ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Sweden's new data protection regime supplements the GDPR

Maria Holmström Mellberg of Cirio Law firm gives an overview of how GDPR provisions have been transposed in Sweden

Sweden's new data protection regime consists of a GDPR-style Data Protection Act, and adjustments to many sectoral laws. The Data Protection Act of 2018 is the third act on data protection since the world's first national data protection law, Sweden's Data Act, came into force in 1973. The new Data Protection Act makes adjustments to the Public Access to Information and Secrecy Act[1] and repeals the previous Data Protection Act[2], which in turn replaced the Data Act of 1973[3].

By May 2018, some 20 commissions of inquiry[4] had been preparing

Continued on p.3

Germany: Facebook's data collection is market abuse

The *Bundeskartellamt's* decision may clash with the One Stop Shop and raises questions about the interaction of competition and DP law. By **Sophie Lawrance** and **Matthew Hunt** of Bristows LLP.

On 7 February 2019, the *Bundeskartellamt* (the federal competition regulatory authority in Germany) completed an investigation into Facebook that had taken almost three years. Unusually for a competition inquiry, this investigation focused centrally on Facebook's data collection practices, and on the relationship between compliance with data

Continued on p.5

Issue 158 **April 2019**

INTERNATIONAL report

ISSUE NO 158 APRIL 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
Maria Holmström Mellberg
Cirio Law, Sweden

Sophie Lawrance and Matthew Hunt
Bristows LLP, UK

Elzbieta Slazyk
Poland

Morgane Christiane and Giorgia Vulcano
Deloitte Consulting, Belgium

Goran Radošević, Sanja Spasenović, and Milica Filipović
Karanovic & Partners, Serbia

Dessislava Fessenko
Kinstellar, Bulgaria

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

comment

Busy times for EU DPAs

As we are approaching the first birthday of the EU GDPR, EU DPAs report a hugely increased workload. Nine months after the GDPR's full application, the members of the European Data Protection Board (EDPB) said that the GDPR cooperation and consistency mechanism is working quite well in practice.

The DPAs said that they make daily efforts to facilitate this cooperation, and meet monthly in plenary sessions, as well as in several subgroups. Six final One-Stop-Shop cases have been dealt with under the cooperation mechanism. The DPAs say that "there is still work to be done at the EDPB level to further streamline the procedure to make the system even more efficient".

This close cooperation means an extra workload, and a strain on resources. Most DPAs have managed to recruit many more staff, for example Ireland's DPA, which has received several cross-border complaints (p.7). Join us in Dublin to learn at *PL&B's* conference on 8-9 May more about Ireland's law and how it is enforced (p.7).

But the EDPB is by no means the only DPA cooperation mechanism. In this issue, Professor Greenleaf reports on the DPA networks around the world (p.11).

This issue reports on many legislative developments: read about Sweden's GDPR-style new data protection law and the various changes to sectoral laws (p.1), Nigeria's new law (p.23), Bulgaria's GDPR implementation (p.10) and Serbia's new law (p.25). Also, in Poland, changes to sectoral laws have been adopted (p.18) and the DPA has imposed a large fine (p.19).

Our correspondents analyse Facebook's situation regarding its data collection, and its exposure to both data protection and competition law (p.1), and how to pre-plan for data breaches and respond with suitable action (p.14).

In the UK, Brexit uncertainty continues, but several friendly jurisdictions have announced that they will treat the UK as an adequate destination for data flows to the UK after it exits the EU (p.8).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

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

Sweden... from p.1

new or updated complementing legislation to form the basis of the Government bills presented to the Parliament during 2018, most of them to be enforceable on 25 May itself.

As mentioned, the main Act supplementing the GDPR is the Data Protection Act[5] (the Act or the new Data Protection Act). The new Data Protection Act includes supplementary provisions to the GDPR. Alongside the Data Protection Act a fairly large number of adjustments to existing laws came into force on 25 May, or a later point during 2018, based on the work carried out by the commissions mentioned above.

During the preparatory work and consultations, some stakeholders stressed that a complete overview of all the supporting acts on public sector data registers (Register Ordinances) should be conducted, since the Register Ordinances are many and diverse and based on the conditions laid out by the Data Act of 1973. Others commented that the Government was not taking a clear stand on whether to expand or reduce the possibilities for processing of personal data beyond the clear requirements from the GDPR. The Government stated that the time available was too limited to allow for a more expansive overhaul of the legislative framework. The government noted that this does not exclude that such a review might be conducted in the future. From a practical perspective, it should be noted that this implies that we now have little insight into how the large number of Register Ordinances will be interpreted under the GDPR and the new Data Act.

The Swedish Data Protection Board (*Datainspektionen*) was, during 2018, given an additional task to facilitate industry's adaptation to the GDPR to ensure that Swedish companies do not lose momentum in their digitalisation efforts in parallel with maintaining a good level of data protection.[6]

The new Data Protection Act

The new Data Protection Act is the main Act supplementing the GDPR. It is a fairly short act containing provisions that complement the GDPR. This has been a priority for the Swedish government. Let us now have a look at some of the chapters to get a good overview of the structure and content of the new Data Protection Act.

Chapter 1: Initial provisions: The first chapter regulates primarily matters in relation to the GDPR's applicability in general. For example, it is stated that the GDPR shall also apply to processing in connection with activities outside EU-law and also some exceptions in relation to defence and police-related matters. The territorial scope is clarified, for example, it is stated that the Act applies to all children residing in Sweden regardless of the location of the controller or processor. Provisions in the Act are subsidiary to provisions in other Swedish Acts, which opens the possibility of conflict with special purpose laws (mainly used for processing by public authorities). It is further clarified that the GDPR and the Act shall not be applied when they violate Swedish constitutional acts. Also, certain sections of the GDPR and the Act shall not apply for processing for journalistic purposes and for academic, artistic or literary creation. Finally, the Act imposes an obligation of confidentiality on Data Protection Officers in respect of information obtained during the performance their duties.

> The Act applies to all children residing in Sweden regardless of the location of the controller or processor.

Chapter 2: Legal basis for processing of personal data: Chapter 2 clarifies important matters in relation to the legal bases for processing in Article 6 of the GDPR, specifically in relation to 6.1 c and e. Children must be at least 13 years old to be able to give consent to the processing of personal data in connection with their use of information society services, such as social media.

Chapter 3: Special categories of personal data: The 11 sections of Chapter 3 regulate matters related to processing of special categories of personal data in Article 9 of the GDPR. It clarifies the requirements in relation to employment laws, social security and social protection laws. The clarifications relate, for example, to collective agreements and processing for statistical purposes.

Regarding processing of data relating to criminal convictions (Article 10), the preparatory work for the Bill mentioned the potential loosening of the wording of the GDPR. The government pointed to the possibility of the relevant authority issuing ordinances instead of case-based permissions, for example regarding the processing of personal data in relation to international sanctions regimes. This might lead to a loosening of the current fairly strict view in Sweden regarding processing of personal data relating to criminal convictions and offences.

The processing of personal identification numbers without consent continues to be lawful in Sweden on condition that it is clearly justified in relation to the purpose of the processing, for example, secure identification. The government is authorized to issue further regulations.

Chapter 4: Limitations: This chapter contains limitations in relation to processing of personal data for archiving and statistical purposes.

Chapter 5: Limitations as to certain rights and obligations: This chapter contains some limitations and exceptions to the information rights of the data subjects.

Chapter 6: Supervisory authority handling and decisions: Chapter 6 concerns the mandate of the Swedish Data Protection Authority (*Datainspektionen*) and administrative fines. Administrative fines can be issued to both private sector companies and public authorities.

Chapter 7: Compensation and appeal: This chapter contains provisions in relation to compensation and procedural aspects in relation to appeal.

Entry into force: These provisions were enforceable as of 25 May 2018.

Other supplementing legislation

Adjustments in the areas of enterprise, innovation and credit information: Adjustments have been made to real estate, company, transportation and intellectual property laws. The adjustments include exceptions from the GDPR to ensure that the important registers can be retained despite, for example, by imposing a limitation on the data subjects' right to limit processing.

Adjustments have been made to the Credit Information Act[7] and the Debt Recovery Act[8]. The Credit Information Act is adapted to the GDPR in relation to the requirements on data processing and the information to the data subject. The processing of genetic data, biometric data to identify an individual and data about sexual preferences are prohibited when carrying out credit information activities. When credit information is disclosed, the data subject is entitled to information about, among other things, the source of the information, for how long it will be stored, and the possibility to lodge complaints with the Data Protection Authority. The actual right for a physical person to have access to the personal data about him or her is regulated by the GDPR (and not the Credit Information Act). As to the Debt Recovery Act, minor adjustments were made. The GDPR and the new Data Protection Act govern the processing of personal data in credit and debt activities.

Entry into force: The adjustments were enforceable as of 25 May 2018.

Laws for the financial sector: Most of the adjustments in financial-sector laws (i.e. among other Banking and Credit, Payments, Securities Markets, Insurance as well as Anti Money Laundering and Terrorist Financing laws) imply that references to the previous Data Protection Act are removed. Explicit references to the GDPR are few and in general no new explicit references to the GDPR or the new Data Protection Act are made.

Noteworthy requirements in this legal area are requirements related to storing personal data (the right to be forgotten), the obligations on regulated entities to have reporting systems in place to enable whistle-blowing, and in addition transaction monitoring to prevent financial crimes.

Entry into force: The adjustments were enforceable as of 25 May 2018.

New Act on camera surveillance

The Camera Surveillance Act from 2013 (*Kameraövervakningslagen*) was replaced by a new Swedish Act on Camera Surveillance (*Kamera-bevakningslagen*) 1 August 2018.[9] The aim of the new law was to increase the possibilities to use camera surveillance as well as increase the protection of privacy and to adapt to the new data protection regime. Requirements for negotiations with the relevant union are found in the law on co-determination in working life. The same authority will grant permissions and supervise.

Entry into force: The adjustments were enforceable as of 1 August 2018.

Data protection in the public sector

When it comes to the public sector, the GDPR allows member states to restrict the scope of the obligations and rights, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure (e.g. Article 6.2, 6.3 with reference to 6.1 c and 6.1 e; Recital 10 in relation to sensitive data).

In brief, this allows for the sector specific laws found in the so-called Register Ordinances, which are laws targeting special sectors or even specific authorities. The Register Ordinances date back from the days of the very first Data Act of 1973. They have developed with time but are still important laws for the public sector to consider alongside the GDPR and the new Data Protection Act.

Most of the adjustments made apply to the very large number of laws in the social and healthcare sectors and include important Acts such as the Social Insurance Act, and the Patient Data Act.

Entry into force: The adjustments were enforceable as of 25 May and as of 1 August 2018.

Brottsdatalagen – Swedish version of the Police Directive

On the same day as the GDPR was issued, 27 April 2016, the new EU Law Enforcement Directive[10] was adopted. In Sweden it had been decided that the new EU Data Protection Directive would be implemented through a new framework act, the Criminal Data Act, alongside specific laws for the respective authorities.

Entry into force: Most of the adjustments were enforceable as of 1 August 2018, but the Authority-specific acts are not yet all in force.

AUTHOR

Maria Holmström Mellberg is a Senior Counsel at Cirio Advokatbyrå/Cirio Law firm, Stockholm, Sweden.
Email:
maria.holmstrom.mellberg@cirio.se

REFERENCES

1 *Offentlighets och sekretesslagen* (2009:400)
2 *Personuppgiftslagen* (1998:204), i.e. the Swedish implementation of the data protection directive 95/46/EG
3 *Datalagen* (1973:289)
4 Commissions of inquiry, which operate independently of the Government and prepare bills, may include experts, public officials and politicians.
5 *Lag (2018:218) med kompletterande bestämmelser* till EU:s *dataskyddsförordning*
6 N2016/07306/FÖF
7 *Kreditupplysningslagen* (1973:1173)
8 *Inkassolagen* (1974:182)
9 *Kameraövervakningslagen* 2013:460 and *Kamerabevakningslagen* 2018:1200)
10 (*Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut* 2008/977/RIF)

Facebook... from p.1

protection and competition laws.

The *Bundeskartellamt* concluded that: (i) Facebook held a dominant position in the German market for social networks; and (ii) Facebook had infringed competition law by abusing this dominant position through its data collection practices. The *Bundeskartellamt* ordered Facebook to cease the infringing behaviour. Although the full decision has not been released yet, the *Bundeskartellamt* has published an explanatory memo[1]. In this article, we explain what Facebook did and why the *Bundeskartellamt* considered that this broke the law in Germany. We then explore the implications of this decision, particularly as regards the overlap between competition law and data protection law, and what other companies should be thinking about for compliance purposes.

