showing that it had tested its approach with user groups. Therefore, it was unable to present any objective evidence to rebut the CNIL’s subjective assessment.

## HOW HAD GOOGLE GOT ITSELF INTO SUCH A MESS?

This was not discussed by the CNIL, but there are two likely reasons. The first possible reason is that, given the runaway success of the Android operating system, Google lost sight of the wood from the trees. What had started off as simple and clear had, after a number of patches, adjustments and improvements, turned into something that was fragmented and confusing. The fact that the Android system is run out of the US, not the EU, probably did not help things either.

The second possible reason is that Google relied too much on the fact that those users with Google accounts also had access to a number of settings and parameters which allowed them to control how their personal data would be used. That approach was fallacious because a) not all Android users would open a Google account, and b) the mere

fact that Google had made this control functionality available (and the CNIL went out of its way to praise the Google tools, as well as the progress Google had made it making privacy more central) was not enough to cure, and legally could not cure, the failings that occurred right at the beginning when the user was onboarded.

### WHY NOT IN THE REMIT OF IRELAND'S DPA?

The CNIL's notice is about 30 pages long. Of those 30 pages, only about 20 cover the issues set out above. The first ten pages consist of Google trying to find legal arguments to escape the clutches of the CNIL and arguing that the right body to regulate Google was the Irish Data Protection Commission or the European Data Protection

Board. However, Google Ireland was not the main establishment, and therefore the Irish DPC not the lead authority, because Google Ireland had no decision-making authority in relation to the Android system (as the CNIL points out, Google Ireland did not even have a DPO). The controller in relation to data collected by the Android system was Google LLC, the US company: there being no main establishment for Android in the EU, the CNIL was free to proceed against Google LLC.

Those first ten pages are an amusing read (for those that like that kind of thing) as Google twists and turns but is slowly reeled in by the CNIL, and there's a particular point where amusing becomes high farce when Google argues that the fact the CNIL's

documents were provided only in French is (together with some other factors) a breach of Article 6 of the European Convention of Human Rights (right to fair trial). Not exactly a huge vote of confidence in Google Translate, and doubly ironic because the argument is brought by one of the largest companies in the world sitting on a cash pile (\$103bn in March 2018) that makes the CNIL's yearly budget look miniscule, and brought against the country that (more or less) invented human rights.

#### AUTHOR

Mark Sherwood-Edwards is Founder of This is DPO, an external DPO service.  
Email: mse@thisisdpo.co.uk

# Japan to issue further data protection legislation

**Hiroshi Miyashita**, Associate Professor, Chuo University, Tokyo, reports on the next steps in Japan after the EU-Japan mutual adequacy decision.

On 23 January 2019, the European Commission and Japan's Personal Information Protection Commission (PPC) adopted a mutual adequacy decision, which represents the world's largest area of safe data transfer<sup>1</sup>. Five days after this decision, Japan's PPC proposed several items to be reviewed for possible amendments to Japan's privacy law, the Act on the Protection of Personal Information (APPI). This law is subject to a three-year cycle review under Art. 12 of its supplementary provisions.

According to the PPC plan, the first proposal will be publicized in spring 2019 followed by a consultation with a wide-range of stakeholders, to be followed by a public consultation on the PPC's plans (see the table). If the Cabinet or *Diet* (Japan's bicameral legislature) decides to amend the APPI, the bill is expected to be submitted in the *Diet's* next ordinary session in 2020 in the three-year legislative cycle from May 2017 to be ready for the next adequacy decision review by January 2021. The following seven items, discussed

below, have been tabled by the PPC:

#### 1. Individual rights with regard to personal data (access, utilization cease and erasure)

- the right to access (clarification of the right of access under the amended APPI)
- rectification, utilization cease and erasure
- opt-out clause (anti data-broker measures)
- diverse forms of data utilization and individual rights
- position of foreign countries (institutions and practices)

#### 2. Breach notification

- effectiveness of law enforcement
- meaning of security management measures
- burden on business operators
- scope and form of notification
- notification to data subjects
- position of foreign countries (institutions and practices)

#### 3. The system to encourage business operators to protect personal information

- authorized personal information

protection organization [a private organization authorized by the PPC to promote self-regulatory frameworks in its business sector under Art. 47 of the APPI]

- self-regulatory practices by business operators
- development of international standards and certification (PrivacyMark, ISO/IEC27001)
- systems similar to a Privacy Impact Assessment (PIA) (for example, Assessment of personal information protection under the MyNumber Act, and reaching the requirements of the innovative data industry utilization plan under the Special Act on Productivity Improvement)

#### 4. Measures regarding data utilization

- systems regarding anonymous processing
- technical developments surrounding data such as Artificial Intelligence and the Internet of Things
- targeted advertising by using

- cookies and social plugins
  - businesses processing personal data (such as information banks)
  - balance between protection and utilization (the relationship between regulation and innovation)
  - international trends
- 5. Penalties**
- deterrent effect on domestic and international business operators
  - effectiveness of law enforcement (monitoring and methods of investigation and enforcement)
  - compliance with the law by business operators
  - position of foreign countries (institutions and practices)
  - relationship with other domestic laws (institutions and practices)
- 6. Extra-territorial application of law**
- ability to enforce the law against foreign companies
  - cooperation with foreign Data Protection Authorities and other enforcement agencies
  - other domestic laws regarding

- extra-territorial application of the law
  - position of foreign countries (institutions and practices)
- 7. International harmonization and cross-border transfer**
- developments regarding international harmonisation of systems
  - cross-border transfers
  - position of foreign countries (institutions and practices)
  - data localisation and government access

In the context of the EU-Japan mutual adequacy decision, the European Data Protection Board (EDPB) issued an “opinion” and the European Parliament adopted a “resolution” on the draft adequacy decision. Some of the issues are reflected in the opinion and the resolution such as:

- restrictions on individual rights (opinion para 77 and 92 and resolution para 13),
- penalties (opinion para 130 and resolution para 21), and
- cross-border transfers (opinion

para 17, 98, 101, 106 and resolution para 20).

In particular, Japan has been active in the Asia-Pacific Economic Cooperation’s Cross Border Privacy Rules (APEC CBPRs), but was excluded from using it for onward transfers under APPI’s Supplementary Rules. Japan’s diplomatic privacy policy may face the dilemma of having both the EU adequacy agreement and the APEC CBPRs unless both the EU BCRs and the APEC CBPRs achieve convergence and seek interoperability<sup>2</sup>. This dilemma is evident in the adequacy decision which states that the ‘APEC Cross-Border Privacy Rules (CBPR) System ...[is] clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules’ (adequacy decision para 79).

#### DATA PROTECTION SCANDALS IN JAPAN

Along with these issues to be discussed in the coming months, there are several data protection scandals and concerns in Japan. A few weeks before the adequacy decision was agreed and published, several Japanese newspapers reported that the law enforcement agencies had prepared a list of companies and accessed their private data on a voluntary disclosure basis without warrant under the Code of Criminal Procedure<sup>3</sup>. According to the newspaper articles, the Prosecutor’s Office had a list of approximately 290 companies on their enquiry sheet<sup>4</sup>.

The major loyalty card program card (T-card), which has approximately 67 million customers for more than 941,000 stores across Japan, has, since 2012, been voluntarily providing customers’ data to law enforcement agencies, on request, without notifying the customers in the loyalty card program’s privacy policy<sup>5</sup>. In Japan, no major companies are transparent about the numbers of data subject access requests and replies<sup>6</sup>.

A lack of transparency about government access to private data, in spite of the commitments expressed in the Annex II (p.20), was one of the concerns of the EDPB (opinion para 146) and the European Parliament (resolution para 23). In addition, the UN Special Rapporteur on the right to privacy also expressed concerned about the

#### REFERENCES

- 1 European Commission, Press Release: European Commission adopts adequacy decision on Japan, creating the world’s largest area of safe data flows. [europa.eu/rapid/press-release\\_IP-19-421\\_en.htm](https://europa.eu/rapid/press-release_IP-19-421_en.htm)  
PPC, Press Release: The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force, 23 January 2019. [www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/](http://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/)
- 2 See Graham Greenleaf, Japan’s proposed EU adequacy assessment: substantive issues and procedural hurdles, *Privacy Laws & Business International Report* vol.154 (2018) pp. 1 & 4-8.
- 3 ‘Public offices or public or private organizations may be asked to make a report on necessary matters relating to the Investigation,’ Code of Criminal Procedure Art. 197 (2).
- 4 The Prosecutor listed how to obtain customers’ data and hold it from the 290 companies, 3 January 2019, Tokyo newspaper (in Japanese). [www.tokyonp.co.jp/s/article/2019010301000873.html](http://www.tokyonp.co.jp/s/article/2019010301000873.html)
- 5 T Card customer data handed to police and prosecutors without court approval since 2012, operator says, *The Japan Times*, 21 January 2019. [www.japantimes.co.jp/news/2019/01/21/national/operator-popular-reward-program-t-card-supplying-clients-personal-information-police-prosecutors/#.XFtT3c\\_7Tow](http://www.japantimes.co.jp/news/2019/01/21/national/operator-popular-reward-program-t-card-supplying-clients-personal-information-police-prosecutors/#.XFtT3c_7Tow) According to the newspaper articles, the government official stated that “there is no help for it being criticized that the Annex II was a temporary excuse. Two year ahead of reviewing the adequacy decision embraces an uneasiness”. Yomiuri Newspaper, 7 February 2019 p.7 (in Japanese).
- 6 LINE, the only major mobile messenger app company in Japan, has publicized its transparency report since 2017. The recent numbers show that LINE received 1,576 requests and replied to 76 percent of the total requests in January to June 2018. [linecorp.com/en/security/transparency/2018h1](http://linecorp.com/en/security/transparency/2018h1)
- 7 UN Special Rapporteur on the right to privacy, Joseph Cannataci, Letter to Prime Minister of Japan, 18 May 2017. [www.ohchr.org/Documents/Issues/Privacy/OL\\_JPN.pdf](http://www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf)
- 8 As for the information bank, see the White Paper on Information and Communications at p.5 [www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/chapter-1.pdf#page=2](http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/chapter-1.pdf#page=2)

lack of transparency and supervision of government access to private data during the legislative process of the so-called Anti-Conspiracy Act in 2017<sup>7</sup>.