Facebook's conduct

It is common knowledge that Facebook collects a substantial amount of data on its users as they use the Facebook social network. It is perhaps less well known that Facebook also collects data through third party websites and services. This includes services like WhatsApp or Instagram, which Facebook owns, and also any other third-party website which uses "Facebook Business Tools", for example having a Facebook "like" or "share" button embedded on a page. Millions of third-party websites have these tools embedded and Facebook collects data on its users when they visit such websites, even if the user does not actually click on the buttons. Facebook's terms of service require users to agree that any data collected through these third-party services can be combined with data from the user's Facebook account, even if they have blocked web tracking in their browser or device settings.

Nature of the abuse identified

The *Bundeskartellamt* determined that Facebook holds a dominant position on the German market for social networks. Companies in dominant positions have special responsibilities. Under Article 102 Treaty on the Functioning of the European Union (TFEU), they are prohibited from abusing their dominant position, for example by taking advantage of a lack of alternative options for users or customers to impose unfair terms or prices. In deciding that Facebook held a dominant position, the *Bundeskartellamt* said that other services such as LinkedIn, YouTube and Snapchat were not sufficiently comparable to a social network to fall within the same market, despite some similarities, and despite the existence of frequent "multi-homing" (i.e use of multiple social networks) by users. This narrow market definition enabled the *Bundeskartellamt* to conclude that Facebook held a market share of over 90%.

The *Bundeskartellamt* described Facebook's conduct as an "exploitative business practice" that abused Facebook's dominant position. It recognised that the business model of a social network funded by advertising requires the processing of personal data, and that users expect this. However, the *Bundeskartellamt* was concerned that Facebook was making the use of its service conditional upon users granting it the extensive permissions necessary to enable Facebook to combine user account data with data collected from third party websites.

The *Bundeskartellamt* assessed Facebook's conduct using data protection principles (particularly those arising under the General Data Protection Regulation (GDPR)). It said that it was entitled to do so under case law of the German Federal Court of Justice, which enables civil law principles to be applied to determine whether business terms are exploitative. Applying these principles, the *Bundeskartellamt* determined that Facebook had no objective justification for collecting data from third party sources and assigning this data to users' Facebook accounts. It had not obtained effective consent from users, the processing of data was not required to fulfil contractual obligations, and Facebook's interest in processing the data did not outweigh users' interests in retaining control over their data.

Although Facebook's service is free, and its users therefore did not suffer a direct financial loss from Facebook's business terms, the *Bundeskartellamt* said that users were damaged through a loss of control over how their personal data is used. The *Bundeskartellamt* referred to the public reports of Facebook's transfer of personal data to third parties such as smartphone manufacturers, to note that "data leakage" is not merely a theoretical risk for users. It also noted that users' personal data is of great value to Facebook, allowing it to optimise its service to tie more users to its network, as well as to improve its targeted advertising services and to reinforce its indispensable position for advertising to customers, which caused further competitive harm.

The *Bundeskartellamt* has now imposed an obligation on Facebook to change its terms of service; Facebook is also required to undertake not to process data collected from third party websites without "voluntary consent" from users, i.e. users must be given a real choice and cannot be required to agree to this practice in order to use Facebook. If users do not consent, or Facebook does not seek their consent, it must severely restrict its processing of users' data. The *Bundeskartellamt* has ordered Facebook to develop proposals for how this restricted processing will operate, noting that several different criteria are feasible, for example: restricting the amount of data collected; limiting the purpose it can be used for; anonymising data; or giving users additional control options.

The *Bundeskartellamt* is likely to carry out technical monitoring of any proposal implemented by Facebook. Though the *Bundeskartellamt* has not imposed any fine upon Facebook at this stage, instead focusing on securing a change in business practices, it is likely to impose a fine if Facebook fails to make the ordered changes to its conduct.

It will be interesting to see if Facebook changes its practices in other countries, or just in Germany. Competition authorities around the world are watching the perceived market power of major platforms such as Facebook, and the *Bundeskartellamt*'s decision will doubtless be carefully reviewed by other European competition authorities. We understand that Facebook intends to appeal the *Bundeskartellamt*'s decision.[2]

The implications of this decision

Although this is the first competition law infringement decision which directly intersects with data protection law, the question of how the two bodies of law interrelate has been the subject of policy considerations for a few years. Notably, in September 2016 the European Data Protection Supervisor (EDPS) released an Opinion on coherent enforcement of fundamental rights in the age of big data[3]. The Opinion proposed establishing a Digital Clearing House through which regulators from various disciplines could voluntarily share information.

The *Bundeskartellamt* has said that it cooperated closely with (unspecified) data protection authorities during its investigation into Facebook, and that those authorities explicitly supported it proceeding with the case. It comes as no surprise then, that the EDPS has commented favourably upon the *Bundeskartellamt*'s investigation. In an article entitled 'This is not an article on data protection and competition law'[4], the EDPS described the *Bundeskartellamt*'s decision as "pioneering" and noted that it could not have taken place without the cooperation of relevant data protection authorities.

The application of competition law to behaviour regulated (and even permitted) under other laws is not a new development. The European Commission has previously established that seeking an injunction based on infringement of standard essential patents can be an abuse of a dominant position under Article 102 TFEU[5]. The CJEU agreed in *Huawei v ZTE*[6], providing a framework for negotiating a licence to standard essential patents that, if followed, offers a safe harbour through which a patent holder can seek an injunction without risking abusing a dominant position. In 2012 the CJEU held that AstraZeneca had abused a dominant position by selectively withdrawing certain marketing authorisations, so that generic pharmaceutical companies could no longer rely on them to bring competing products to market, even though this conduct was permissible under the regulatory regime applicable at the time[7].

These cases extended the scope of EU competition law. While they showed the effectiveness of competition regulators in holding companies to account, they arguably did so at the cost of using competition law to fill regulatory gaps rather than amending the relevant body of law directly (although in the second case mentioned above, regulatory change did follow). Data protection law in Europe has been subject to a very substantial overhaul in the past years. The *Bundeskartellamt*'s actions could be taken to suggest a lack of confidence in these reforms to protect consumers.

The *Bundeskartellamt*'s decision also appears to clash with the One-Stop-Shop principle envisaged by the GDPR. Facebook's base of operations in Europe is in Ireland, and the Irish Data Protection Commission is its lead supervising authority. According to European Commission guidance, the Irish Data Protection Commission should have primary responsibility for dealing with a cross-border data processing activity[8]. Instead, the German competition authority has investigated Facebook's conduct in Germany only. However, since Facebook is collecting data from third-party websites from around the world, it would seem artificial to claim that Facebook's conduct does not have a cross-border element, despite the investigation's focus on users in Germany.

To date, there is no evidence that any of the data protection authorities that the *Bundeskartellamt* worked with intend to bring a separate investigation into the conduct scrutinised in the decision. But what about data protection authorities in other EU Member States that were not contacted by the *Bundeskartellamt*? What would happen if they investigated the same conduct by Facebook or another company but concluded that it was permissible under data protection law? What about a potential future scenario where a competition regulator takes unilateral action to investigate a competition law infringement based on data protection principles without working with any data protection authorities? It is easy to see how this could lead to different standards and different rules being enforced in different European Member States, despite the aim for harmonisation under the GDPR. Whether or not any such tension arose in this particular case, it seems clear that there is potential for conflict between regulatory regimes in the future.

What does this case mean for other companies?

The conduct assessed by the *Bundeskartellamt* to be abusive in this case was relatively narrow. The *Bundeskartellamt* has made clear that it has not examined the collection of data generated by WhatsApp and Instagram (both Facebook-owned), only the combination of that (and other third-party) data with users' Facebook accounts. It has also adopted a very narrow product market (excluding services like LinkedIn and Snapchat from the definition of social network) and has assessed the geographic market as being national in scope.

In the light of those limitations, it could be argued that this case should be confined to its facts and easily distinguished from any future investigations. However, in reality, this case is part of a growing trend of competition regulators taking an interest in data. Although the European Commission in the Facebook/WhatsApp merger said that "privacy-related concerns flowing from the increased concentration of data within the control of Facebook…do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules"[9], regulators have been considering other ways in which data is relevant to competition law. The *Bundeskartellamt* worked with the French competition authority to produce a joint paper on Competition Law and Data in 2016[10] which includes a section on data-related anti-competitive conduct. The *Bundeskartellamt* has also launched a sector inquiry into online advertising, noting that "the issue of access to and the processing of data is also highly relevant from a competition point of view"[11], and in October 2018 the UK's Competition and Markets Authority confirmed that it is also considering an inquiry into the digital advertising market[12]. In March 2019, in a statement to the EU Parliament, Competition Commissioner Margrethe Vestager noted that: "data accumulation in the hands of a single firm may raise competition concerns. At the same time, when firms collect personal data, a degradation of data protection may

result in harm to competition that can be addressed by EU competition law"[13].

Data-rich companies certainly need to be aware of this Facebook decision. However, they also need to be aware of the trend for data-related inquiries more generally. Particularly where data has high monetary value (for example, in terms of driving advertising revenue), it will be important for companies to think about their proposed approach to data protection compliance in the round with competition law colleagues. This is all the more the case if competition authorities adopt similarly narrow market definitions to the ones the *Bundeskartellamt* has used here, as these increase the risks of any given company being found to hold a dominant position.

Even companies which are not dominant in these fields need to be aware of these developments. Competition authorities' interest in data is not limited to abuse of dominance investigations or merger assessments. The potential for investigations based on anti-competitive collusion under Article 101 TFEU also exists. For example, the Commission has suggested that privacy could be regarded as a non-price parameter of competition[14]. If this is the case, if companies operating within a market in which privacy is an important factor in the decision to purchase a product or service all agreed (even informally) to relax their privacy policies to make it easier to monetise data, this could amount to an infringement of competition law under Article 101.

The *Bundeskartellamt*'s decision may prove to be an outlier. It could also prove to be one of the first of many cases in which the lines between data protection and competition law are blurred. In either case, companies should be aware of the relevance of data to competition compliance.

AUTHOR

Sophie Lawrence is a Partner, and Matthew Hunt is an Associate, in Bristows LLP's Competition Practice in London and Brussels.
Emails: Sophie.Lawrance@Bristows.com
Matthew.Hunt@Bristows.com

REFERENCES

1 www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5 (accessed 26 March 2019).
2 newsroom.fb.com/news/2019/02/bundeskartellamt-order/ (accessed 26 March 2019).
3 secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf
4 edps.europa.eu/sites/edp/files/publication/19-03-11_cpi_buttarelli_en.pdf (accessed 26 March 2019; subscription required).
5 Case COMP/C-3/39.939 Samsung and Case AT.39985 Motorola.
6 Case C-170/13.
7 Case C-457/10 P.
8 ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235 (accessed 26 March 2019).
9 Case No COMP/M.7217, paragraph 164.
10 www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2 (accessed 26 March 2019).
11 www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/01_02_2018_SU_Online_Werbung.html (accessed 26 March 2019).
12 data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/the-internet-to-regulate-or-not-to-regulate/oral/91636.html (accessed 26 March 2019).
13 www.europarl.europa.eu/doceo/document/E-8-2019-000001-ASW_EN.pdf (accessed 27 March 2019).
14 European Commission, Competition merger brief, February 2015, page 6. (ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf, accessed 26 March 2019).

Ireland received 136 cross-border complaints under GDPR by end of 2018

Ireland dealt with 136 GDPR One-Stop-Shop complaints from 25 May to 31 December 2018, the Data Protection Commission (DPC) says. Under the GDPR, Ireland's 'lead supervisory authority' has primary responsibility for dealing with a complaint or an issue in cross-border cases lodged by individuals with other EU Data Protection Authorities, if the company's main establishment is in Ireland. Ireland's DPC is the lead supervisory authority for a broad range of US-based multinationals, such as Apple, Facebook, Microsoft, Twitter, Dropbox, Airbnb and LinkedIn.

This new channel of enforcement requires close cooperation between DPAs, many resources, and time. As the complainant communicates directly with the DPA where the complaint is lodged, in many cases the DPA has to translate the information into the relevant national language.

The DPC's workload has increased significantly due to the multinational technology sector. In the period between 25 May and 31 December 2018, the DPC was notified of 38 personal-data breaches involving 11 multinational technology companies. As of 31 December 2018, the DPC had 15 statutory inquiries (investigations) open in relation to multinational technology companies' compliance with the GDPR.

The DPC continues to act, or commenced acting, as lead reviewer in relation to 11 applications for Binding Corporate Rules. It is expected that it will issue decisions on several of these applications in the first half of 2019.

• *Learn more about these issues and compliance with Ireland's Data Protection Act 2018 at the Privacy Laws & Business conference on 8-9 May 2019 in Dublin in association with McCann FitzGerald. See www.privacylaws.com/ireland*

See Ireland DPC's Annual Report at www.documentcloud.org/documents/5753493-DPC-Annual-Report-25-May-31-December-2018.html

UK secures post-Brexit data flow deals with nine countries

Several jurisdictions consider the UK will remain as an adequate destination in the future. **Laura Linkomies** reports.

Privacy Laws & Business has been informed by the UK Department for Digital, Culture, Media and Sport (DCMS, responsible for data protection), that the following countries have publicly indicated that data will continue to flow freely *to* the UK after exit from the EU: Argentina[1], Faroe Islands[2], Guernsey[3], Isle of Man[4], Israel[5], Jersey[6], Switzerland[7], Uruguay[8], US[9].

The original UK exit date 29 March passed due to recent developments. As the UK Prime Minister failed to gain support for her Brexit Withdrawal Agreement in Parliament, the other EU Member States offered her two dates:

- A delay up to 31 October if the UK parliament approves the Withdrawal Bill and finds a compromise on the political declaration.
- The UK will have to hold European election in May or leave without a deal on 1 June.

With this background, the rest of the world is uncertain how data transfers will work when the UK will become a third country. If the withdrawal deal is agreed on, everything will continue as normal during the transitional period (until 2020). However, the above-mentioned countries – all in possession of an EU adequacy decision – have declared that they will allow data flows to continue. The UK, for its part, has said that data flows *from* the UK to the EU and adequate countries will continue uninterrupted. The UK has issued two sets of regulations[10] to ensure continuous data flows from these countries to the UK, and to recognise existing adequacy agreements. The regulations will come into force when the UK exits the EU. The UK Information Commissioner's Office has issued its own guidance on Brexit and data flows.[11]

Some explanations behind the decisions

Argentina's resolution states that the personal data protection standards provided by the United Kingdom of Great Britain and Northern Ireland have been maintained and even strengthened.

Uruguay states that all countries named in its Resolution, including the UK, have adequate protection standards and means to ensure their effective application.

The **Guernsey** Data Protection (Authorised Jurisdiction) (Bailiwick of Guernsey) Ordinance, 2019 adds the United Kingdom to be a designated and authorised jurisdiction in terms of data transfers. The **Isle of Man** Data Protection (withdrawal from the EU)(UK and Gibraltar) Regulations 2019 specify that the "applied GDPR" must be construed in accordance with regulation 5(1) of the GDPR (Principles relating to processing of personal data) and the Implementing Regulations of the so-called Police Directive. The **Jersey** European Union (United Kingdom Exit – Miscellaneous Amendments) (Jersey) Regulations 2019 state that from the date (if any) on which the United Kingdom becomes a country outside the European Economic Area until (if later than that date) the end of 2020, the United Kingdom is to be treated as not being a third country for the purpose of the Jersey 2018 Data Protection Act.

The US

The **US** has a partial adequacy decision from the EU. It has said that during the transition period the European Commission's decision on the adequacy of the protection provided by EU-US Privacy Shield will continue to apply to transfers of personal data from the UK to Privacy Shield participants. "During the Transition Period, the United States will consider a Privacy Shield participant's commitments to comply with the Framework to include personal data received from the UK in reliance on Privacy Shield with no additional action on the part of a participant required."

In case of a no deal, Privacy Shield participants must take the following measures:

1. Privacy Shield organizations must update their public commitment to comply with the Privacy Shield to include the UK. Public commitments must state specifically that the commitment extends to personal data received from the UK in reliance on Privacy Shield. If an organization plans to receive Human Resources (HR) data from the UK in reliance on Privacy Shield, it must also update its HR privacy policy.
2. Organizations must maintain their current Privacy Shield certifications, recertifying annually as required by the Framework.
3. Of course, it has to be noted that the EU-US Privacy Shield is currently under challenge before the EU courts and further challenges may occur.

Other developments

All of the above countries have gained an EU adequacy decision. Of that "adequacy" group, Canada, New Zealand and Andorra have not made any public declarations.

The Office of the **New Zealand** Privacy Commissioner currently has no guidance for companies on data transfers between NZ and UK after the Brexit date. A spokesman told *PL&B* that they are not aware of any legislative measures in New Zealand for that contingency, and this is unlikely to be a priority. The NZ Foreign Affairs and Trade Department does not mention data flows on its website about Brexit.[12] The ICO says on its website that "discussions with NZ are ongoing".

So for NZ it may be a wait and see situation to establish what the EU Commission will say in future regarding the UK's adequacy status. The EU

Commission is of course also assessing the validity of the existing adequacy decisions. In his Eighth Report to the European Commission on 'The Application of the Legal Data Protection Standards In New Zealand'[13], of 21 December 2018, Privacy Commissioner, John Edwards, notes that "nothing has changed in the last six months… the level of data protection in New Zealand has not been diminished during this period. I trust that this is reassuring for the purposes of the Commission's monitoring of the level of data protection under New Zealand law."

It remains to be seen whether the European Commission will continue to view **Canada's** PIPEDA as adequate. Given that the UK is Canada's third-largest export market, data transfers are of great importance.

The Office of Federal Privacy Commissioner of Canada said that an agreement between the UK and Canada may not be necessary due to the fact that, under PIPEDA, transferring organisations remain accountable for information that has been transferred to another organisation.

That is also the view of Lyndsay Wasser, Co-Chair of McMillan's Privacy & Data Protection and Cybersecurity Groups in Toronto, Canada. "Canada's privacy law does not take the same approach as the GDPR – there is no adequacy requirement. When transferring data to a third party, organisations remain responsible for it, and rely on contractual arrangements to ensure they fulfil the security and privacy requirements."

Organisations need to conduct a risk assessment and study the law of the country they are transferring data to. Wasser said that in terms of UK, nothing will change in the near future even when the UK leaves the EU. "If the UK is no longer in the EU, that will not be a bar for data transfers, unless a particular risk was identified. Where UK adequacy would come to question, is onward transfers under the GDPR," Wasser said.

In **Japan**, the Personal Information Protection Commission issued a news release on 15 March[14] clarifying that the UK intends to maintain the adequacy decisions in the EU and with Japan. Japan will continue to designate the UK under the Art. 24 of Japan's Act on the Protection of Personal Information (the equivalent country).

On 14 March, the **Dubai International Finance Centre** (DIFC) announced that it regards the UK as an adequate country for data flows[15]. The Centre failed to respond to *PL&B's* enquiry about the details. The Dubai Data Protection Law applies only to businesses registered in the DIFC.

REFERENCES

1 Resolution (in Spanish) - www.boletinoficial.gob.ar/#!DetalleNorma/202373/20190226
2 Ministerial Order, http://dat.fo/00003/00157/
3 Ordinance – http://www.guernseylegalresources.gg/article/170185/Data-Protection-Authorised-Jurisdiction-Bailiwick-of-Guernsey-Ordinance-2019
4 Data Protection (withdrawal from the EU)(UK and Gibraltar) Regulations 2019 www.tynwald.org.im/business/opqp/sittings/20182021/2019-SD-0139.pdf
5 Current privacy law – www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf
6 European Union (United Kingdom Exit – Miscellaneous Amendments) (Jersey) Regulations www.jerseylaw.je/laws/enacted/Pages/RO-009-2019.aspx#_Toc945781
7 EU Exit technical notice – www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html
8 Resolution (in Spanish) - www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-42019
9 Privacy Shield guidance – www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs
10 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019, www.legislation.gov.uk/ukdsi/2019/9780111177594
11 ico.org.uk/for-organisations/data-protection-and-brexit/
12 www.mfat.govt.nz/en/countries-and-regions/europe/united-kingdom/brexit-the-uk-and-europe/
13 privacy.org.nz/assets/Uploads/Supplementary-Report-on-NZ-Adequacy-to-EC-21-December-2018-A609354.pdf
14 www.ppc.go.jp/files/pdf/310315_houdou.pdf (in Japanese)
15 www.difc.ae/business/operating/data-protection/adequate-data-protection-regimes/

Organisations fall short on internal monitoring

GPEN, the DPAs' global enforcement network, conducted its 2018 sweep on accountability. 18 GPEN members made contact with 667 organisations in 18 countries during the 'sweep'. The findings include:

- When it comes to monitoring internal performance in relation to data protection standards, many organisations were found to fall short, with around a quarter who responded having no programmes in place to conduct self-assessments and/or internal audits.
- Nearly 75 percent of organisations contacted had people and processes in place to respond appropriately to a data breach.

The Sweep was jointly coordinated by the Office of the Privacy Commissioner (OPC), New Zealand, and the Information Commissioner's Office, UK. The names of participating DPAs have not been revealed.

- *See privacy.org.nz/assets/Uploads/GPEN-Sweep-2018-International-report.pdf*

Bulgaria introduces a range of derogations from the EU GDPR

The legislator passed amendments to the Personal Data Protection Act on 26 February which entered into force on 2 March. **Dessislava Fessenko** reports from Sofia.

Bulgaria has introduced a set of specific requirements[1] relating to the processing of personal data in addition to the requirements under the EU General Data Protection Regulation (the GDPR). Such specific requirements (commonly known as "derogations") are allowed by the GDPR in certain areas, such as employment, the role of data protection officers, and data protection impact assessments, as long as they introduce more detailed or tailored rules on data processing without deviating from the letter or spirit of the GDPR.

Bulgaria has taken advantage of this possibility under the GDPR to introduce, among others, specific requirements.

Data Protection Officers: Bulgaria-based businesses may appoint as data protection officers (DPOs) individuals who are based abroad. However, those individuals need to be registered with the Bulgarian Data Protection Authority in the same way as Bulgaria-based DPOs are, based on a standard registration form. The new rules set no further specific requirements regarding the appointment of DPOs. The initial draft of the rules envisaged that Bulgaria-based businesses would also be required to designate a DPO if they process the personal data of more than 10,000 individuals. This requirement has been now been set aside and not introduced. DPOs would need to be appointed only in the conditions envisaged under the GDPR, i.e. in cases of regular and systemic monitoring or large-scale data processing.

Surveillance of public areas: There is a need for bespoke policies in case of large-scale data processing or large-scale systemic monitoring of publicly accessible areas. Bulgaria-based companies would need to introduce bespoke rules and procedures for data processing in cases of: (i) large-scale data processing; or (ii) systemic large-scale surveillance of public areas (such as video surveillance). Such rules would need to clearly set out, among others, the grounds, scope and mechanics, purposes and duration of the surveillance, as well as the means for the protection of the rights of individuals and information security measures. In cases of video surveillance, such rules must also elaborate on territorial scope and means of video surveillance, duration of storage of the video footage, and ensure appropriate means/media for informing data subjects of the existence of video surveillance. To devise adequate rules in this respect, companies would first need to complete a data processing impact assessment (DPIA) as required under the GDPR, and then reflect the DPIA's conclusions and recommendations in their bespoke policies on surveillance.

Individuals' personal identification numbers may not be made public, unless required by law. Personal identification numbers may not be used as the sole identification to grant access to IT systems or for the provision of services.

Collecting and storing copies of personal identification documents (e.g. ID cards and driving licenses) is in principle prohibited. Copies of such documents may be made and stored only when required by law. Consent or legitimate interest would not serve as a reliable ground of such processing.

Data processing for employment purposes

Employers may not make and keep on file copies of employees' personal identification documents, unless explicitly required by law (as per above).

Internal policies: Employers must adopt a set of internal policies regulating whistleblowing systems, acceptable/restricted use of internal resources (e.g. IT systems, devices and equipment, etc.), and systems for monitoring access to work premises, working hours and work organisation. These policies must be tailored to the essence and specificities of the employer's activities and not use merely standard documents.

Legitimate interest and consent: If employers collect and process data that is not directly related to and necessary for the employment relationship, they must be able to justify their legitimate interest or seek the employee's consent for this additional data processing. Businesses should take care not to over-rely on such consent, as under the GDPR it would be considered invalid if not freely given, which is often the case in an employer-employee relationship.

Recruitment: Employers must have clear rules on retention and storage of job applicants' personal data. No data may be stored for longer than six months without the employees' explicit consent. The same rules apply to documents on unsuccessful candidates' unsuitability, (e.g. physical or mental fitness) unless specifically requested by law.

Other areas

Minors' consent to data processing: Bulgaria-based information services providers may collect and rely on consent directly from minors only if they are aged 14 or older. Otherwise, consent must be sought from the minors' parents or guardians.

Data processing by media: Media outlets need to strike a balance between data protection and freedom of expression and information. Data protection does not by default override freedom of expression/information. The media may process personal data for journalistic purposes only if it does not intrude on the individual's personal life.

AUTHOR

Dessislava Fessenko is Of Counsel and co-head of the firm-wide TMT sector at Kinstellar, a Bulgarian law firm in Sofia. Email: dessislava.fessenko@kinstellar.com

REFERENCE

1 See www.cpdp.bg/en/index.php?p=element&aid=1194 (in English)

Global data privacy 2019: DPAs, PEAs, and their networks

Most regulators are cooperating with their peers through several DPA networks, some of which have decision-making powers. By **Graham Greenleaf**.