The so-called “information bank system” is planned to be put into place in March 2019 for collecting and sharing personal data in personal data stores with the consent of the data subjects<sup>8</sup>.

The Act on Anonymously Processed Medical Information to promote research development in the medical area entered into effect in

May 2018 for the purpose of big data analytics in the medical area.

An automatic facial recognition system will be introduced for identification checks at the ceremony for the Emperor’s thirtieth anniversary of his reign on 24 February and at any similar ceremony in the future. These plans on the use of biometric data will further contribute to privacy debates in Japan.

Japan’s adequacy decision, along with the valuable opinion by the EDPB and the resolution by the European Parliament, provide future homework

for Japanese stakeholders and also the other third countries seeking an EU adequacy decision.

## AUTHOR

Hiroshi Miyashita is Associate Professor at Chuo University, Tokyo, Japan.  
Email: hmiya.64r@g.chuo-u.ac.jp

# Global data privacy laws 2019: 132 national laws and many bills

The rush to update existing privacy laws reflects the need or wish to become European Union GDPR-compliant. By **Graham Greenleaf**.

In 2017-18, the number of countries that have enacted data privacy laws has risen from 120 to 132, a 10% increase. These 132 jurisdictions have data privacy laws covering both the private sector and public sectors in most cases, and which meet at least minimum formal standards based on international agreements.<sup>1</sup> At least 28 other countries have official Bills for such laws in various stages of progress, including nine that have introduced or replaced Bills in 2017-18. Many others, in the wake of the GDPR and “modernisation” of Convention 108, are updating or replacing existing laws.

The accompanying global Tables give details of these data privacy laws and bills, as at January 2019. They are the 6th edition, since the 1st edition in 2011 identified 76 countries having such laws.<sup>2</sup> The 4th edition (January 2015) identified 109 countries,<sup>3</sup> and the 5th edition (January 2017) identified 120.<sup>4</sup> These Tables have been cited by various international bodies as the most authoritative assessment of the global tally of countries with data privacy laws.<sup>5</sup>

## NEW AND REVISED LAWS, AND BILLS

New laws enacted in 2017-18 are first reviewed, followed by a brief note of

laws revised and strengthened, and then Bills for new law, or to revise existing laws.

**Twelve additional countries with new laws:** The twelve new laws enacted since the 2017 5th edition of this survey are as follows. The first four of these laws have been analysed previously in PLBIR.<sup>6</sup>

1. **Cayman Islands** (Caribbean) – Data Protection Law 2017, Law 33 of 2017.
2. **Mauritania** (West Africa) – Loi 2017-020 sur la protection des données à caractère personnel.
3. **Niger** (West Africa) – Loi 2017-28 relative à la protection des données à caractère personnel.
4. **Guinea-Conakry – Republic of Guinea**, formerly French Guinea (West Africa) – Loi L/2016/037/AN relative à la cybersécurité et la protection des données à caractère personnel.
5. **Algeria** (North Africa) – Law No. 18-07 dated 10 June 2018 on the protection of individuals in the processing of personal data will commence operation one year after the national data protection authority it creates is established. It goes beyond minimal data protection requirements in a few areas, including processing primarily based on

express consent (with detailed exceptions), protection of categories of sensitive data, and requirements for cross-border transfers. Like many African laws, it also includes requirements for registration of data processors, and prior authorization of processing in some cases.

6. **Brazil** (South America) – The General Data Privacy Law (GDPL) of Brazil (Law No. 13,709 of 14 August 2018) was the most anticipated data privacy law of recent years, due to Brazil’s economic and political importance. It is based substantially on the EU’s GDPR,<sup>7</sup> with similar requirements for data exports limited by adequacy requirements of the destination, data protection impact assessments, data protection officers, data breach notifications to the DPA and the data subject, limits on automated processing, and administrative fines of up to 2% of a company’s previous year’s revenue in Brazil. The outgoing President created a Data Protection Authority on 28 December 2018 as one of his final acts,<sup>8</sup> but it needs to be ratified by the legislature in its next session.
7. **Panama** (South America) – The Law of Protection of Personal Data

was enacted by the Panamanian legislature on October 24, 2018, but has not yet been gazetted (after which it will take effect in two years). The National Authority of Transparency and Access to Information will administer the law, assisted by the National Authority for Government Innovation in relation to information and communication technologies. The law has been criticised by civil society groups as rushed and too weak.<sup>9</sup>

8. **St Kitts & Nevis** (Caribbean) – The Data Protection Act 2018 was enacted on May 4, 2018, just after the complementary Freedom of Information Act 2018. The Act is largely derived from an Organization of Eastern Caribbean States (OECS) model,<sup>10</sup> drawing upon EU sources as well as the OECD. It is the third country to enact a law based on this model. It covers both the public sector and the private sector in respect of commercial transactions. The Act goes beyond minimal principles by including requirements in relation to sensitive data, and limits on data retention. The Information Commissioner also administers the FOI Act, and is empowered to issue enforcement notices. Data subjects can take civil actions to seek compensation for breaches of the Act, and there are a range of criminal penalties.

9. **Lebanon** (Middle East) – The Electronic Transactions and Personal Data Law (E-Transactions Law) was enacted in October 2018, with Part V applying to Personal Data Protection. The personal data provisions apply to all automatic and non-automatic processing of data of a personal nature (not limited to e-commerce), with broad definitions of personal data, processing, processors and data subjects. It has some provisions going beyond basic protections, such as those concerning automated processing. However, no data protection authority is created, and the law has been criticised as being under the control of the Executive.<sup>11</sup>

10. **Bahrain** (Middle East) – Bahrain's Law on the Protection of Personal Data was published on 19 July 2018, and will come into effect on 1

GEOGRAPHIC DISTRIBUTION OF DATA PROTECTION LAWS			
Region	Countries	DP Laws	Percentage
Africa	58	25	43%
Caribbean	29	12	41%
Other European	29	26	90%
EU	28	28	100%
Asia	28	15	54%
Latin America	22	12	55%
Middle East	14	8	57%
Pacific Islands	13	0	0%
Central Asia	6	2	33%
N. America	2	2	100%
Australasia	2	2	100%
<b>TOTAL</b>	<b>231</b>	<b>132</b>	<b>57%</b>

August 2019.<sup>12</sup> The law establishes a Data Protection Authority, and an unusual intermediary role for 'Data Protection Supervisors'. The law's extraterritorial scope covers those outside Bahrain carrying out Bahrain-based processing. The planned operation of Amazon Web Services cloud computing centres from Bahrain is said to be a motivating factor.<sup>13</sup> Bahrain becomes the second of the Gulf Cooperation Council member states, after Qatar, to have a national data protection law.

11. **Bhutan** (South Asia) – The Information, Communications and Media Act of Bhutan 2018<sup>14</sup> was passed by the National Assembly in 2017, and came into force in mid-2018. The Act contains sufficient provisions to give Bhutan a minimal data privacy law. Although only applying to provision of the 'ICT and Media Sectors', and providers and users of their service, 'ICT services' are given a very broad

meaning, and will normally include public facilities (and thus the public sector), so the law will cover almost any use of electronic information. The act also establishes a Bhutan Infocomm and Media Authority which is not fully independent, but has powers to investigate and resolve complaints. There are provisions for compensation, and for offences.

12. **People's Republic of China** (North Asia) – The Cybersecurity Law of 2016 appeared ambiguous as to whether it provided a right of individual access (it possibly implied one), and was also of somewhat uncertain scope.<sup>15</sup> However, these doubts are now sufficiently resolved. The E-Commerce Law of 2018 (in force 1 January 2019), a law of China's second highest legislative body, is both of wide scope within the private sector, and explicitly provides that users may make 'inquiries' concerning their information.<sup>16</sup> These approaches are

consistent with the recommended standard entitled Information Security Techniques - Personal Information Security Specification promulgated by China's National Standardization Committee, and effective 1 May 2018.<sup>17</sup> These data protection laws co-exist with the Social Credit system, which is emerging as the world's most pervasive and totalitarian surveillance system.<sup>18</sup>

Fifty countries have enacted new data privacy laws in the first nine years of this decade, an average of 5.5 per year. Continuation of this growth in 2019 would result in at least 55 new laws for the whole decade, a total of at least 137 by 2020.

It is worth re-stating that the inclusion of laws in this list only means that they meet the minimum formal requirements for a data privacy law, and says nothing about whether the laws are effectively enforced (a much more complex and contentious enterprise, as 'adequacy' assessments show), or about the data surveillance context in such laws exist (of which China is the prime example), and which may largely nullify their potential benefits.

**Geographical distribution:** The new laws listed above demonstrate the continuing global diffusion of data protection laws, being from West Africa; North Africa; South America; Caribbean; Middle East; and North and South Asia. The table (p.15) shows regional analysis of all 132 laws, where the whole number of countries in a region<sup>19</sup> is compared with the number

**many other countries:** Numerous countries have also updated their data protection laws since 2017, invariably strengthening them in ways which reflect some aspects of the GDPR.