The networks of Data Protection Authorities (DPAs) and (as they are sometimes called) Privacy Enforcement Agencies (PEAs) have continued to expand in numbers of members, and in their activities, in 2017-18. This article analyses the details of those networks set out in the 2019 Global Tables of Data Privacy Laws (Supplement to *Privacy Laws & Business International Report*, Issue 157, 16 pages), and completes the analyses started in that issue.[1] The last two columns of the Table identify the DPA/PEA, where one exists, in each of the 132 countries with data privacy laws,[2] and each network of which they are a member.

Halls of Shame: Inoperative laws and missing DPAs

Enacted data privacy laws can be made ineffective by various means, which need to be called out. Laws which have not been brought into force for more than two years after enactment, or where a Data Protection Authority has not been appointed to make the law operative two years after enactment, after two years, qualify for the two Halls of Shame in this analysis.

No DPA provided for: Although the existence of an independent data protection authority is often regarded as essential for an effective data protection law, legislation in 14[3] of the 132 countries does not create any separate DPA at all, but leaves data privacy enforcement up to other State institutions. China, India, Indonesia and the US are the most important examples, but in 2019 it is possible that any of them might change their position on this.

Whether Brazil's new law includes a data protection authority depends on whether Congress, by 4 June 2019, affirms a decree creating a DPA made by the outgoing President at the end of 2018.[4]

No appointment of a DPA: In other countries, the law purports to create a DPA, but no such appointments have been made within two years of enactment (date as indicated in the Table), and the law has not come into effective operation. At least 11 countries have so far failed to appoint a DPA, as required by their law, including: the Dutch Caribbean territories of Aruba, Curacao and Sint Martin (2011); Nicaragua (2012); Chad (2015); Madagascar (2015); Equatorial Guinea (2016); Mauritania (2016); Guinea (Conakry) (2016); and Bermuda (2016). Many African countries are only newly in this list, and may well exit from it by the next edition. Angola (2011) escaped from this Hall of Shame in 2017-18 by finally appointing its DPA.

A small number of laws do create a specialised DPA, but explicitly provide that it is not independent of the government, and must follow government instructions when and if issued. These include Malaysia and Singapore (which do not have public sector jurisdiction) and Macau (which does). There is considerable evidence of independent action by at least Singapore's and Macau's DPAs.

Laws not brought into effect: South Africa is the most important discreditable example here, having appointed its Information Regulator in December 2016, but most provisions of its 2013 Protection of Personal Information Act (POPI) are still not in force after six years. [5]

In addition to the above countries whose laws are ineffective because of failure to appoint a DPA, a few other countries without provision for a DPA have failed to bring their laws into force for at least two years after enactment (date as indicated in the Table), including St Vincent & Grenadines (2003) and Seychelles (2004).

Conclusions: Only 10% of national laws do not create specialised DPAs, and only very rarely are explicitly subject to government control. Another 10% have not appointed a DPA within a reasonable time (or in three cases brought their law into force). The result is that 80% of the 132 countries with data privacy laws have them administered by appointed and functioning, specialised DPAs (almost always independent). How well they do their job as regulators is another question, but specialist, functioning DPAs are the rule, not the exception.

Networks: Associations of DPAs and PEAs

There are three types of associations of data protection bodies: (i) those created by international treaties, agreements or legislation; (ii) informal networks oriented to policy development; and (iii) informal networks oriented toward enforcement actions. There are overlaps between the three types.

Background on each of the DPA/PEA associations in (ii) and (iii) discussed in this article can be obtained from the 2017 and 2015 analyses.[6] Other than for new associations, this article focuses on updating membership details.

Bodies created by international treaties, agreements or legislation: The most important associations of DPAs are those created by international treaties, agreements or legislation, because they are usually given some formal powers under those instruments, and sometimes a separate legal identity. These powers may become increasingly important as data privacy issues become more important to multi-national blocs with economic and political power. Three such bodies are significant at present.

The EDPB (European Data Protection Board) – The Board is comprised of the 28 national DPAs (EU's GDPR art. 68).[7] The European Data Protection Supervisor (EDPS) participates in some decisions and also provides the secretariat, and the European

Commission participates without voting rights. European Economic Area Members, Norway, Iceland and Liechtenstein, have permanent seats on the European Data Protection Board (EDPB). The three countries may speak at meetings, and may vote on issues but their votes are recorded separately from those of the 28 EU Members of the EDPB. Switzerland, which has a separate treaty with the EU, has no right to attend EDPB meetings, but has a special status and may be invited to attend as an observer for meetings, for example, covering Schengen-related matters.

The EDPB has extensive powers under the GDPR – art. 70 lists 23 tasks of the Board, of which the most significant may be its opinions and (in some cases) binding decisions under the consistency mechanism (art. 70(1)(t)). Its members are listed in the Table. The Board replaces the former Article 29 Working Party under the previous 1995 Directive.

The Council of Europe Convention 108 Consultative Committee – The Committee is not comprised directly of DPAs from the 54 Parties to Convention 108, but consists of representatives of those Parties. However, a country may choose to appoint its DPA to represent it on the Committee, and often does so. It is nevertheless included in the 'DPA Associations' column in the Table, including non-party countries or DPAs accredited as Observers to the Committee. The Consultative Committee prepares reports on the laws of countries applying for accession to the Convention. Under the new Convention 108+, when it comes into force, the new Convention Committee has reinforced powers, including that of monitoring the compliance of parties to the Convention. The current Committee, with membership from 54 Parties (including seven non-European), plus fourteen Observer countries/DPAs, is the most global data privacy "treaty body".

The Joint Oversight Panel (JOP) of the APEC Cross-border Privacy Rules system (CBPRs) consists of three members of the APEC Privacy Sub-group appointed for a two-year term.[8] Technically, these are representative of APEC member economies, but governments sometimes appoint their DPAs or PEAs. APEC is not a treaty, and nor is the CBPRs, but the JOP makes findings about which economies are entitled to participate in CBPRs, and which companies are qualified to act as "Accountability Agents" (AAs) under CBPRs.

Policy-oriented networks: The important new network the *African DPA Network (Réseau Africain des Autorités de Protection des Données Personnelles or RAPDP)* established in 2016 during the second African Data Protection Forum, met informally for the first time in 2018 in Morocco with South Africa as the newest of its ten members.[9] Discussions focused on finding solutions to reinforce the voice of Africa within the different international organizations dealing with privacy, such as the ICDPPC. The first separate Conference of the African DPA Network will be held in Accra, Ghana in June 2019. The African Union Convention on Cyber-security and Personal Data Protection 2014 makes it a goal of African DPAs to set up cooperation mechanisms among themselves and with other DPAs (Art. 12.2(m)), but does not formally establish such a grouping. According to its articles of association (art. 5)[10], the aim of the network is to create an institutional framework to share privacy practices, to support the implementation of national data protection legislations and to foster mutual cooperation between African DPAs.

The changes to membership status in 2017-18 in the other policy-oriented networks are as follows (only considering national authorities /representatives):

- **ICDPPC** (International Conference of Data Protection and Privacy Commissioners)[11] has four new national members – Montenegro, South Africa, Japan and Turkey – plus a replacement member for Argentina.[12] ICDPPC also includes some sub-national and sectoral DPAs, and this membership also continues to expand.[13] Some countries also share data protection responsibilities between more than one DPA.[14]
- **CTN** (the Common Thread Network of DPAs of Commonwealth member countries and territories[15]) now has members from 13 countries (plus sub-national DPAs) including new members Cayman Islands and South Africa. Many DPAs in Commonwealth countries are not yet members, including Malaysia, Singapore, Antigua & Barbuda, St. Lucia, and Trinidad & Tobago. The overlapping organisation BIIDPA (British, Irish and Islands' Data Protection Authorities)[16] is active with nine members but has not added new members since 2016.
- **AFAPDP**, the Francophone Association of DPAs,[17] has full members from 20 countries, with voting rights, and many other observer members.
- **APPA** (Asia-Pacific Privacy Authorities) now includes the Philippines in its 19 members.
- **REDIPD** (*La Red Iberoamericana de Protección de Datos*, also called the *RedIberoamericana* or Latin American Network)[18] now includes Chile as its 23rd member (all Latin American countries, plus Spain, Portugal and Andorra).
- Of the various European networks, **EDPA** (The European-wide "Spring Conference" association of DPAs), meeting since 1990, has not appointed recent new members, and has delayed a decision concerning Turkey. Nor has **CEEDPA** (Central and Eastern Europe Data Protection Authorities)[19] added new members. Establishment of **RNDPAEPC** (Regional Network of Data Protection authorities in Eastern Partnership Countries) was supported by an establishment grant, but does not seem to have continued, and is not in the Table.

There is still no Caribbean organisation of DPAs, nor one for Portuguese-speaking countries.

Enforcement networks: The changes to membership status in 2017-18 in the enforcement-oriented networks are as follows (only considering national authorities / representatives):

- **GCBECA**, ICDPPC's **Global Cross-Border Enforcement Cooperation Arrangement**)[20] established by resolution of the 2014 ICDPPC Conference in Mauritius now has members from 11 countries (both national and sub-national DPAs in some cases), with Germany having joined in 2017.

They are listed in the Table.

- **GPEN**, the Global Privacy Enforcement Network[21] has included five new members in 2017-18[22] (Cayman Islands, Turkey, Ukraine, Abu Dhabi (UAE) and Qatar), so that it now has members from 51 countries (plus sub-national and supra-national members). A significant new sub-national member is the Californian Attorney-General's Office. GPEN's most significant recent public activity are its GPEN Sweeps, which in 2017 looked at website privacy notices,[23] and in 2018 accountability.[24]
- **GPEN Alert** is a separate network within GPEN, and administered by the US Federal Trade Commission (FTC) on behalf of its 11 participants (listed in the Table, except Singapore, its newest national member). British Columbia is a new sub-national member. It facilitates information sharing on individual investigations, and therefore has high security requirements.[25]
- **APEC-CPEA** (Cross-border Privacy Enforcement Arrangement) is an enforcement cooperation network of which membership is required for countries becoming involved in the APEC-CBPRs system, but is open to other APEC member DPAs/PEAs as well.[26] It has members from eleven countries (listed in the Table), including Taiwan and the Philippines as new members since 2017.[27]
- **UCENet** deals with prevention of spam ("unsolicited commercial email"). Participation is not limited to DPAs,[28] but the five DPAs that are members[29] are listed in the Table.

Conclusions

Where a DPA or PEA has been established, and the law is more than two years old, the record of national DPAs and PEAs in joining these networks is reasonably good. There are only 13 such DPAs that are not a member of at least one such association.[30] Almost all of the above associations have obtained modest increases in membership in 2017-18.

While membership of most of the above policy and enforcement-oriented associations has not yet reached its maximum extent, progress toward this goal continues for most of them. This is valuable for the future of data protection in that it promotes consistent development of principles in polities with common interests and traditions, and facilitates collective action.

INFORMATION

The assistance of Sophie Kwasny, Hannah McCausland, Laura Linkomies, Danilo Doneda, Bertil Cottier, Clarisse Girot and Pablo Palazzi is acknowledged with gratitude. Responsibility for all content remains with the author. Separate acknowledgments accompany the Tables.

REFERENCES

1 G. Greenleaf 'Global data privacy laws 2019: 132 national laws and many bills' (2019) 157 *Privacy Laws & Business International Report*, 14-18; G. Greenleaf 'Global data privacy laws: New eras for international standards' (2019) 157 *Privacy Laws & Business International Report*, 19-20.
2 New 2019 data privacy laws in Nigeria (a regulation) and Uganda now make that total 134 and adds two more data protection authorities.
3 Countries with no separate DPA: Azerbaijan; China; Colombia; India; Indonesia; Kyrgyz Republic; Kazakhstan; Malawi; Paraguay; Qatar; St Vincent & Grenadines; Taiwan; Vietnam; and the US.
4 The National Congress on 27 March 2019 nominated a mixed Commission of both Senators and Representatives to evaluate the Presidential Decree, and which has until 4 June to report on the text, which will have also to be approved by both houses or it will lose its effect.
5 Information Regulator (South Africa) www.justice.gov.za/inforeg/index.html
6 G. Greenleaf 'Data Privacy Authorities (DPAs) 2017: Growing Significance of Global Networks' (2017) 146 *Privacy Laws & Business International Report*, 14-17 ssrn.com/abstract=2993186; G Greenleaf 'Global Data Privacy Laws 2015: Data Privacy Authorities and Their Organisations' (2015) 134 *Privacy Laws & Business International Report*, 16-19 papers.ssrn.com/sol3/papers.cfm?abstract_id=2641772
7 EDPB membership edpb.europa.eu/about-edpb/about-edpb_en
8 Appointed from the APEC Privacy Subgroup of the Electronic Commerce Steering Group (ECSG) of the Asia-Pacific Economic Cooperation (APEC).
9 Full membership to the network is limited to countries which already have appointed DPA; countries which have adopted national data protection law (or who are in the process of adopting such a law) are granted observer status (art. 6 articles of association). These notes on RAPDP have benefitted from joint work with Prof Bertil Cottier.
10 RAPDP articles of association cnilbenin.bj/statut/. So far this constitution is available only in French (though Arabic, English and Spanish are also official languages of the Network).
11 ICDPPC icdppc.org/
12 The Argentinian National Data Protection Authority was a member since 2003. The National Access to Public Information Law adopted in September 2016 created the National Access to Public Information Agency as an independent authority and autonomous office, also tasked with the oversight of the National Data Protection Act and thus replacing the National Data Protection Authority.
13 For example, in 2017-18, new members included the Bavarian Data Protection Authority, (*Bayerisches Landesamt für Datenschutzaufsicht*); *Die Landesbeauftragte für den Datenschutz*, Lower Saxony (Federal Republic of Germany); and the Supervisory Body for Police Information Management (Belgium).
14 For example, in 2017 the Korea Communications Commission (Republic of Korea) also became a member, even though Korea's Personal Information Protection Commission was already a member.
15 Common Thread Network commonthreadnetwork.org: "a forum for data protection and privacy authorities of Commonwealth countries".
16 BIIDPA members include the UK, Ireland, Cyprus, Jersey, Isle of Man, Malta, Gibraltar and Bermuda idpc.org.mt/en/Pages/dp/int/bidpa.aspx
17 AFAPDP www.afapdp.org/
18 RedIPD, list of members www.redipd.org/la_red/Miembros/index-iden-idphp.php
19 CEEDPA www.ceecprivacy.org/main.php, meeting since 2001.
20 Enforcement Cooperation Arrangement FAQs icdppc.org/participation-in-the-conference/enforcement-cooperation-arrangement-faqs/
21 GPEN www.privacyenforcement.net/
22 New GPEN members: Armenia; Georgia; Ghana; Japan; Jersey; Malta; Morocco. These memberships were inadvertently omitted from the Table when first published. Please update incomplete copies.
23 GPEN Press Release by UK ICO www.privacyenforcement.net/content/gpen-sweep-2017-international-enforcement-operation-finds-website-privacy-notices-are-too
24 For results, see ico.org.uk/about-the-ico/research-and-reports/information-rights-research/
25 "GPEN Alert is a separate information-sharing tool for GPEN members that uses the secure Consumer Sentinel Network (CSN) platform infrastructure and user interface, but is otherwise segregated from the CSN database. Participating privacy enforcement authorities may use GPEN Alert to notify other member authorities of their privacy investigations and enforcement actions, particularly those that have cross-

REFERENCES (CONTINUED)

border aspects, for purposes of potential coordination and cooperation. To be a member of GPEN Alert a DPA must be a GPEN member and sign on to the MOU and Data Security and Minimum Safeguards Certification." (from GPEN's website)
26 APEC-CPEA www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx
27 APEC-CPEA members: Australia, NZ, USA, HK SAR China, Canada, Japan, Korea, Mexico, Singapore.
28 See UCENet website www.ucenet.org/member-organizations/
29 DPAs that are UCENet members – Canada, Ireland, Spain, UK, US
30 The DPAs of these jurisdictions are not members of any association: Angola; Antigua & Barbuda; Dubai IFC; Faroe Islands; Greenland; Lesotho; Malawi; Malaysia; Qatar FC; Sao Tome & Principe; St Lucia; Yemen; Zimbabwe.

Managing international data breaches in practice

Morgane Christiane and **Giorgia Vulcano** of Deloitte Consulting & Advisory discuss the need for pre-breach planning and post-breach responsiveness.

The financial and reputational disruption an organization faces in the event of a data breach is inestimable. The GDPR has brought about a new reporting obligation, and the numbers are rising. In its report 'GDPR, Six Months On: Balance'[1], the Belgian Data Protection Authority stated that between 25 May 2018 and 21 November 2018, 317 data breaches were reported and the industries mostly affected were health care, insurance, public administration and defence, telecommunication & BIPT (Belgian Institute for Postal Services and Telecommunications), and financial services. From a pan-European perspective, DLA Piper's GDPR data breach survey revealed that more than 59,000 data breaches were reported to Data Protection Authorities[2] between the entry into force of the GDPR on 25 May 2018, and International Data Protection Day on 28 January 2019.

A company may never be fully secure. However, there are comprehensive measures that can be integrated in its cyber defense strategy to help minimize the repercussions suffered and the impact on data subjects' rights and freedoms.

Legal background

The legal framework that guides data breach preparation and response procedures may vary depending on the applicable laws and regulations, including Member State laws and other legal instruments such as the EU NIS and e-Privacy directives. If an incident detected qualifies as a personal data breach, the applicable law(s) will need to be identified. For the purposes of this article, only the specific data breach requirements of the GDPR will be taken into consideration.

Under the GDPR, companies must have in place technical and organizational measures and be ready to respond to a data breach[3].

The suggested data security regime foreseen under Article 32 of the GDPR and its recitals identify measures that are relevant to the protection of the data, according to the company's risk and exposure to data breaches. It is thus critical for companies to perform an internal assessment of the data they process to determine what risk-based security measures are appropriate to them.

In line with the regulatory requirements, an adequate breach response plan should allow a company to detect, address and mitigate a data breach without serious disruptions to the everyday business and in a timely manner (i.e. within the timeline foreseen under the GDPR).

In the following, we outline how the implementation of an appropriate data security regime and breach notification procedures can help a company build the infrastructure needed to comply with the Regulation, and effectively respond in the event of a personal data breach.

Organizational process: Detection and reporting

Incident detection plays a key role in a company's breach response plan. It may sometimes take years before a company is able to detect an incident, highly compromising its capacity to mitigate the financial and reputational consequences, especially when the incident amounts to a personal data breach that impacts the rights and freedoms of data subjects.

Human error and oversight are often the most common causes of breaches, particularly when employees are not fully capable of detecting and timely reporting a data breach. To this end, putting into place clear and user-friendly guidelines, along with the appropriate training, can prepare staff ahead of the breach and ensure a rapid and appropriate reaction before an "incident" occurs.

Further to this, increasing the employees' awareness and knowledge of what types of incidents should be reported, within which timeframes, to whom in the organization, and how they should do so, can overall help familiarize them with the processes and appreciate what is expected from them in case of an incident.

Types of incidents: Employees should be able to recognize an incident when they notice one and have a clear understanding of what they should be reporting. A company should be able to define which types of incidents have to be reported (e.g. security incidents, privacy incidents, confidentiality incidents, etc.), and to provide clear definitions of the different types.

Timeframes: Under Article 33 of the GDPR, a notifiable data breach

must be reported to the concerned Data Protection Authority, without undue delay, and within 72 hours of having become aware of it. This means that when it is relatively clear, or when it has been established with a "reasonable degree of certainty", that an incident compromises personal data, the clock starts ticking[4]. To comply with this timeframe, companies should consider defining clear communication timeframes in their breach response plan, for example mentioning that employees need to report incidents immediately or within a specific timeframe to an identified person or team. Managers should also ensure that a breach response plan can be properly executed in terms of timing, resources and required effort. Whilst most companies may already have in place security incident and data breach guidance, it is not obvious that they can anticipate the new, evolving types of threats, or ensure that employees are fully aware of the existence and further development of the relevant guidelines and procedures.

Companies acting as processors should also consider following a timeframe, in order to ensure that the Controller is notified "without undue delay" after the Processor becoming aware of a personal data breach[5].

Reporting channels: Companies should determine their reporting channels, exploring the options that are most suitable to their size and structure. In addition, companies might want to consider appointing an intermediary (with clearly defined responsibilities), when the size or the location of the company suggest so. For example, some may opt for allowing an employee to report the incident by completing a short predefined form and send it via e-mail to a concerned intermediary (e.g. a specific Incident Response Team) or, if there is no intermediary appointed, directly to the DPO. The objective of involving intermediaries is to avoid the DPO becoming overloaded with all the reported incidents.

Intermediary or not, in a scenario like the above, companies might consider creating a specific mailbox for incident reporting purposes only, to avoid the risk that incident reports are lost or overlooked. Another option companies might want to consider is using a ticketing system to centralize all incidents and have a first triage in place (automatic or manual) assigning the tickets to the appropriate team.

Breach notification: When an incident is detected and reported, and the company determines that it amounts to a personal data breach with the likelihood of resulting in a risk to the rights and freedoms of natural persons, then Article 33 of the GDPR applies and companies must activate a notification procedure.

Organizational process: Assessment and notification

Risk assessment: When a company detects that an incident amounts to a personal data breach, it must assess and measure the severity of the data breach and the likely impact on the rights and freedoms of the individuals involved. Based on that assessment, it determines whether the notification obligation to the Supervisory Authority and, eventually, to the data subjects, is triggered. To do so, companies may resort to available methodologies such as the European Union Agency for Network and Information Security (ENISA)'s "Recommendations for a methodology of the assessment of severity of personal data breaches", or prepare an internal template to structure the risk assessment. To this end, the Article 29 Working Party (WP29)'s Guidelines on Personal data breach notification provide that the assessment should take into account the "severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring" and namely, the type of breach, the nature, sensitivity, and volume of personal data, the ease of identification of individuals, the severity of consequences for individuals, the special characteristics of the individual, the special characteristics of the data controller, and the number of affected individuals[6].

Cross-Border Notification Duties: In case of a notifiable data breach, companies need to report it to the competent Supervisory Authority in accordance with Article 55 of the GDPR. However, Article 56 provides that in the case of cross-border processing, "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor". Further to this, and as suggested by the WP29's Guidelines on Personal data breach notification, "when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify"[7].

In line with the above, in order to report a notifiable data breach within the 72 hours mandated by the GDPR, companies undertaking cross-border transfers of personal data must have identified the lead Supervisory Authority they will have to deal with. Supervisory authorities may provide a breach notification form on their website, with a different level of detail required (for example, the number of questions and the quantity of information that the breach notification form prepared by the Belgian Data Protection Authority requires compared with the one provided by the ICO). Familiarizing themselves with the required fields and acknowledging the time and effort needed to complete the form may help companies save time in the actual breach situation. If the lead Supervisory Authority does not provide a form for breach notification, then companies may want to consider having in place a template, in the language used by the lead Supervisory Authority, and to include the details specified in article 33[8]. In addition, companies should ensure they are aware of any other specific requirements ahead of time (for example, authentication requirements such as currently is the case in Spain).

As mentioned earlier, the severity and significance of the data breach may also require notification to the data subjects without undue delay[9]. As a pre-breach measure, companies should consider having a template in place to communicate to the individuals involved, in line with Article 34 of the GDPR, "at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)". As a cross-border breach may impact the rights and freedoms of data subjects in different countries, having a multi-lingual template, translated to the languages of the data subjects, can help coordinate and speed up the communication. This is also supported by the WP29 guidelines mentioned earlier. Further to this,

companies might want to consider having multi-lingual contact points for the data subjects to reach out to.

Documentation and breach remediation: To satisfy the accountability requirement, companies should implement a central repository to record, along with the relevant documentation, both notifiable and non-notifiable data breaches, as outlined in Article 33.5 of the GDPR. The record should include "the facts relating to the personal data breach, its effects and the remedial action taken". The DPO, who should play a key role when it comes to breach preparedness and response, and who should be informed of the data breach, may be an appropriate keeper of such records[10].

In line with the above, companies may consider putting in place a breach evaluation form to help them identify adequate data breach remediation actions, address their vulnerabilities and, overall, improve their cyber preparedness and response strategy. These measures may include, for example, additional training for employees, reviewing and adjusting the relevant data protection policies and procedures, improving reporting processes, strengthening the security measures and enhancing the Privacy by Design approach.

Conclusion

Companies should understand how critical it is for their financial and reputational wellbeing to invest in compliant and effective security regimes and breach notification procedures. According to Deloitte's General Data Protection Regulation (GDPR) survey, 17% of respondents claim that if a breach occurred, they would no longer use a service or buy from an organisation[11].

Business objectives and talent may also suffer from the repercussions of a breach. From a business objectives standpoint, a company may see its strategy, priorities and key focus areas compromised by having to dedicate its resources to breach management. With regards to talent, it may become challenging to attract new talent or maintain current employee engagement and morale as a breach may damage the confidence and perception of the company itself.