The EU's General Data Protection Regulation (GDPR), although it provides for uniform data protection rules applying across the EU, also requires EU Member States to exercise choice in implementing certain GDPR requirements,<sup>20</sup> and to implement other GDPR requirements such as administrative fines in order to fit the procedures of the local legal system. As a result, all 28 EU Member States must implement new data protection laws. During 2017-18, 23/28 have done so, with laws still only in draft in five: Bulgaria; Czech Republic; Greece; Portugal; and Slovenia. Details of the 23 amending laws can be found elsewhere,<sup>21</sup> and new titles of laws are in the Table. Many jurisdictions have decided to implement in a separate law the LED Directive (the so called "Police" Directive). By decision of 6 July 2018, the EEA Joint Committee announced the incorporation of the GDPR in EEA countries, Norway, Iceland and Liechtenstein, and regulations have followed.

Because of the need to accede to the new Convention 108+, the 25 non-EU countries that are parties to Convention 108 will also need to amend their laws in coming year in order to ratify Convention 108+. Serbia, Moldova, Montenegro and San Marino have done so in 2017-18.

Other significant examples of

which are incompatible. Provisions similar to the GDPR include extra-territorial application, privacy by design, direct liability of processors, data breach notification to the DPA and to the data subject, approved codes of conduct, onus of proof on the data controller in most cases, detailed requirements for adequacy of the level of protection offered by third countries, data protection impact assessment, mandatory data protection officers, meaningful information required about the logic involved in automated data decisions, a right to data portability, and a right to be forgotten. Other GDPR features like data minimization, demonstrable controller accountability, and certification proceedings have not been replicated.

**Mauritius** updated its 2004 law on 22 December 2017, and the new Data Protection Act 2017 (Act No. 20 of 2017), a GDPR-influenced law previously noted.<sup>23</sup> Although a small African island, Mauritius is significant because of the strength of its economy, because it was the second non-European party to Convention 108, and because it is in the early stages of applying for an adequacy assessment under the GDPR.

**Uruguay**, the first non-European country to accede to Convention 108 (and already a signatory to Convention 108+), also has a positive adequacy assessment from the EU. To maintain both these statuses, Uruguay needed to update its data protection law. It did so with Law No. 19.670, which strengthened four aspects of its law: extra-territorial scope; data breach notification; accountability (requiring controllers to implement other GDPR elements); and data protection officers.<sup>24</sup>

The two countries of the **Channel Islands**, Crown Dependencies of the UK, the Bailiwicks of Guernsey and Jersey, are not subject to the laws of either the UK or the EU (and are not members of the Council of Europe). The **Isle of Man**, not part of the UK, also has self-governing status, and also with foreign affairs and defence handled by the UK. All three jurisdictions have already updated their data protection legislation with the aim of compliance with the GDPR. All three are currently classed as adequate under the 1995 Directive, a status which is to

---

## In all regions, except the Pacific Islands, at least one third of countries now have a data privacy law.

---

of countries with data privacy laws, and the percentage result then shown.

Of the total of 231 countries, the 132 with data privacy laws constitute 57%, so since about 2014 (then 115 countries with laws) the majority of countries have had data privacy laws. In all regions, except the Pacific Islands, at least one third of countries now have a data privacy law.

**Revised and stronger laws in**

updated legislation outside the EU include Mauritius, Benin, Uruguay, Canada and the Channel Islands. Details follow.

**Benin** has enacted the most GDPR-like legislation outside the EU.<sup>22</sup> Its "Code du numérique" (enacted 13 June 2017), is a comprehensive "cyberlaw" of more than 650 articles. Chapter V on data protection is a substitute for those parts of its law of 2009 on data protection

be re-examined under the GDPR in coming years.

**Canada's Digital Privacy Act** (S.C. 2015, c. 32) of 2018 amends its existing law (PIPEDA) to introduce data breach notification requirements, but otherwise does little to address the differences between Canadian law and the GDPR. It too has adequacy status under the Directive.

Other countries that updated their laws in 2017-18 include Peru, the Kyrzyg Republic, and Kazakhstan.

**Bills for new laws and stronger laws:** Many countries claim ambitions to enact new or stronger laws so as to be able to consider applying for 'adequate' status under the EU's GDPR. Other countries are enacting or updating a data privacy law without expressing such ambitions.

*Recent Bills for new laws:* At least nine additional countries (since 2016) without data privacy laws have official data privacy bills for new laws under consideration: **Barbados, Kenya, Jamaica, Iran, Zambia, Pakistan, El Salvador, Suriname and Egypt.** Altogether 28 countries are known to have official Bills for new laws (see the Tables).

*Major updating Bills for existing laws:* Important recent Bills to update or replace existing laws, but not yet enacted, include those in the following countries (shown in the Tables<sup>25</sup>): **Argentina, Chile, Israel, India, Indonesia, Korea, New Zealand, Thailand, Tunisia and Zimbabwe.** It is obvious from the economic importance of this list of countries that the impetus to update existing laws, in order to make them potentially GDPR-compliant, has become a significant driver of international law reform. This is the most important data privacy development in 2018. Argentina and New Zealand are examples of necessity to maintain existing EU adequacy status, whereas Korea is a country currently seeking GDPR adequacy status. Three of the Asian countries – India, Indonesia and Thailand – are in the process of replacing largely useless and limited existing laws with completely new laws with strong GDPR-like elements.

*For whom the Bill tolls:* Unlike Uruguay, Canada, Jersey and Guernsey (all with newly updated laws), there are countries that currently have EU ade-

## REFERENCES

- 1 For the standards applied, see a summary in Greenleaf, G 'Global data privacy laws 2015: 109 countries, with European laws now in a minority' (2015) 133 *Privacy Laws and Business International Report*, 14-17, February 2015.
- 2 Greenleaf, G 'Global Data Privacy Laws: Forty Years of Acceleration' (2011) 112 *Privacy Laws and Business International Report*, 11-17, September 2011 [ssrn.com/abstract=1946700](http://ssrn.com/abstract=1946700)
- 3 Greenleaf, G. 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority' (2015) 133 *Privacy Laws & Business International Report*, February 2015
- 4 Greenleaf, G 'Global Tables of Data Privacy Laws and Bills (5th Ed 2017)' (2017) 145 *Privacy Laws & Business International Report*, 14-26 [papers.ssrn.com/abstract\\_id=2992986](http://papers.ssrn.com/abstract_id=2992986)
- 5 For example, the European Commission Exchanging and Protecting Personal Data in a Globalised World (Communication from the Commission to the European Parliament and the Council), 10 January 2017, COM(2017) 7 final, footnote 32; see also European Data Protection Supervisor (EDPS) [edps.europa.eu/sites/edp/files/publication/16-02-05\\_closing\\_remarks\\_cpdp\\_en.pdf](http://edps.europa.eu/sites/edp/files/publication/16-02-05_closing_remarks_cpdp_en.pdf), UN Special Rapporteur on the Right of Privacy [www.ohchr.org/Documents/Issues/.../SR.../2018AnnualReportAppendix2.docx](http://www.ohchr.org/Documents/Issues/.../SR.../2018AnnualReportAppendix2.docx), Council of Europe [www.coe.int/en/web/data-protection/articles-speeches-presentations](http://www.coe.int/en/web/data-protection/articles-speeches-presentations), and UNCTAD [unctad.org/en/Pages/DTL/STI\\_and ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx](http://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx)
- 6 G. Greenleaf and B Cottier 'Data privacy laws and bills: Growth in Africa, GDPR influence' (2018) 152 *Privacy Laws & Business International Report*, 11-13
- 7 P. Palazzi 'Brazil enacts Data Privacy Law', (2018) 155 *PLBIR* 11.
- 8 Alfaro, Ferrer & Ramire 'Panama: Personal Data New Law' 21 November, 2018 [www.afra.com/2018/panama-ley-de-proteccion-de-datos-personales/](http://www.afra.com/2018/panama-ley-de-proteccion-de-datos-personales/)
- 9 Access Now [www.accessnow.org/panama-civil-society-demands-an-open-process-for-rushed-data-protection-bill/](http://www.accessnow.org/panama-civil-society-demands-an-open-process-for-rushed-data-protection-bill/)
- 10 'St. Kitts and Nevis' legislators pass Data Protection Bill 2018' *St Kitts & Nevis Observer*, 4 May 2018 [www.thestkittsnevisobserver.com/local-news/st-kitts-and-nevis-legislators-pass-data-protection-bill-2018/](http://www.thestkittsnevisobserver.com/local-news/st-kitts-and-nevis-legislators-pass-data-protection-bill-2018/)
- 11 'An "Ugly" New Data Protection Law in Lebanon' [docs.google.com/viewerng/viewer?url=http://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette\\_ENGLISH.pdf&hl=en\\_US](https://docs.google.com/viewerng/viewer?url=http://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette_ENGLISH.pdf&hl=en_US) A copy of the law is appended to the article.
- 12 Al Tamimi & Company 'Catching the wave: New Data Protection Law in Bahrain' [www.tamimi.com/law-update-articles/catching-the-wave-new-data-protection-law-in-bahrain/](http://www.tamimi.com/law-update-articles/catching-the-wave-new-data-protection-law-in-bahrain/)
- 13 Asim Jusic, quoted in (2018) 155 *PLBIR* 10.
- 14 Information, Communications and Media Act of Bhutan, 2018 [www.dit.gov.bt/information-communications-and-media-act-bhutan-2018](http://www.dit.gov.bt/information-communications-and-media-act-bhutan-2018)
- 15 G Greenleaf and S Livingston 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 *Privacy Laws & Business International Report*, 1-7
- 16 E-Commerce Law of the People's Republic of China (Standing Committee of the National People's Congress, 31 August 2018) Art 24 "Where e-business operators receive applications for inquiries, modification, or deletion of user information, they shall promptly make the inquiry, or modify or delete the user information, after identity verification" (Source: China Law Translate).
- 17 G. Greenleaf and S. Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law' (2017) 150 *Privacy Laws & Business International Report* 25-28.
- 18 For a very current report, see K. Needham 'Millions are on the move in China, and Big Data is watching' *Sydney Morning Herald*, 6 February 2019 [www.smh.com.au/world/asia/millions-are-on-the-move-in-china-and-big-data-is-watching-20190204-p50vlf.html](http://www.smh.com.au/world/asia/millions-are-on-the-move-in-china-and-big-data-is-watching-20190204-p50vlf.html)
- 19 The number of 'countries per region' is based, with modifications to accommodate my division into regions, on Internet World Stats, Country List [www.internetworldstats.com/list1.htm#geo](http://www.internetworldstats.com/list1.htm#geo) The total of 231 countries includes non-UN members, and sub-national regions with distinct top-level domains (such as Hong Kong or Jersey), and therefore is at least as extensive as the criteria I use for a 'country'. All such lists commence from slightly differing assumptions.
- 20 These include obligations to appoint DPOs, the age at which children can consent online, additional conditions for processing of sensitive data, and additional conditions for processing criminal information.
- 21 Linklaters 'Status of National Laws under the General Data Protection Regulation' Table, November 2018, gives a convenient summary of the factors in the previous footnote. Further details of many of the implementing laws can be found in issues of *Privacy Laws & Business International Report*.
- 22 This note draws on joint research with Prof. Bertil Cottier.
- 23 For a brief analysis, see Greenleaf and Cottier, above.
- 24 A. B. Nougères 'Uruguay moves towards the EU GDPR standard' (2018) 156 *PLBIR* 20.
- 25 In the Table of existing laws (not the Bills Table), these are shown by 'B(201x)' in the 'Latest' column, to show there is a reform Bill, and its year.
- 26 This is implied by the joint effect of GDPR arts. 45(3) and 45(9). otherwise they would have 'indefinite adequacy'.
- 27 See G. Greenleaf 'Global data privacy laws 2019: New eras for international standards' p.19 in this issue.