Although the most expected costs of a data breach are the imposed fines and penalties, there are some additional less obvious consequences such as the legal consequences that stem from contractual arrangements with the processors, the complaints brought by data subjects, and the need to invest more in public relations and communications.

Whilst dedicating resources, time and expertise on pre-breach planning and post-breach responsiveness and evaluation will not fully neutralize the cyber risk exposure, it will allow a company to minimize the business repercussions and ensure conformity with the regulatory requirements. For example, some companies are setting privacy-specific metrics and goals to measure and assess their maturity by analyzing the number of reported incidents and closed incidents with a trend analysis. This may allow a company, for example, to show the effectiveness of their privacy compliance program and identify the need of implementing additional measures and safeguards, such as increasing their privacy awareness. Similarly, some companies initiate breach readiness exercises consisting of breach drills, walkthroughs or scenario stress testing. These simulations help companies evaluate their response capabilities by testing and exercising their data breach management. Further to this approach, a company may improve its discovery capabilities by allowing the privacy and security professionals to work together during incidents so as to determine the impact, assess the risks of data exposure and define the next actionable steps across functions.

AUTHORS

Morgane Christiane and Giorgia Vulcano are Privacy and Data Protection Senior Consultants at Deloitte Consulting & Advisory CVBA in Brussels.
Email: mchristiane@deloitte.com

REFERENCES

1 *Autorité de protection des données* (Data Protection Authority for Belgium), «Le RGPD après six mois : bilan", published on the 23rd of November 2018, available at https://www.autoriteprotectiondonnees.be/news/le-rgpd-apres-six-mois-bilan
2 DLA Piper, "DLA Piper GDPR data breach survey: February 2019", 6th of February 2019, available at bit.ly/2GIWaZ3. For more information also see The European Data Protection Board, "GDPR in numbers" data available at bit.ly/2Rdeyef. According to the latter, 255 Cross border investigations were initiated by the Data Protection Authorities as of January 2019.
3 According to Article 4.12, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". When a personal data breach occurs, companies have a duty to assess its likeliness "to result in a risk to the rights and freedoms of natural persons" (Article 33.1 of the GDPR) and if so, report it to the competent Supervisory Authority without undue delay and within 72 hours from becoming aware of the breach. In addition to the latter, Article 34.1 of the GDPR provides that if the breach "is likely to result in a high risk to the rights and freedoms of natural persons" (Article 34.1 of the GDPR), then it shall also be communicated to the data subjects, unless one of the exceptions identified under paragraph 3 of the same disposition applies.
4 Working Party Article 29, "Guidelines on Personal data breach notification under Regulation 2016/679". Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, p. 11.
5 General Data Protection Regulation, art. 33, § 2.
6 Working Party Article 29, "Guidelines on Personal data breach notification under Regulation 2016/679". Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, p.24-25
7 Working Party Article 29, "Guidelines on Personal data breach notification under Regulation 2016/679". Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, p. 17
8 These are: (i) the nature of the personal data breach; (ii) the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) the likely consequences of the personal data breach; (iv) the measures taken or proposed to be taken by the controller to address the personal data breach.
9 See Annex B of the WP29 guidelines for a non-exhaustive list of data breaches that are likely to affect the rights and freedoms of the data subjects.
10 Working Party Article 29, "Guidelines on Personal data breach notification under Regulation 2016/679". Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, p.28
11 Deloitte, North Western Europe, "A new era for privacy GDPR six months on" (p.17). The survey was based on 1,100 responses from individuals with involvement in GDPR within their organisations and 1,650 responses from consumers, and was conducted across 11 countries.

Thailand adopts comprehensive new DP law with extra-territorial effect

Thailand's Personal Data Protection Act (PDPA) was approved by its National Assembly on 28 February 2019, for submission for royal endorsement and then publication in the Government Gazette. It will come into effect one year after such publication. A Cybersecurity Act was approved at the same time. These developments occurred three weeks before Thailand's first general elections since a military coup in 2014. The composition of the new government is not yet finalised.

The PDPA is based on a GDPR-influenced Bill proposed by the current (junta) government in May 2018 (examined in Greenleaf and Suriyawongkul 'Thailand's draft data protection Bill: Many strengths, too many uncertainties' *Privacy Laws & Business International Report* June 2018, pp. 22-25), but it has many differences from that Bill.

Some notable points on which the Act differs from that 2018 Bill, takes a different approach to the EU's GDPR, or are significant for businesses outside Thailand, are as follows:

- The PDPA is a comprehensive Act, unlike the private-sector-only laws in the rest of ASEAN (Philippines excepted). It exempts few parts of the private sector (credit reporting has a separate law) or public sector (courts, legislature, security and law enforcement), but further exemptions can be made by decree.
- The PDPA will have extra-territorial effect (similar to the GDPR) in relation to marketing to, or monitoring of, persons in Thailand. Processing outside Thailand by a controller or processor located in Thailand is also covered.
- A Personal Data Protection Committee (PDPC) is established as the primary body to administer the law, but it has no legislatively guaranteed independence. There is also an Office of the PDPC, which is a government department. Expert Committees will determine complaints.
- Genetic and biometric data have been added to the categories of 'sensitive personal data', consistent with the GDPR.
- Data exports from Thailand can occur to countries which have an "adequate level of protection", as determined by the PDPC. However, "adequate" is to be determined by criteria set by the PDPC, so it cannot be assumed that it will mean the same as it does in the EU.
- Additional provisions allowing data exports include a form of Binding Corporate Rules (BCRs), and undefined 'appropriate safeguards', both to be based on standards set by PDPC.
- Many breaches of the PDPA can result in administrative fines, for which the highest maximum amount is 3 million baht (approx. US$100K). This is now a low maximum by international standards, but may still be a deterrent to some local businesses.
- Data subjects have a right to seek compensation from a court for any breaches of the Act (and with few defences provided), and the court may impose additional compensation up to double the original amount (i.e. 'triple damages').
- Appointment of data protection officers (DPOs) will be required, with exceptions for a 'small sized business' (criteria to be specified by PDPC).

• *PL&B will publish a more detailed analysis of the PDPA once a full English translation becomes available.*

ICCA and IBA to issue guide on international data protection arbitration

ICCA, The International Council for Commercial Arbitration, and IBA, The International Bar Association are to produce a guide on international data protection arbitration.

The guide will identify the ways in which data protection may need to be taken into account during the course of an arbitration. As it is not possible to address all the data protection laws that might apply to an arbitration, the guide will use the GDPR as an example of the types of rules that may be imposed. It will offer an overview of the regulatory framework, followed by an explanation of how data protection obligations may impact both the individuals involved in arbitration and the arbitral process itself.

The ICCA-IBA Joint Task Force on Data Protection in International Arbitration Proceedings is chaired by Kathleen Paisley (Ambos Law, Brussels, New York and London) on behalf of ICCA, and Melanie van Leeuwen (Derains & Gharavi, Paris) on behalf of the IBA. Members include Lawrence Akka QC (20 Essex Street), Rosa Barcelo (Squire Patton Boggs), Niuscha Bassiri (Hanotiau & van den Berg), Lisa Bingham (ICCA), Markus Burianski (White & Case), Hugh Carlson (Three Crowns), Daniel Cooper (Covington & Burling LLP), Javier Fernandez-Samaniego (Samaniego Law), Hilary Heilbron QC (Brick Court Chambers), Robert Maddox (Debevoise & Plimpton), Charlie Morgan (Herbert Smith Freehills LLP), Philippe Pinsolle (Quinn Emanuel Urquhart & Sullivan LLP) and Jacques de Werra (University of Geneva).

• *A draft guide for public comment will be available soon. See www.arbitration-icca.org/news/2019/418/icca-and-iba-establish-task-force-on-data-protection.html*

Poland's new GDPR-style law

The government has introduced sectoral legislation. **Elzbieta Slazyk** reports from Poland.

Poland was one of the first EU Member States which implemented new domestic data protection legislation before the GDPR entered into force on 25 May 2018 (*PL&B International Report* 153).

Poland's Data Protection Act (Polish DP Act) was adopted on 10 May 2018 and published in the Official Gazette on 24 May 2018. The Polish government made use of the GDPR derogations and the Polish DP Act differs slightly from other EU Member States.

The Polish DP Act provides for criminal penalties in two situations:

- when anyone processes personal data without being authorised to process the data;
- when preventing the Personal Data Protection Office from carrying out an inspection.

These breaches can be subject to fine or even imprisonment for up to two years.

A data controller is obliged to nominate staff who are allowed to process personal data. For example, the finance department is not authorised to process the personal data in the HR department. Best practice to demonstrate compliance is a written form of authorisation and maintaining a register of the authorised staff.

After 25 May 2018, one of the challenges was the application of Polish regulations to the GDPR. Due to uncertainty of interpreting some laws, the Polish government was working on standardization of Sectoral Acts in line with GDPR requirements.

The Ministry of Digital Affairs, in charge of coordinating the Act on Changes to the Sectoral Acts, has emphasised that Poland is one of the first EU countries preparing such comprehensive regulations. The draft of the Act on Changes to the Sectoral Acts relates to 168 other acts, e.g. the financial services sector, sport and tourism, culture and national heritage, health protection (including access to medical records), internal affairs and administration, environmental protection, education, investment and development, science, entrepreneurship and technology. The draft regulates, for instance, conditions for the processing of employees' personal data by employers, and the type of data to be processed.

It also includes a proposal to amend the Penal Code, aimed at penalizing attempts at fraudulent conduct under the pretext of protecting personal data. Moreover, the draft includes important changes to the banking and insurance sectors in terms of profiling. The Act assumes that insurance companies will be able to make decisions based only on automated data processing of data, including profiling, with regard to risk assessment processes when concluding insurance contracts and settling claims. This means that a decision that is based solely on automated processing, including profiling, can be made without the consent of the data subject. A similar regulation presupposes an amendment to the banking law. However, for both sectors, the requirement was introduced to provide a data subject with the right to challenge such a decision, express their own views and invite employee intervention.[1]

On 21 February 2019, all Members of Parliament voted for sectoral changes. Currently, this proposal is with the Senate, before commencing the final stages of the Parliamentary process.

Poland's Labour Law previously stated that processing criminal records was allowed only when required by law for specific roles such as a teacher or policeman, and lawyers. In May 2018, a bill on rules for obtaining information on criminal records of job candidates and employees in the financial sector was adopted by the Polish Parliament. Employers in the financial sector are now entitled to process information about convictions and offences of job candidates and employees. Non-financial businesses are not entitled to process this information. The Act on Changes to Sectoral Acts determined that the employer is eligible to collect data of job candidates and employees in accordance with the Labour Code. If the employer would like to collect more data directly from candidates and employees, consent is required. Consent in not needed for processing of personal data relating to criminal convictions and offences.

Polish Supervisory Authority

In October 2018, Dr. Edyta Bielak-Jomaa, President of Poland's Supervisory Authority wrote a letter summarizing the first half of the year applying the new data protection regulations. She said that in the previous six months, problems with the application of the new law were sometimes even absurd, and these practices caused by the fear of high fines have focused the public attention in a special way. Meanwhile, in their shadow, both entrepreneurs and public administration as well as all other entities obliged to apply the GDPR introduced many valuable solutions which promote better protection of personal data.[2]

GIODO, Poland's Supervisory Authority, has issued some guidelines for businesses and organizations. For instance, GIODO requires a Data Protection Impact Assessment (DPIA) for whistleblowing. The criteria include the carrying out of the DPIA for whistleblowing when the processing of data concerns persons "whose assessment and the services they provide depend on entities or persons which have authoritative and/or assessment-related powers". The Polish Supervisory Authority gives an example of systems for reporting irregularities (for example, related to corruption) - in particular when employees' data are processed by such systems.

In January, GIODO clarified how to transfer personal data from Poland to the UK in the case of a Brexit "no-deal" scenario and launched consultations regarding standard clauses for a data processing agreement.

In accordance with the annual plan of audits and investigations approved by GIODO's President, in 2019 the

Polish Supervisory Authority is going to investigate the processing of personal data in the following sectors and areas:

- telemarketing;
- profiling in the banking and insurance sector;
- monitoring systems; and
- recruitment.