quacy status under the Directive, but who will need to have this status renewed under the GDPR within four years.<sup>26</sup> Some have not yet strengthened their laws for this purpose, but others –

Argentina; New Zealand; and Israel – have Bills in progress, which may or may not prove to be adequate. The clock appears to be ticking for all of them.

CONCLUSIONS

In 2017-18, the momentum toward stronger and more globally pervasive data privacy laws is the strongest it has been in any two-year period. This is seen primarily from the 10% increase of countries with data privacy laws to 132; the 28 or more additional countries planning to enact such laws; and the very important bills to strengthen existing laws in many countries, particularly in Asia. The move toward stronger standards within such laws is reflected not only by the GDPR adherence of EU member states, but also in the constant inclusion of many GDPR-like

principles in both new and revised laws outside the EU.

Exactly which new principles are being adopted most often, influenced by both the GDPR and the growing influence of Convention 108/108+,<sup>27</sup> requires further analysis. It is also as yet uncertain which *de facto* international standards will be established by ‘adequacy’ requirements under the GDPR.

Expansion and updating of data privacy laws means little unless they are enforced effectively, and the most important indicia of that is usually an active national data protection authority (DPA), including DPAs acting collectively.

INFORMATION

Valuable information and comments for this article have been received from Clarisse Giroit, David Banisar, Sophie Kwasny, Laura Linkomies and Jill Matthews. They are acknowledged with gratitude, but responsibility for all content remains with the author. Separate acknowledgments accompany the Tables. See also the article ‘New eras for international standards’ p.19 in this issue. The next issue of this International Report will include the final article in this series, ‘Data privacy authorities (DPAs) 2019’ analysing growth of the networks in which DPAs are involved.

## Second Annual Review confirms that EU-US Privacy Shield continues uninterrupted

The EU Commission’s review from December 2018 says that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the US. The report, issued on 19 December, states that the steps taken by the US authorities to implement the recommendations made by the Commission in last year’s report have improved the functioning of the framework.

There are still issues that could be improved, the Commission says. It expects the US authorities to nominate a permanent Ombudsperson by 28

February 2019 to replace the one that is currently acting. The Commission says that if the Ombudsperson position has not been filled on a permanent basis by that time, it will consider taking appropriate measures under the GDPR. However, similar warnings made previously have not been followed through.

The Trump Administration responded on 18 January saying that it plans to nominate DocuSign Chairman and former CEO Keith Krach as the permanent Ombudsperson.

More than 3,850 companies have now been certified to Privacy Shield. The improvements made include

compliance reviews. Out of the 100 companies that have been checked, 21 had issues that have now been solved. Additional compliance review procedures also include the analysis of Privacy Shield participants’ websites to ensure that links to privacy policies are correct, the report says. The Department of Commerce has put in place a system to identify false claims which prevents companies from claiming their compliance with the Privacy Shield, when they have not been certified.

- See [europa.eu/rapid/press-release\\_IP-18-6818\\_en.htm](http://europa.eu/rapid/press-release_IP-18-6818_en.htm)

## Mutual EU-Japan adequacy decision in force

The adequacy framework for the transfer of personal data between Japan and the European Union, the first on a mutual basis, was adopted and applied starting on 23 January 2019.

Commissioner Haruhi Kumazawa, Personal Information Protection Commission, Japan and EU Commissioner Věra Jourová welcome the adoption. With this mutual adequacy arrangement, Japan and the EU reaffirm their commitment to shared values in the field of privacy, and to strengthen their cooperation in shaping global standards based on a high level of protection of personal data, they say in a statement.

She continued, clearly referring to future adequacy negotiations with other countries: “This adequacy decision creates the world’s largest area of safe data flows. Europeans’ data will benefit from high privacy standards when their data is transferred to Japan. Our companies will also benefit from a privileged access to a 127 million consumers’ market. Investing in privacy pays off; this arrangement will serve as an example for future partnerships in this key area and help setting global standards.”

A joint review will be carried out after two years to assess the functioning of the framework. “This will cover

all aspects of the adequacy finding, including the application of the Supplementary Rules and the assurances for government access to data. The Representatives of [the] European Data Protection Board will participate in the review regarding access to data for law enforcement and national security purposes. Subsequently a review will take place at least every four years,” the EU Commission says.

- See [https://www.ppc.go.jp/en/about/roles/international/cooperation/2019\\_0123/](https://www.ppc.go.jp/en/about/roles/international/cooperation/2019_0123/) and [http://europa.eu/rapid/press-release\\_IP-19-421\\_en.htm](http://europa.eu/rapid/press-release_IP-19-421_en.htm)

# Global data privacy laws: New eras for international standards

**Graham Greenleaf** analyses the latest developments in global privacy laws.

In 2017-18 there have been major changes to some of the international agreements affecting privacy, in terms of both their contents and their parties. They are summarised in this article, and the countries affected are detailed in the accompanying Tables.

My survey of new and revised laws in 2017-18<sup>1</sup> (p.14) makes it clear that the EU's GDPR has established a new "global benchmark" for data privacy protection, to which non-EU countries are already aspiring to align their laws in very varying degrees. However, the GDPR coming fully into force on 25 May 2018 created a more concrete "international standard": those countries which wish to obtain or retain a finding by the European Commission that they "ensure an adequate level of protection" (GDPR art. 45) must satisfy the requirements of art. 45. As at the end of 2018, the first two assessments of new countries (Japan and Korea) had not been concluded.<sup>2</sup> However, the EU-Japan mutual adequacy decision was completed in January 2019. Re-assessments of countries already held adequate under the 1995 Directive had not commenced.<sup>3</sup>

## CONVENTION 108 & 108+: RATIFICATIONS AND ACCESSIONS

The "modernisation" of data protection Convention 108 was completed, by the parties to the existing Convention agreeing to a Protocol amending it, on 18 May 2018 (one week before the GDPR came fully into force). The new version (called "108+" to distinguish it) will not come into force for some years.<sup>4</sup> However, now that it is open for signature (since 10 October 2018), any new countries wishing to accede will have to accede to both the Protocol (i.e. to 108+) as well as to Convention 108. Argentina, Burkina Faso and Morocco, the three countries which had commenced but not completed the accession process, are still able to accede to 108 alone.<sup>5</sup> Twenty-five Parties, (see Tables) have now signed Convention

108+,<sup>6</sup> but none have yet ratified it. The signatories from outside the EU are Andorra, Norway, Iceland, the Russian Federation and Uruguay.

Since 2017 (and prior to these changes), three more countries outside Europe (Tunisia, Cape Verde and Mexico) became Parties to Convention 108, joining Uruguay, Senegal and Mauritius to bring the number of Parties to 53.

The UN Special Rapporteur on the Right to Privacy (SRP) has recommended that all UN member states should accede to Convention 108+ and implement its provisions in their domestic law, and where possible to implement additional GDPR principles, while leaving the door open to a broader international agreement at a later date.<sup>7</sup> The EU also endorses accession to Convention 108 by countries seeking a positive adequacy assessment (GDPR, recital 105).

## AFRICAN UNION CONVENTION: 11 SIGNATURES, THREE RATIFICATIONS

The African Union Convention on Cyber Security and Protection of Personal Data (2014) has relatively high data protection standards, and a potential membership of 55 African countries. It is the most significant data privacy Convention other than the increasingly global Convention 108. Two years ago it had eight signatories and one ratification (Senegal), but as of November 2018, it has 11 signatories<sup>8</sup> (of which Comoros, Ghana and Zambia are new), plus three ratifications (Guinea-Conakry, Mauritius and Senegal).<sup>9</sup> These last two are also Parties to Convention 108. Fifteen ratifications are required for it to enter into force, so it is likely that this will occur, given that there already fourteen signatories or ratifications. Nine of the 24 African countries with data privacy laws have at least signed the Convention.

With new laws in Niger and Guinea-Conakry, nine<sup>10</sup> of the 15 ECOWAS states in West Africa have enacted data

privacy laws to comply with their existing obligations under the ECOWAS Supplementary Act. The "ECOWAS laws" are the strongest data privacy laws in Africa.

## UN PRIVACY COMMITMENTS: MOST HAVE RATIFIED

Of the 11 new countries with data privacy laws, all except Bhutan and St Kitts & Nevis (both UN member states) have ratified the International Covenant on Civil and Political Rights, 1966 (ICCPR), Article 17 of which requires privacy protections.<sup>11</sup> The position is slightly less impressive concerning ratifications of the 1st Optional Protocol to the ICCPR, which allows individuals to make "communications" (complaints) to the UN Human Rights Committee, including concerning state failures to implement ICCPR Article 17.<sup>12</sup> There are no ratifications by St Kitts & Nevis and Bhutan, or by Lebanon or Bahrain. The position of the other 128 countries with data privacy laws is as set out in the 5th edition (2017) of this survey: by far the majority of countries with data privacy laws have also ratified both the ICCPR and the 1st Protocol, and therefore participate in the UN human rights system. However, a minority do not, an issue that the UN Special Rapporteur on the Right to Privacy could address.

## APEC CBPRs: NEGLIGIBLE OPERATION, DESPITE 'COMMITMENTS'

In 2017-18 Singapore, Australia and Taiwan ("Chinese Taipei" in APEC-speak) were approved to participate in the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System (CBPRs). APEC's Electronic Commerce Steering Group Joint Oversight Panel (ECESG-JOP) held that their laws met APEC requirements. Mexico (2014), Canada (2014), and Korea (2016) obtained approval earlier. If and when any of these six countries appoint

“Accountability Agents” (AAs), then companies in their jurisdictions can apply to be certified as CBPRs-compliant. Until then, “participation” in APEC CBPRs has no practical effect. None of these countries has yet appointed an AA. Canada called for applicants to be AAs in 2017.<sup>13</sup> It seems that some countries say they wish to participate in APEC CBPRs, and take preparatory steps, but then do not do so.

As at January 2019, only the US (24 companies certified since 2013<sup>14</sup>) and Japan (three companies certified since 2016<sup>15</sup>) have appointed AAs,<sup>16</sup> so after six years of operation, APEC CBPRs only involves a tiny number of US and Japanese companies. CBPRs is therefore of negligible practical significance as yet. The European Commission states in its Decision concerning Japan’s adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate.<sup>17</sup> This will further diminish the business case for CBPRs. On the other hand, APEC CBPRs has been recognised in the USMCA tripartite free trade agreement (see below; not yet in force).

**FTAs: POTENTIAL CLASHES COMMENCE**

In 2017-18 the previous Trans Pacific Partnership (TPP) was scrapped after President Trump refused US ratification, but it was then replaced by the 11 other parties (see the Tables) proceeding with the Comprehensive and Progressive TPP (CPTPP) which was largely the same in its provisions limiting data export limitations and data localisation. It came into force between its six ratifying parties (to date) on 30 December 2018.<sup>18</sup> The US-Mexico-Canada FTA has similar provisions but is not yet in force. The above provisions in these free trade agreements (FTAs) may be inconsistent with provisions in the laws of some of these countries (including provisions necessary for EU adequacy), and also with their other international obligations such as in Convention 108.<sup>19</sup> As parties to CPTPP, it is arguable that Japan, New Zealand and Canada may already have made commitments inconsistent with being considered adequate by the EU; and Mexico may have done similarly in relation to its commitments under Convention 108.

**CONCLUSIONS**

The steady expansion of Convention 108 beyond Europe is slowly making it apparent that it is the only viable global data privacy treaty, reinforced by its endorsement by both the EU’s institutions and GDPR, and by the UN SRP. Progress toward the African Union’s own treaty coming into force is gaining momentum but is far from complete. APEC’s CBPRs, despite ostensible participation, remains of negligible practical significance.

**INFORMATION**

Valuable information and comments for this article have been received from Clarisse Giroit, David Banisar, Sophie Kwasny, Laura Linkomies and Jill Matthews. They are acknowledged with gratitude, but responsibility for all content remains with the author. Separate acknowledgments accompany the Tables. See also the article ‘132 national laws, & many bills show European influences’ p.14 in this issue. The next issues of this International Report will include the final article in this series, ‘Data privacy authorities (DPAs) 2019’ analysing growth of the networks in which DPAs are involved.

**REFERENCES**

- 1 G. Greenleaf ‘Global data privacy laws 2019: 132 national laws, & many bills show GDPR influence’, in this issue.
- 2 See [ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\\_en](http://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)
- 3 See discussion of Bills relevant to such assessments in Greenleaf ‘Global data privacy laws 2019: 132 national laws...’.
- 4 For details see G. Greenleaf (2018) ‘Modernised’ data protection Convention 108+ and the GDPR’ 154 Privacy Laws & Business International Report 22-3
- 5 Greenleaf ‘Modernised’ data protection Convention 108+ and the GDPR’
- 6 Council of Europe Chart of signatures and ratifications of Treaty 223, as at 9 January 2019 [www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures)
- 7 United Nations General Assembly, seventy-third session Report of the Special Rapporteur on the right to privacy, 17 October 2018, para. 117(e).
- 8 Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia.
- 9 African Union Convention on Cyber Security and Personal Data Protection – Status List (as at 12 November 2018) [au.int/sites/default/files/treaties/29560-sl-african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_1.pdf](http://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf)
- 10 Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Guinea, Ivory Coast, Mali and Niger
- 11 International Covenant on Civil and Political Rights (signatures and ratifications) [treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=IV-4&chapter=4&clang=\\_en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en) (as at 4 January 2019).
- 12 ICCPR 1st Protocol, ratifications [treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=IV-5&chapter=4&clang=\\_en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-5&chapter=4&clang=_en) (as at 4 January 2019).
- 13 See Gazette [www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf](http://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf) at p. 242.
- 14 TrustAct APEC CBPR Certified Companies [www.trustarc.com/consumer-resources/trusted-directory/#apec-list](http://www.trustarc.com/consumer-resources/trusted-directory/#apec-list) as at 7 January 2019.
- 15 See JIPDEC’s APEC CBPRs Certified Companies list [english.jipdec.or.jp/protection\\_org/cbpr/list.html](http://english.jipdec.or.jp/protection_org/cbpr/list.html) (as at 7 January 2019).
- 16 APEC CBPRs Accountability Agents listing [cbprs.org/accountability-agents/](http://cbprs.org/accountability-agents/)
- 17 [European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [ec.europa.eu/info/sites/info/files/draft\\_a\\_adequacy\\_decision.pdf](http://ec.europa.eu/info/sites/info/files/draft_a_adequacy_decision.pdf)
- 18 Australia, Canada, Japan, Mexico, New Zealand and Singapore (with Vietnam to commence on 14 January 2019) – See DFAT Australia CPTPP site [dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx](http://dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx)
- 19 G. Greenleaf ‘Asia-Pacific free trade deals clash with GDPR and Convention 108’ (2018) 156 Privacy Laws & Business International Report, 22-24.

# New Zealand's Privacy Bill: Light at the end of the tunnel?

**Katrine Evans** of Hayman Lawyers explains the reforms that are in the pipeline.

It's been just over seven years since the New Zealand Law Commission published its recommendations to update New Zealand's Privacy Act, so that the legislation can deal better with some of our modern information challenges. The new Bill enacting many of those recommendations was finally introduced into Parliament in March 2018, and we are now waiting for the Select Committee report.

This article focuses on some of the important new features in the Bill, and what those features may mean for businesses.

## THE BILL IS MOSTLY BUSINESS AS USUAL

Often, with law reform, it's just as important to understand what hasn't changed, as to understand the new provisions in a Bill.

The Privacy Bill is a good example. At first sight, it isn't obvious how much is still essentially the same. The Bill looks different. It substantially restructures many existing provisions. It also often simplifies the wording, with the aim of making the legislation easier to use. Generally, this is useful – though, inevitably, a few confusions have crept in along the way, and the Select Committee will need to iron them out.

However, in practice, the Bill mostly re-enacts the existing law. In particular, the privacy principles and most core aspects of the Bill have proved flexible and practical enough to cope with the radical changes in our information environment since the Act was first passed in 1993. We're all going to have to get up to speed with the new section numbers and different ways of expressing existing concepts, but in most respects, we should find that things are largely business as usual.

## MANDATORY BREACH NOTIFICATION

The most obvious new feature of the Bill is the introduction of mandatory notification of breaches, both to the

Commissioner and, in many cases, to affected individuals.

Making notification mandatory (clauses 117-123 in the Bill) will mean that New Zealand law is more in line with requirements in many other jurisdictions. Affected individuals will receive advice that enables them to take steps to protect themselves. Agencies such as businesses may have greater incentives to invest in stronger privacy and security settings, to reduce the chances of suffering breaches that harm individuals, damage trust in the business and are expensive to fix.

However, many submissions to Select Committee have criticised the relatively low and uncertain threshold for notification. A notifiable breach, at the moment, is defined in clause 117 as "a privacy breach that has caused any of the types of harm listed in section 75(2)(b) to an affected individual or individuals, or there is a risk that it will do so." The types of harm referred to are those where the privacy claimant has to prove that there has been an "interference with privacy" under the Act: that is, some kind of actual loss (such as financial loss), loss of a benefit or an opportunity to do something, or significant emotional distress of some variety. While the connection in some ways seems logical, in practice, it is not always clear that the types of harm listed in section 75(2)(b) has actually occurred or may occur. Proving harm tends to be the subject of detailed evidence in privacy cases at Tribunal level. It is often inherently uncertain – so it does not operate as a clear threshold to decide whether notification is required. Also, all that is required is that there is a "risk" that the breach will cause harm – the likelihood of that risk eventuating, or the level of harm that it would cause if it did occur do not come into it. This level of uncertainty about the threshold will almost certainly lead to over-notification of breaches – particularly as failure to notify the Privacy Commissioner will be an offence, attracting a

potential fine of up to NZ\$10,000 (clause 122). In turn, this could frustrate the purpose of the legislation and lead to unnecessary compliance costs for agencies, annoyance for people receiving notices, and burdensome reporting for the Commissioner.