GIODO will also control public sector data processing by maintaining records of processing activities and documenting data breaches by data controllers. The Supervisory Authority will also take a look at such entities as: the Police, Border Guards and detention centres, checking their use of technical and organizational measures aimed at preventing unauthorized access, copying, changing or deleting data. Scheduled inspections are prompted by numerous factors (including complaints, questions and reports of violations of personal data protection) indicating an increased level of threat to the protection of personal data.[3]

Bielak-Jomaa also said during one of her interviews that there has never been and there will never be any security system, which would completely stop data leaks. If data breaches take place, the Polish Supervisory Authority will investigate what data has leaked and how. GIODO will assess how organisations cooperate in clarifying the case after breach notification. If, according to the principle of accountability, the organisation shows that it has done everything possible to secure the data, and yet the leak has occurred, the inspector will take this into account. If the violation is not at a large scale, it will not have to impose a penalty. However, if the organisation misleads the authority, hides the leak of sensitive data and/or the breach was repeated, the penalty will be painfully large to avoid similar situations in the future.[4]

Statistics in Poland

The Panoptykon Foundation was established in Poland in 2009 by a group of lawyers to express their opposition to surveillance. Their mission is to protect fundamental rights and freedoms in the context of fast-changing technologies and growing surveillance.[5]

The Panoptykon Foundation presented statistical data related to the total number of complaints and the total number of data breach notifications received by the Polish Supervisory Authority in October 2018 and January 2019.

Figures gathered by Panoptykon Foundation for a period of time 25 May – 25 November 2018 are as follows:

- 4,068 complaints were submitted by individuals;
- 1,800 data breaches were notified by business and other organizations.[6]

Comparing figures from 25 September 2018, when 2,833 complaints were submitted to the Polish Supervisory Authority, the number of complaints have increased rapidly. It shows that GDPR awareness in Poland is significant, and businesses, other organisations as well as individuals treat GDPR requirements and rights very seriously.

INFORMATION

Since the article was written, the Sectoral Act was signed into law on 4 April and will enter into force 14 days after publication in the Official Journal. The new President of the Polish DPA, Jan Nowak, was appointed at the end of March and started his term on 12 April.

AUTHOR

Elzbieta Slazyk is an Attorney-at-law in Poland.
Email: elzbieta.slazyk@gmail.com

REFERENCES

1 gdpr.pl/rzad-przyjal-projekt-nowelizacji-168-ustaw-dostosowujacje-do-zapisow-rodo
2 uodo.gov.pl/pl/138/679
3 uodo.gov.pl/pl/138/679
4 www.rp.pl/Kadry/310229977-Edyta-Bielak-Jomaa-o-RODO-Kary-beda-surowe-i-dotkliwe—jako-ostrzezenie.html
5 en.panoptykon.org/about
6 www.gdprtoday.org/gdpr-in-numbers-3/

Poland imposes €220,000 GDPR fine

Poland's Data Protection Authority has imposed its first GDPR fine (around €220,000) for a failure to fulfil the GDPR's information obligation.

Piotr Drobek, Director of the Analysis and Strategy Department, explained that the company in question (not named) did not meet the information obligation in relation to over six million people. Out of about 90,000 people who were informed about the processing by the company, more than 12,000 objected to the processing of their data. The controller should have informed individuals about the collection of data, the source of their data, the purpose and the period of the planned data processing, as well as data subjects' rights under the GDPR.

The company made representations claiming it was too expensive to send everyone registered mail. The DPA found that the infringement was intentional. When imposing the fine, the authority also took into account the fact that the controller did not try to rectify the situation.

Commenting on the decision, Izabela Kowalczuk-Pakuła, Partner at law firm Bird & Bird, said in her blog: "The decision will impact data brokers, data aggregators, banks (for Know Your Customer, KYC, purposes*), recruitment agencies (short/long list services, market research services), and their clients and any other data controllers that collect data from public sources. They may decide to change their business model to shape the service to be a processor more than a controller. However, their clients that use the data broker service, if they are considered as a data controller, should also consider notifying sole traders. As a result, we will have more privacy notices in our mail boxes and in our SMS boxes."

"We believe that there are strong arguments to say that spending so much money to send the information notice should be considered as a disproportionate effort."

- *See edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_en*

*A requirement in the securities industry.

CPDP 2019: GDPR's effects are felt far and wide

The EU is considering the possibility of legislating for Artificial Intelligence. **Laura Linkomies** reports on this and other GDPR-related topics from Brussels.

"Is the GDPR the panacea for all the legal issues arising from an increasingly data-driven world?" asked *Paul de Hert*, Professor at Vrije Universiteit Brussels, one of the organisers of the CPDP conference in Brussels in January. The programme certainly covered many aspects where GDPR's influence is felt, from cross border access and adequacy to class action and the GDPR's global impact.

Karolina Mojzesowicz, Deputy Head, Data Protection Unit at the European Commission, said that the EU Commission is now considering whether additional legislation is needed for Artificial Intelligence (AI). The EU Commission wants to consider all fundamental rights together. GDPR only addresses personal data. Freedom of expression and non-discrimination are other aspects to take into account, she said.

A high-level expert group met twice in January to discuss the issues. Any AI regulation must be flexible enough to provide for innovation and to protect data protection rights at the same time, Mojzesowicz said.

"We are assessing whether national and EU frameworks are fit for purpose for the new challenges. By mid-2019 we will publish a report on the gaps identified in AI. The expert group has worked on the guidelines which are now under consultation[1]."

Member States think that the guidelines should be more useable and practical. Perhaps a different instrument should be considered for public and private sector uses of AI. Another challenge is how big a margin of error is acceptable in automated decisions and machine learning.

Stakeholder views on AI

Pierre-Emmanuel Mazaré, a research engineering manager at Facebook Artificial Intelligence Research, in charge of the engineering aspects for Paris-based AI research projects ranging from chatbots to computer vision, spoke about artificial intelligence and machine learning. He is involved in developing ethical guidelines for AI as a member of the EU expert group. "This is a very challenging topic. Which kind of AI goes too far in discriminating, for example? Under what circumstances does it breach fundamental rights?"

"Europe recognises privacy as a fundamental right, but other countries do not necessarily have this view. For example, in the US privacy sits with intellectual property rights in legal terms."

"The EU should now look at the nuances; how can companies demonstrate that they have ethical principles, and what are the consequences of non-compliance?"

He thought that the EU has in mind a self-regulatory scheme for AI. However, it will be challenging to understand what kind of principles will eventually be mandatory. The EU strategy 2030 is about sustainability. "I hope the EU will be able to present a clear policy for AI. It would be great to establish EU AI as the most sustainable in the world."

Frederike Kaltheuner of Privacy International said that the discussion on automated decision-making urgently needs to address profiling. What is the role of AI in advertising? Civil society has been active on hate speech. It is difficult to define, however. Should companies engage with it? How does a global company define race locally, or sexual orientation?

Professor *Dr Christoph Lütge*, who is Director of the new 'TUM Institute for Ethics in Artificial Intelligence' at the Technical University of Munich, and holds The Peter Löscher Chair of Business Ethics and Global Governance at the same university (which will be supported by Facebook with US$ 7.5 million) said that we need to address the fears that are gaining currency among the population, even if we cannot solve them now. Otherwise this technology will not gain acceptance. "We are setting up an institute for AI with interdisciplinary research for ethical guidelines in AI," he said.

Between the two Commissions

One of the most interesting sessions of the conference was a dialogue with *Bruno Gencarelli*, who heads the international data flows and protection unit at the European Commission, and Ireland's Data Protection Commissioner, *Helen Dixon*.

When asked what has been the biggest surprise with regard to the GDPR, Dixon said that, on the pleasant side, the huge reaction to awareness campaigns, and enthusiasm. A downside has been the confusion about how data protection principles apply in the real world.

Gencarelli said that the European Data Protection Board (EDPB) is now dealing with cross-border cases. There have been changes to the governance framework but the system is working well. Less positive is the over-reaction by some stakeholders, and over-compliance. There is never enough education, but privacy is finally taken seriously.

He said that the DPAs have now issued 16-18 guidelines. The consultation on the GDPR's territorial reach has just ended. Gencarelli said that more information is needed (from the Commission) as certain legal advisers have been a bit excessive and created confusion in the first few months. He commented that the "risk-based approach is not understood well enough. We need to report by 2020 how the GDPR is working. In June 2019, one year since GDPR entered into force, the Commission will organize an event to take stock."

Dixon reported a large increase in

complaints. The quality of data breach reporting is improving. At the end of January, the DPA had received 4,000 notifications. Although there is a certain amount of over-notification, this is a good educational opportunity. Not every breach needs to be notified.

She also said that regulating specific sectors is a challenge, for example in the adtech sector. The rigidity of controller/processor roles is challenging. Guidance is needed on Subject Access Requests and their use, for example by disgruntled ex-employees. Proportionality of search does apply but there are no certain limits until we have case law in this area.

Gencarelli was asked about the recent Japan adequacy decision and which country would come next. He said: "These are not the Olympics! The Japan decision is very important as it shows how much more convergence we have in privacy than was the case just a few years ago. We are now able to have an arrangement in place that is much more comprehensive. Japan's system on international transfers is similar to ours, they also have an adequacy tool, so it is a mutual tool."

Could this mutual decision be a way forward for other countries? It depends on what the other system provides for, Gencarelli said. "If one of the tools is adequacy, we are ready to study adequacy also from their side. We can explore that possibility."

Dixon said that Ireland has started a consultation on children's data, as the GDPR does not give ideas on what the safeguards for children should be. "We have seen a range of issues come up, for example, how children can exercise their rights without parental consent. The age limit is 16 in Ireland. But how do Internet platforms verify age? How do you know it is a parent who is giving approval? There are no definitive answers. We are engaging with every school in Ireland to reach a sophisticated understanding on this."

Defending the GDPR – one year on

Moderating the session, *Ruth Boardman*, Partner at law firm Bird & Bird said that we do not want the Cambridge Analytica method used on European territory. "We need to differentiate between consumers and citizens. There is a difference. If marketing online is being used to sell products, it is not the same thing as using private information to target political advertisements to people. This is a very dangerous development which was used in the UK Brexit referendum campaign – with more and more evidence coming to light."

Marit Hansen, Privacy Commissioner Schleswig-Holstein, Germany, said that it would have been ideal to have had a European consensus earlier on implementation. As a result of the GDPR, many controllers have changed their data processing. Companies have improved their housekeeping as they been forced to audit and delete data.

Michal Boni, MEP, said that he had some concerns on 'defending' the GDPR. "We need to promote the GDPR. Criticism is often based on ignorance."

GDPR's influence in Africa

Half of African countries have now legislated in data protection, a CPDP panel revealed. What is behind this trend, apart from the GDPR? *Patricia Poku*, Data Protection Commissioner of Ghana, said that although much progress has been made, many challenges remain, not least due to the vast cultural differences and language barriers between African countries. Africa is a very large continent so bringing all countries together is a big task. But work at the African Union brings countries together. In 2014 it adopted a convention on E-commerce, cybersecurity and personal data protection. Africa may need to define its own approach that is separate from the GDPR, Poku said. In June 2019 Ghana's DPA will organise the first African DP conference to discuss these issues.

Sophie Kwasny, Head of Data Protection at the Council of Europe discussed the relevance of Convention 108 for Africa. As accession is open for non-member states, Cape Verde, Senegal and Tunisia have already acceded, with Burkina Faso and Morocco pending, as well as Gabon and Ghana from the observer countries. As Convention 108 is often seen as the first step towards adequacy, it has much relevance outside Europe.

Estelle Masse of Access Now, a civil society group focusing on privacy and based in Brussels, talked about the role of civil society in Africa: they represent peoples' rights and have a role in oversight of accountability. "We talk to people about the importance of privacy, and try to raise a public debate, also raise awareness in institutional bodies. We provide technical support but no legal representation. We denounce violations when we see that European companies do not offer the same protections to African users as European users. Our role is also to highlight problems."

Lahoussine Anis, Secretary General at Morocco's Data Protection Authority said that there is DP legislation now in 23 African countries with drafts in another seven countries. He said that in 2016, the African Network of Data Protection Authorities was created. Current members include Mali, Senegal, Cape Verde, Ghana, Burkina Faso, Tunisia, Ivory Coast, Benin, and Morocco. The action plan is to promote privacy and data protection in Africa, develop cooperation and synergy between African DPAs, enhance visibility of the network internationally and set up channels of communication/cooperation with African institutions. But DPAs lack resources, and people have a wrong perception of data protection as a barrier rather than a facilitator to the use of ICT. In addition, there is lack of cooperation among stakeholders, which work in silos.

Boris Wojtan, Director of Privacy at GSMA which represents the interests of mobile operators worldwide, spoke about his organisation's work in Africa. "We are engaging more with Africa, for example, we produced a report on the digital economy, data privacy and mobile money. Mobile money is an African invention which started in Kenya, and is used in 90 countries now. It is very empowering for individuals. Our members are supportive of data privacy rules, but there are challenges. First of all, the rules need to be the right kind, not too prescriptive. We need the positive elements from the GDPR to embrace accountability. Africa is culturally very diverse. Now DPAs have a crucial role in describing the intended direction of travel. Should it be the GDPR? But it is only one source for data protection rules. There is also

Convention 108. We need a holistic view on Africa."