Instead, the majority of submitters have suggested that the threshold should be changed to require notification only of breaches that are at the serious end of the spectrum. The standard in the new Australian legislation is a commonly cited model. Raising the threshold would be more in line with the Law Commission's view of the utility of mandatory notification, and would avoid breach fatigue problems. It would also bring the New Zealand law more into line with the standard for notification elsewhere, which would make life simpler for businesses that operate across borders.

The weight of submissions is such that it seems more likely than not that the Select Committee will make significant changes to the notification provisions before referring the legislation back to Parliament. Exactly what those changes will be, though – and whether there will be a further round of consultation to test their workability – is a moot point.

## PROTECTION FOR INFORMATION THAT IS SENT OFFSHORE

Under the existing Act, the Commissioner can prohibit onward transfers of personal information that is sent to New Zealand from offshore. However, there is less protection for information that originates in New Zealand and that is then sent offshore – either by way of transfer to an offshore organisation, or for the purposes of storage or processing.

The provisions in the Bill (principle 11(3)-(6)) clarify the existing (but not always well understood) position that the agency in New Zealand remains responsible for the information wherever it happens to hold or process it

(clause 8). The changes to principle 11 will also prevent the agency from disclosing information to an overseas person unless:

- that overseas person is purely acting as an agent for the New Zealand entity (and so the New Zealand entity is still principally liable)
- the individual authorises the disclosure (the standard of authorisation is not clear, but there is a strong chance that it would have to take the form of express and informed consent)
- the overseas person is in a “prescribed” (that is, whitelisted) country, or
- the New Zealand entity believes the overseas person has to provide at least equivalent protection for the information as it would get in New Zealand (for instance through contracts).

These conditions for offshoring information are alternatives, not cumulative. This ensures that there are few barriers to using business solutions such as cloud computing, which is useful from a practical perspective. But it stops short of requiring businesses to perform due diligence, export only to whitelisted countries, or have model contractual clauses.

The fact that the New Zealand entity is still liable if something goes wrong with an overseas agent should serve to encourage businesses to engage several different layers of protection for the information (including

### NEW POWERS FOR THE COMMISSIONER

The Privacy Commissioner currently only has recommendatory powers – with a couple of minor exceptions (such as the ability to determine charges for access to information), he cannot make enforceable decisions. That is going to change in two important respects under the Bill.

First, the Commissioner will be able to make first instance, enforceable determinations on complaints about inadequate responses to subject access requests (clause 96). He will be able to determine that the agency (for instance a business) should have provided access, and direct the agency to provide the requested information, or specified aspects of it. The Commissioner can also determine how that access is to be provided.

The agency can appeal the determination to the Tribunal within 20 working days of receiving the determination (clause 110-111). If it does not appeal, but fails to comply with the determination, the requester can ask the Tribunal to enforce the determination (clause 109). Failure to comply with an access order without reasonable excuse is an offence, with a potential penalty of NZ\$10,000. This underscores the centrality of subject access rights in the New Zealand privacy landscape.

Secondly, the Commissioner will be able to issue notices requiring agencies to comply with aspects of the privacy principles where the Commissioner has found the agency to be in breach

respondent party in the litigation. Liability is strict – it’s not an excuse that breaching the notice (or breaching the Act) was unintentional or without malice (clause 131(5)(a)). If the agency ignores the compliance notice, the Commissioner will be able to get it enforced in the Tribunal. The only defence available to the agency would be that it had fully complied with the notice (clause 130) – a pure factual matter. It would not be able to turn a failure to respond to the notice into an appeal on the merits of the case.

The moral of the story for businesses therefore appears to be that the Commissioner will still have a strong dispute resolution focus – there are multiple references in the Bill to the fact that he has to use his best efforts to resolve matters informally and keep them out of a litigation environment. But if an agency is in breach and fails to settle, the Commissioner will be carrying a bigger stick. If he wields that stick, the business will need to act quickly to either comply or appeal. It’s a case of put up, or shut up.

The Commissioner’s powers in the Bill largely implement the recommendations of the Law Commission. Any changes are likely to be minor and for the purpose of clarifying the provisions, rather than more sweeping. So it’s probably a good time for businesses to review their practices and fix their most obvious problems before the Commissioner comes calling.

### WHAT’S NOT IN THE BILL

Unfortunately, what the Privacy Bill doesn’t do is to introduce further updates to cover issues that have emerged during that seven year hiatus since the Law Commission reported. It’s essentially a 2011 law. While that’s a great deal better than nothing, many submitters – including the Privacy Commissioner – have urged the Select Committee to take the opportunity to add provisions on issues such as data portability, automated processing and algorithms, and protecting people against being re-identified from supposedly anonymised data sources.

The reality is that it’s hard to get privacy reform onto the legislative agenda: if we don’t do it now, we might still be playing catch-up for a long time to come. As well as better protecting

---

## Adding these types of features would also more explicitly align the Bill with key aspects of the GDPR.

---

the matters listed), but they have the freedom to determine how they are going to manage that responsibility. The law will not expressly prohibit them from exporting the information in many instances (which means that the protections are relatively soft) – but the tenor of the legislation probably means that failures to take obvious steps to protect the information will be particularly strongly frowned upon if something goes wrong.

(clause 124- 132). The Commissioner will be able to specify what the agency needs to do to fix the problem. This compliance notice power applies either after investigation of a complaint, or after an own motion investigation by the Commissioner.

Again, the agency has a right of appeal to the Tribunal (though it has to exercise it within 15 working days: clause 131(2)), and in that case the Commissioner himself would be the

people's privacy, adding these types of features would also more explicitly align the Bill with key aspects of the GDPR, and would therefore help to ensure that the law here remains "adequate" - a subject that was on the minds of many submitters to the Select Committee.

Whether the Select Committee will take the opportunity to update the law for the 2018/2019 environment is uncertain. If it does, many people hope that there will be another short round of consultation to make sure that the

way in which the proposals are drafted is manageable and proportionate. For instance it will be important to make sure that any data portability right is framed in a way that is workable in practice. As with breach notification, the drafting should also be tailored to fit reasonably well with similar overseas requirements, in order to reduce the compliance burden for those who operate in the transborder business world.

So currently, New Zealand is

playing a waiting game, pending the Select Committee report back on the legislation (currently listed as due on 13 March 2019). Further significant changes may be possible. But at least there is light at the end of the tunnel.

#### AUTHOR

Author: Katrine Evans is a Senior Associate at Hayman Lawyers, New Zealand.  
Email: [k.evans@haymanlawyers.co.nz](mailto:k.evans@haymanlawyers.co.nz)

## Facebook's conduct "exploitative abuse"

Germany's *Bundeskartellamt*, the national competition regulator, says that the extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of a dominant position, and it is imposing restrictions on Facebook's processing of user data.

The authority announced on 7 February its decision that Facebook has no effective justification for collecting data from other company-owned services, like WhatsApp, Instagram, and Facebook Business Tools or for assigning these data to the Facebook user accounts.

Andreas Mundt, President of the *Bundeskartellamt* said: "As a dominant company Facebook is subject to special obligations under competition law. In the operation of its business model the company must take into account that Facebook users practically cannot switch to other social networks. In view of Facebook's superior market

power, an obligatory tick on the box to agree to the company's terms of use is not an adequate basis for such intensive data processing. The only choice the user has is either to accept the comprehensive combination of data or to refrain from using the social network. In such a difficult situation the user's choice cannot be referred to as voluntary consent."

Facebook's terms of service and the manner and extent to which it collects and uses data are in violation of the European data protection rules to the detriment of users, the *Bundeskartellamt* says. As there is an interface between competition law and data protection law, it has been in close cooperation with EU data protection authorities.

In the authority's assessment, Facebook's conduct represents above all a so-called exploitative abuse. Dominant companies may not use exploitative practices to the detriment of the

opposite side of the market, i.e. in this case the consumers who use Facebook.

Andreas Mundt: "Today data are a decisive factor in competition. In the case of Facebook they are the essential factor for establishing the company's dominant position. On the one hand there is a service provided to users free of charge. On the other hand, the attractiveness and value of the advertising spaces increase with the amount and detail of user data. It is therefore precisely in the area of data collection and data use where Facebook, as a dominant company, must comply with the rules and laws applicable in Germany and Europe."

Facebook has one month to appeal the decision to the Düsseldorf Higher Regional Court.

• See [www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2019/07\\_02\\_2019\\_Facebook.html](http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2019/07_02_2019_Facebook.html)



### events diary

#### Integrating Ireland's data protection law into everyday business

8 and 9 May 2019

McCann FitzGerald, Dublin

This one-and-a-half day PL&B conference aims to help you work constructively with Ireland's Data Protection Commission (DPC). Speakers include Helen Dixon, Data Protection Commissioner, Ireland; Joanne Neary, Solicitor, DPC, Ireland; and Tony Delaney, Head, Special Investigations Unit, DPC, Ireland.

#### Key issues covered:

- Demonstrating GDPR and DP Act compliance
- Handling complex access requests
- Enforcement and defending your reputation
- International transfers of personal data.

See [www.privacylaws.com/ireland](http://www.privacylaws.com/ireland)

#### GDPR's influence ripples around the world PL&B 32nd Annual International Conference

1-3 July 2019

St John's College, Cambridge

DPA speakers include Andrea Jelinek, Chair, European Data Protection Board, in her first conference presentation in the United Kingdom; Elizabeth Denham,

UK Information Commissioner; Eduardo Bertoni, Director, Data Protection Authority, Argentina; and Daniel Therrien, Privacy Commissioner of Canada.

This residential conference is an opportunity to mingle with DPAs, companies, and lawyers from around the world. See the 45 confirmed speakers from 16 jurisdictions and their sessions at [www.privacylaws.com/ac](http://www.privacylaws.com/ac)

#### Asian Privacy Laws

30 October 2019

Linklaters, London

Speakers: Professor Graham Greenleaf, Asia-Pacific Editor, *Privacy Laws & Business* and Adrian Fisher, Partner, Linklaters, Singapore.

See [www.privacylaws.com/asia](http://www.privacylaws.com/asia)

# Data protection bills in Kenya, Uganda, Tanzania and Zambia

Emma Anderson provides a data protection update for these four African countries.

With the continuous advancement of technological innovation comes increased cross-border flows of personal data. According to Deloitte, e-commerce has brought with it a new era of international trade, specifically in the African continent, where business growth and foreign direct investment have brought forth many new opportunities<sup>1</sup>. Due to business in the African continent expanding, organisations need to understand the African personal data protection landscape<sup>2</sup>. This article focuses on Kenya, Uganda, Tanzania, and Zambia.

## KENYA

Over the past decade, Kenya's technology and communication sector has increased rapidly, yet without a comprehensive data protection framework in place. In 2009, 2012, and 2013 draft data protection bills were produced but have since lapsed. The Minister of Information, Communication and Technology, Joe Mucheru, stated that Kenya "cannot ignore the fact that we have become a digital economy and therefore we need to have all the protections that are needed."<sup>3</sup> Furthermore, Kenya has signed the African Union Convention on Cyber Security and Personal Data Protection<sup>4</sup>, which calls for member states to adopt legal frameworks for data privacy and cybersecurity.

Currently the main national laws that regulate the collection and use of personal data in Kenya include the:

- Constitution of Kenya 2010 (Article 31 in particular),
- The Information and Communication Act 2009 (specifically Article 31, 83, and 93),
- The Information and Communication (Consumer Protection) Regulations 2010 (Section 15.1),
- The Consumer Protection Act 46 of 2012, and
- The Access to Information Act 31 of 2016.

Medical data is governed by:

- The HIV Prevention and Control Act 14 of 2006,
- The Public Health Act Cap 202,
- The Health Information Systems Policy 2009,
- The Kenya National eHealth Policy 2016 – 2030, and
- The Health Act 21 of 2017.

Together these acts and policies have controlled some aspects of data protection. However, there is no general protection of personal data privacy in common law.

**Draft Bill:** In the summer of 2018, The Ministry of Information, Communications and Technology (ICT Ministry) released the draft Data Protection Bill 2018<sup>5</sup>. The 2018 Data Protection Bill seeks to elaborate on Article 31 C and D of the Constitution of Kenya, 2010<sup>6</sup>. The Bill specifies how data can be stored and shared.

**Similarities to the GDPR:** The Bill borrows from and reflects the principles of data protection envisioned in the GDPR. The Bill will require controllers and processors to abide by principles of meaningful user consent, collection limitation, purpose limitation, data minimisation, and data security. Furthermore, the Bill establishes data subject rights including the right to access and to be informed of the use of their data, rights to rectification, and rights to object to processing of their personal data. The Bill establishes territorial scope, covering entities both resident in Kenya and those which are not (provided that the personal data processed is of data subjects in Kenya). The Bill sets out to establish the Office of the Data Protection Commissioner which Kenya does not currently have. This Bill will also require data processors and controllers to register with the Data Protection Commissioner where they will receive a Registration Certificate that is valid for three years. The Bill also establishes data-related offences and details penalties for not adhering to the law.

**Differences to the GDPR:** There are some provisions in the GDPR that differ or are non-existent in Kenya's Draft Bill. Including:

- Consent: This Bill leaves room for interpretation when it comes to consent. Kenya's Bill is not explicit about consent needing to be freely given, as it is in the GDPR. Also, there is no requirement to keep a record of consent. The GDPR (Article 7.1) advises consent records should be kept as they may be used for evidence if challenged.
- The Bill could also be clearer in the restrictions imposed on data controllers and processors around purpose limitation, collection limitation, and data retention limitation.
- Furthermore, the Bill does not contain the principle of data minimisation as an obligation which is in contrast to the GDPR (Article 5.1).

This bill appears to be a step in the right direction in terms of data protection. The bill is being reviewed and refined before presentation to parliament for enactment.

## UGANDA

Similarly, Uganda has a draft bill for data protection, The Data Protection and Privacy Bill 2015 (Memorandum 21 Feb 2016)<sup>7</sup>, which has yet to be passed. Currently, the existing legal framework that supports aspects of data protection in Uganda include the:

- The Constitution of the Republic of Uganda—Article 27,
- The Access to Information Act 2005 (Act No 6 of 2005)—Section 26,
- The Computer Misuse Act 2011 (Act No 2 of 2011)- Section 18,
- The Electronic Signatures Act 2011 (Act No 7 of 2011)—Section 81,
- The Uganda Communications Act 2013 (Act No 1 of 2013).

The Draft Data Protection and Privacy Bill 2015 will consolidate existing legislation and provide more complete data protection. The Bill aims to

protect the privacy of the individual and their personal data through the regulation of the collection and processing of personal information. This Bill was influenced by Data Protection Directive (1995), the predecessor to the GDPR.

**Similarities to the GDPR:** Uganda's Bill is similar to the GDPR in that it sets out the types of personal data that can be collected/processed, the data subjects rights (Part 5 of the Data Protection and Privacy Bill 2015), offers protection of privacy (Article 6), defines the lawful basis for processing (Article 8), explains consent and how it should be obtained (Article 9), has a section on data minimisation (Article 10), contains rules on ensuring the quality of information and data correction (Article 11 and 12), provides data retention guidelines (Article 14), and defines data security (Article 16-19). Furthermore, the Bill places the National Information Technology Authority of Uganda in charge of registering every person, institution or public body that collects or processes personal data, in the data protection register (Article 25).

**Differences to the GDPR:** The Bill differs from the GDPR in that:

- It does not clearly establish the territorial scope of application of the law like the GDPR does (GDPR Article 3). The Bill does not clearly explain if the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in Uganda, regardless of whether the processing takes place in Uganda or not.
- Furthermore, Uganda's Bill (in Article 4) does not clearly define the conditions for 'consent.' The conditions for the consent in the GDPR ensure consent is meaningful, informed and freely given.

Comments on this Bill are being submitted to the ICT Committee of Parliament with the hope that the Bill will pass in the coming year.

#### TANZANIA

Currently, Tanzania does not have a data protection law. However, the Government has been drafting a Bill (since 2009) to be tabled before Parliament for discussion. It is not yet

clear when the Bill will be published. This future law will consolidate people's rights when it comes to data protection<sup>8</sup>. The law will also put into place procedures and guidelines on protecting personal data, as well as solidifying appropriate procedures for gathering personal information<sup>9</sup>.

Despite not having a specific law or bill for data protection, Tanzania has other legislation that is currently used as proxy indicators to safeguard personal data including:

- The Constitution of the United Republic of Tanzania—Article 16(1-2) stating the right to privacy,
- The Electronic and Postal Communications Act of 2010—Section 98 and 99,
- The Electronic and Postal Communication (Consumer protection) Regulations (GN. No. 427 of 2011) - Section 6,
- The Cybercrimes Act 2015—Section 7,
- The Registration and Identification of Persons Act (CAP 36 R:E 2012),
- The Records and Archives Management Act (No. 3 of 2002)—Section 16,
- Access to Information Act (No 9 of 2016)—Section 6.1 and Section 22,
- The Statistics Act (No 9 of 2015)—Section 25.1, and
- The Electronic and Postal Communications (Online Content) regulations 2018—Regulation 11.

Until the future data protection bill is written and passed, the existing legislation above should be followed by data collecting and processing entities.

#### ZAMBIA

Currently Zambia does not have data protection legislation but has drafted The Data Protection (Repeal) Bill 2018. According to the World Bank, there is limited data protection provisions in Zambia and there have not been comprehensive data protection laws to safeguard the personal information of consumers<sup>10</sup>. On 29 January 2016, Zambia signed the African Union Convention on Cyber Security and Personal Data Protection. By signing this agreement, Member States are required to develop legislation to combat violations of privacy that may be generated by the collection,

#### REFERENCES

- 1 Deloitte (2017) 'Privacy is Paramount: Personal Data Protection in Africa'. Available at: [www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za\\_Privacy\\_is\\_Paramount-Personal\\_Data\\_Protection\\_in\\_Africa.pdf](http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf)
- 2 African countries that have data protection laws in place: Morocco, Tunisia, Western Sahara, Senegal, Mali, Cape Verde Islands, Burkina Faso, Cote d'Ivoire, Ghana, Benin, Gabon, Angola, Rwanda, Seychelles, Comoros, Madagascar, South Africa, Lesotho, and Mauritius. [www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za\\_Privacy\\_is\\_Paramount-Personal\\_Data\\_Protection\\_in\\_Africa.pdf](http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf)
- 3 Miriri, D. (2018) 'Kenya to Publish Draft Data Protection Bill This Month-Minister'. Available at: [af.reuters.com/article/kenyaNews/idAF-L8N1TD3EI](http://af.reuters.com/article/kenyaNews/idAF-L8N1TD3EI)
- 4 Available here: [au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](http://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)
- 5 Available here: [www.parliament.go.ke/sites/default/files/2017-05/Data\\_Protection\\_Bill\\_2018.pdf](http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf)
- 6 Article 31 refers to Privacy. It states: 'Every person has the right to privacy, which includes the right not to have—(c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed.'
- 7 Available here: [parliamentwatch.ug/wp-content/uploads/2016/10/Data-Protection-and-Privacy-Bill-2015.pdf](http://parliamentwatch.ug/wp-content/uploads/2016/10/Data-Protection-and-Privacy-Bill-2015.pdf)
- 8 Domasa, S (2017) 'Tanzania: Personal Data Protection Law on Horizon'. Available at: [allafrica.com/stories/201712210571.html](http://allafrica.com/stories/201712210571.html)
- 9 *Ibid.*
- 10 The World Bank (2012) 'Diagnostic Review of Consumer Protection and Financial Literacy'. Available at: [responsiblefinance.worldbank.org/~media/GIAWB/FL/Documents/Diagnostic-Reviews/Zambia-CPFL-Vol-I.pdf](http://responsiblefinance.worldbank.org/~media/GIAWB/FL/Documents/Diagnostic-Reviews/Zambia-CPFL-Vol-I.pdf)
- 11 Available here: [www.zicta.zm/Downloads/The%20Acts%20and%20SIs/ICT%20Acts/ect\\_act\\_2009.pdf](http://www.zicta.zm/Downloads/The%20Acts%20and%20SIs/ICT%20Acts/ect_act_2009.pdf)

processing, transmission, storage, and use of personal information. The Data Protection (Repeal) Bill 2018 was drafted as a result of signing the agreement, yet little has been said about the bill.

This Bill's aim is to repeal and replace the Electronic Communications and Transactions (ECT) Act No. 21 of 2009<sup>11</sup>. The intention of the ECT is to certify that individuals are consulted when it comes to the collection of personal information and to ensure that their information is protected. However, the ECT contains

significant gaps in terms of data protection as it is designed specifically for the consumer and business sector rather than the free movement of personal data more generally. The Data Protection (Repeal) Bill 2018 is waiting to be passed by Parliament.

**CONCLUSION**

By looking at these four countries, it is clear that they are working towards passing data protection bills yet this appears to be a lengthy process. However, it is also important to recognize that even if there are no

specific Data Protection Acts, there are often other pieces of legislation that regulate aspects of the collection and use of personal data.

**AUTHOR**

Emma Anderson is a consultant for NGOs and a recent graduate of The University of Oxford with an MPhil in Medical Anthropology.

## Singapore's Privacy Commission issues large fines for non-compliance

In a landmark decision, Singapore's Personal Data Protection Commission (PDPC) issued on 15 January the highest fines it has ever imposed to date in the SingHealth breach case - aka "the worst breach of personal data in Singapore's history" perpetrated by "a skilled and sophisticated threat actor", Clarisse Girot of the Asian Business Law Institute (ABLI), reports. It involved "the personal data of some 1.5 million patients and the outpatient prescription records of nearly 160,000 patients .... exfiltrated in a cyber attack."

Financial penalties of \$750,000 and \$250,000 were imposed on Integrated Health Information Systems (IHIS) and SingHealth respectively for breaching their security obligations under the Singapore Data Protection Act.

From a legal point of view, the decision is interesting in several respects: PDPC provides details of the breach of their data security obligations by IHIS and SingHealth with a great level of detail, by referring to its own growing set of precedents as well as to guidance issued by the Privacy Commissioners

of Hong Kong and Canada. The decision also carefully qualifies the status of IHIS as a "data intermediary" under the Personal Data Protection Act and weighs aggravating and mitigating factors to set the level of the respective fines, Girot says.

- See [bit.ly/2tqbFh6](http://bit.ly/2tqbFh6) and [www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS--150119.pdf](http://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS--150119.pdf)

## Ireland advises on Brexit 'no deal' implications

Ireland's Data Protection Commission (DPC) on 8 February, published its advice that after 29 March, the UK will become a third country in terms of international data transfers. In the event of a 'no deal' UK exit from the EU, organisations in Ireland will require a transfer mechanism to be in place such as standard contractual clauses.

The DPC states that the next steps to consider for organisations transferring data to the UK, including Northern Ireland, are:

Map the personal data being transferred to the UK currently.

Determine if the transfers will need to continue beyond 30 March 2019.

If this is the case, then assess the

various transfer mechanisms to decide which one best suits the situation and work towards having it in place before 30 March 2019.

- See [www.dataprotection.ie/en/news-media/latest-news/dpc-issues-important-message-personal-data-transfers-and-uk-event-no-deal](http://www.dataprotection.ie/en/news-media/latest-news/dpc-issues-important-message-personal-data-transfers-and-uk-event-no-deal)

## EDPB adopts more DPIA lists

The European Data Protection Board (EDPB) adopted opinions on the Data Protection Impact Assessment (DPIA) lists submitted by Liechtenstein and Norway in its January plenary. A DPIA is a process to help identify and mitigate data protection risks that could affect the rights and freedoms of individuals.

While in general the data controller needs to assess if a DPIA is required before engaging in the processing activity, national supervisory authorities have compiled lists of the kind of processing operations which are subject to the requirement for a Data Protection Impact Assessment. The board adopted

22 opinions during the September 2018 plenary, and four at the December 2018 plenary. Although the board aims at consistency, there are some national variations.

- See [edpb.europa.eu/our-work-tools/consistency-findings/opinions\\_en](http://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en)

## EU Advocate General: Right to be Forgotten is limited to EU

The Advocate General of the EU's Court of Justice of the European Union (CJEU) says that the Right to be Forgotten should only apply within the EU. The EU Charter's right to data protection must be balanced against other Charter rights, such as the right of access to information. These rights must be applied with a territorial link to the EU, and cannot be broadly interpreted to apply across the whole world, Covington LLP reports.

The Advocate General, Maciej Szpunar, emphasizes that EU regulators cannot reasonably be expected to make the balancing test for the entire world. Szpunar released his opinion in January

regarding a 2016 enforcement action carried out by the French Supervisory Authority (CNIL) against Google. In that case, the CNIL ordered Google to de-reference links to webpages containing personal data. According to the CNIL, the de-referencing had to be effective worldwide. Google challenged the CNIL's decision before the French administrative court, which then referred this matter to the CJEU.

Spuznar is opposing the CNIL's view. While a worldwide obligation to de-reference is not desirable, Spuznar does believe that Google should be required to make every effort to de-reference the relevant links across the EU

(and not just in France). This includes by means of "geo-blocking", irrespective of the search engine domain used – for example, a user of Google.com, Google.fr or Google.de should not see the relevant links if it can be established that the user is in the EU (for example, on the basis of the user's IP address).

The opinion of the Advocate General will now be considered by the CJEU. The CJEU often follows the general analysis of the Advocate General.

- See [www.insideprivacy.com/data-privacy/eu-advocate-general-right-to-be-forgotten-is-limited-to-eu/](http://www.insideprivacy.com/data-privacy/eu-advocate-general-right-to-be-forgotten-is-limited-to-eu/)

## Netherlands doctor has 'Right to be Forgotten', says Amsterdam court

A Dutch surgeon has won a Right to be Forgotten case which concerned Google's listings on doctors' fitness to practise.

The surgeon had been formally disciplined for her medical negligence, but after an appeal, this was changed to a conditional suspension under which she was allowed to continue to practise. She complained to the Data Protection Authority in the Netherlands that her

name continued to be present on Google's link to an unofficial blacklist.

The DPA initially did not support the complaint based on the fact that the surgeon was still on probation and the information remained relevant. However, the district court of Amsterdam subsequently ruled the surgeon had "an interest in not indicating that every time someone enters their full name in Google's search engine, (almost)

immediately the mention of her name appears on the 'blacklist of doctors', and this importance adds more weight than the public's interest in finding this information in this way".

- See [www.theguardian.com/technology/2019/jan/21/dutch-surgeon-wins-landmark-right-to-be-forgotten-case-google](http://www.theguardian.com/technology/2019/jan/21/dutch-surgeon-wins-landmark-right-to-be-forgotten-case-google)

## EDPB advises on Brexit implications for data transfers and BCRs

In the event of a no-deal Brexit, the UK ICO would no longer be able to approve Binding Corporate Rules (BCRs) in cooperation with the other European Economic Area (EEA) DPAs. The European Data Protection Board (EDPB) advises that current BCR holders need to identify the new BCR Lead Supervisory Authority. Organisations wishing to make a BCR application, if headquartered in the UK, need to identify the most appropriate BCR Lead Supervisory Authority in an EU Member State.

Companies whose BCRs are at the review stage by the ICO also need to identify a new BCR Lead Supervisory Authority. The new BCR Lead Supervisory Authority will take over the application and formally initiate a new procedure at the time of a no deal Brexit.

If a draft ICO decision for approving BCRs is pending before the EDPB at the time of a no-deal Brexit, the company needs to identify a new BCR Lead Supervisory Authority.

With regards to international data

transfers from the EEA to the UK, the Board lists all the available mechanisms, such as standard contractual clauses. According to the UK government, data transfers from the UK to the EEA will continue uninterrupted in the event of a no-deal Brexit.

- See [edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexite\\_en.pdf](http://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexite_en.pdf)  
[edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexite\\_en.pdf](http://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexite_en.pdf)

# Join the Privacy Laws & Business community

## Six issues published annually

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

Stay informed of data protection legislative developments in 125+ 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 tribunal 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.

### Included in your subscription:

#### 1. Online search functionality

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.

#### 2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

#### 3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

#### 4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

#### 5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

#### 6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

#### 7. Helpline Enquiry Service

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

**To Subscribe: [www.privacylaws.com/subscribe](http://www.privacylaws.com/subscribe)**

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

## Subscription Fees

### Single User Access

*International Reports* £560 + VAT\*

*UK Reports* £450 + VAT\*

*UK & International Reports* £900 + VAT\*

\* VAT only applies to UK based subscribers

### Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

### Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

### International Postage (outside UK):

Individual International or UK Edition

Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions

Rest of Europe = £50, Outside Europe = £70

## Satisfaction Guarantee

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

*Privacy Laws & Business* also publishes the United Kingdom Report.

[www.privacylaws.com/UK](http://www.privacylaws.com/UK)