Data protection in Islamic countries

For the first time ever, I heard a panel address Islamic legal conceptions of privacy. *Nighat Dad* of the Digital Rights Foundation, a Pakistani human rights lawyer, said that there is a lack of a personal data protection law, but the right to privacy is mentioned in the constitution. The privacy of home is stressed, which ties into cultural concepts and language. Once a woman leaves home, she is offered less protection. Lawyers shy away from domestic violence cases saying it is a domestic matter. In rape cases women are blamed if they have not covered up. No law can be adopted without approaching the Islamic Council, even when already passed by parliament.

Lahoussine Aniss, Secretary General of the Moroccan DPA said that the topic is very challenging. Privacy is a moral and ethical value, and these are very central to Muslim life.

Sonny Zulhuda, Associate Professor at International Islamic University, Malaysia, said that the Koran has a very general statement about privacy – it rules against unjust exploitation of others. The Koran gives guidelines for parents to educate children to respect others – for instance, there is a domestic rule about not entering the parents' bedroom, so there is clear guidance on privacy. There are also mentions of protection of reputation, honour and dignity.

Protecting privacy in Islam is about respecting dignity and honour, and avoiding unnecessary naming and labelling, she said.

Patrick Penninckx, Head of Department - Information Society at Council of Europe said that Muslim countries are very diverse. There are not only countries with a Muslim majority but also the countries in Europe which have a large Muslim minority. Convention 108 is very influential and is open to any country in the world with DP legislation. A number of countries with a Muslim majority, such as Albania, Bosnia and Turkey have already ratified it. Observers include countries such as Abu Dhabi and Indonesia.

Are religious beliefs sensitive data in Islam? What about data regarding sexual life? The Moroccan legislation makes an exception for special category of data, and does not include sexual orientation/life. Another aspect is Sharia law, a religious law forming part of the Islamic tradition. The UK has many Sharia councils. "To what extent does this interfere with data protection legislation?" he asked.

Zulhuda said that many laws are inspired by rules from Sharia law. But Malaysia has its own legal system, and laws adopted by parliament. Any inconsistency in law with Sharia law does not give a way for people to challenge it in the courts.

Class action under the GDPR – the state of play

The possibility for representative action is a new element in European data protection law, although Member States differ in their approach. In some Member States, it is possible to sue for compensation and many civil society organisations help individuals in this area. A CPDP panel approached the issue of collective redress from the angle of civil society.

Maryant Fernandez Perez of the European Consumer Organisation, BEUC, said that the large majority of people do not seek compensation individually because it is difficult. There are now several class actions against Facebook in different countries. NGOs like BEUC can bring a complaint to the DPA on behalf of individuals.

"Under the GDPR it is possible to gain compensation for both material and non-material damages. But this depends on whether the individual Member State allows for that, and individuals give a mandate. Workable redress is available only in a few Member States. Currently, we have an EU proposal for a directive on representative action. BEUC has several demands there. We want a binding instrument at EU level, a directive that covers immaterial and material damages, introduces the 'loser pays principle', allows for collective action without a mandate, etc."

Karolina Iwanska, of Panoptykon Foundation spoke about the role of civil society in Poland.

NGOs can represent data subjects and join ongoing procedures as a third party, but they cannot act without individuals' mandates. Polish procedural law, however, says that NGOs can issue cases on behalf of individuals. So there is a conflict with DP law. There is no collective action in the sense that in the administrative courts, an individual has to be involved. NGOs cannot act in civil courts. Panoptykon therefore mostly engages in strategic litigation. "We choose priorities. When it comes to collective action, it enables individuals to feel empowered and also creates pressure for DPAs to act faster. It changes the status quo by changing bad practices," she said.

Nick McAleenan, a Partner at JMW solicitors in the UK said that Article 80 in the new 2018 UK Data Protection Act allows for class action. DP Act 2018, Section 187 on 'Representation of data subjects with their authority' replicates GDPR's Article 80.1. The government should provide regulation of collective action, he said. In 30 months' time, the government will reflect whether GDPR Art 80.2 will be implemented (so that any organisation, association or body may act independently of a data subject's mandate) – but there is not much political appetite there, he thought.

INFORMATION

The CDPD Conference took place 30 January – 1 February in Brussels, see www.CDPDconferences.org

REFERENCES

1 The consultation closed on 1 February. See ec.europa.eu/digital-single-market/en/news/have-your-say-european-expert-group-seeks-feedback-draft-ethics-guidelines-trustworthy
The Expert Group issued the Guidelines for Trustworthy AI on 8 April.

Nigeria regulates data privacy: African and global significance

This newly adopted law includes many of the GDPR's features, but fails on data transfer provisions. By **Graham Greenleaf**.

The regulation of data privacy by Nigeria, the most populous country in Africa and the seventh in the world (population of 186 million), is an event of significance in the evolution of the world's data privacy laws. Other factors also make Nigeria significant for privacy: it has Africa's largest economy, overtaking South Africa in 2014; as an officially English-speaking country, it will help open up a broader discussion of data protection in a continent dominated by francophone progress (South Africa's developments having been moribund as yet); and as a country with roughly equal Muslim and Christian populations, it joins Indonesia, Turkey and Malaysia as major Muslim countries with data privacy laws.

The Nigerian Information Technology Development Agency (NITDA) issued the Nigerian Data Protection Regulation 2019 (the Regulation)[1] on 25 January 2019, coming into effect immediately upon issue (Preamble). The Regulation is made pursuant to the Nigerian Information Technology Development Agency Act of 2007 (NITDA Act). Although the Act makes it a function of NITDA to "develop guidelines for electronic governance" (and so on) (art. 6(c)), and to "make such regulations as in its opinion are necessary or expedient for giving full effect to the provisions of the Act" (art. 32), it does not say, unlike the Preamble to the Regulation that the Act authorizes it to "develop regulations for electronic governance". There is therefore perhaps some doubt as to whether the Regulation is *ultra vires*, but this article proceeds on the assumption that it is valid.

Previous Guidelines on Data Protection 2013, issued by NITDA, did not qualify as a data protection law, both because of deficiencies of content, and lack of enforceability. The Regulation of 2019 does not share these deficiencies. The Regulation may eventually be replaced by a stand-alone primary law. The Digital Rights and Freedom Bill, which passed both houses of the Nigerian Parliament in 2018, has in March 2019 been refused signature by newly re-elected President Buhari, on the grounds that it covered too many subject-matters in too little detail, and overlapping other pending Bills.[2] At least for now, this Regulation under the NITDA Act is Nigeria's first data privacy law, and is very detailed on data protection compared with that Bill. This article will identify the main features of the Regulation, emphasising its similarities to and differences from the European Union's General Data Protection Regulation (GDPR).

Nigeria's regional obligations

Nigeria is the 26th African country to regulate data privacy (of 54 African Union member states), and the 134th in the world. It is not yet a signatory to the African Union's data protection Convention.[3] However, as a party to the treaty establishing the Economic Community of West African States (ECOWAS), it is bound by the Supplementary Act on Personal Data Protection Within ECOWAS (2010), the only binding data protection agreement in force in Africa. The Regulation may make Nigeria the tenth of 15 ECOWAS states to comply with that obligation, though issues arise concerning full compliance (discussed below).

> The 'outsourcing exemption' should be a fatal defect in relation to EU adequacy, which is odd for a law clearly intended to emulate many aspects of GDPR.

Scope of Regulation

The scope of the Regulation is the same as for the GDPR on most important issues: the definitions of "data subject"; "personal data" (both in terms of "identifiability"); "data controller" (and "data administrator" to mean the same as "data processor") are all familiar from the GDPR. "Sensitive personal data" includes "any other sensitive personal information", and so is probably broad enough to include biometric and genetic information.

The Regulation "applies to all transactions intended for the processing of Personal Data," (cl. 1.2(a)), and thus to the whole of the private and public sectors, as confirmed in the Preamble. Such transactions are stated to be "in respect of natural persons in Nigeria". The Regulation also applies to persons "residing outside Nigeria who are citizens of Nigeria" (cl. 1.2(b)), but this might be read to apply only when the processing concerned takes place in Nigeria. Unlike the GDPR, there is no application to extra-territorial processing targeting Nigerian residents.

The Regulation also has no application to processing concerning foreign non-residents of Nigeria, even if it takes place within Nigeria. Nigeria's law will therefore not apply at all to personal data transferred to Nigeria from overseas, including from the EU. This "outsourcing exemption" should be a fatal defect in relation to EU adequacy, which is odd for a law which is otherwise clearly intended to emulate many aspects of the GDPR, and means that transfers from the EU to Nigeria for outsourced processing will need to have other "appropriate safeguards" or applicable exceptions.

Enforcement and administration

The Regulation designates the NITDA as "the Agency" to administer the Regulation (cl. 1.3(xxvi)), and gives it various powers, for example to licence Data Protection Compliance Organisations, to receive audit information, to make adequacy decisions in relation to foreign countries, and to develop and manage international cooperation mechanisms (art. 4.3). It therefore appears that NITDA is the data protection authority (DPA) for Nigeria.

NITDA is not independent, because the Minister may give it general directions concerning the carrying out of its functions (NITDA Act 2007, art. 27). This is not consistent with the ECOWAS Supplementary Act requirement of an independent DPA.

In relation to civil remedies such as compensation, NITDA is to establish an Administrative Redress Panel to investigate allegations of breach of the Regulation, issue administrative orders pending the outcome of investigations, and determination of appropriate redress, with breaches of the Regulation being construed as breaches of the NITDA Act (cl. 4.2). Individuals also retain their right to "seek redress in a court of competent jurisdiction" (cl. 4.2(1)). It is not clear from the NITDA Act that breaches of the NITDA Act could result in such redress.

Data controllers (but not data administrators/processors) are also liable for fines for breaches ("in addition to any other criminal liability"). If they deal with more than 10,000 data subjects annually, the fine is 2% of "annual gross revenue" (presumably domestic, not global), or 10M Nigerian Niara (about US$27,500), whichever is greater. For controllers dealing with fewer than 10,000 data subjects annually, the fine is 1% or US$5,500. Unless very robust assessments of annual gross revenue are made, these fines are unlikely to be major deterrents.

The Regulation establishes a compliance oversight system under NITDA control (cl. 4.1):

- All controllers must publish, within three months, data protection policies complying with the Regulation;
- Each controller must designate a Data Protection Officer (DPO) to ensure compliance, but the data controller may "outsource data protection to a verifiably competent firm or person";
- All controllers must conduct "a detailed audit of its privacy and data protection practices" (with minimum details specified) within six months, and provide a summary to NITDA, and annually thereafter (depending on the number of data subjects);
- NITDA will register, licence and regulate Data Protection Compliance Organisations (DPCOs) who shall, "on behalf of' NITDA", monitor, audit, and train all controllers, as well as advise on compliance.

It is not clear whether a DPCO can also be an outsourced DPO, and whether licensed DPCOs have a monopoly on compiling and submitting audits. There is considerable potential for conflicts of interests in these arrangements. Both the AU Convention and the ECOWAS Supplementary Act envisage some formalities of at least DPA notification of processing. This may be the reason why the Regulation does so even though the GDPR does not, although the above requirements could also be seen as consistent with an extensive version of the GDPR's Data Protection Impact Assessment (DPIA) requirements.

Controller obligations

The requirement of "lawful processing" is central, as with the GDPR, but the ground of processing to protect the legitimate interests of a controller is absent (cl. 2.2). Other fundamental obligations include data quality, storage limitation and security, the existence of a duty of care on anyone entrusted with personal data, and accountability for compliance with 'the principles contained' in the Regulation (cl. 2.1). These give a basis for enforcement.

Almost all aspects of the GDPR's stronger approach to consent are present, either in the definition of "consent", or the detailed restrictions on obtaining it (cl. 2.3). A strong element is the high level of obligations and liability that data controllers have for the data 'administrators' (processors) that they choose, including a due-diligence-like obligation to check their record in previous handling of personal data (cl. 2.4). Written contracts requiring adherence to the Regulation are required (cl. 2.7).

Data subject rights

Many GDPR-like data subject rights are provided, including (cl. 3.1) notice of:

- Transparency when providing access to data subjects;
- Detailed notice prior to collection of personal data (cl. 3.1(7)), including
  - Existence of automated data processing, with "meaningful information about the logic involved";
  - Intent of processing for purposes other than that for which the data are collected (side-stepping the otherwise apparently strict limits in cl. 2.1(1)(a));
  - Whether an intended transfer to a foreign country is to one where the NITDA has made an adequacy decision (but only the right to be informed of any safeguards to be adopted, not automatic notice);
- Correction and supplementation, with advice to previous recipients (cl. 3.1(8), (13));
- Deletion / "right to be forgotten" in similar terms to the GDPR (cl. 3.1(9)-(10), (13);
- Restrictions on processing, also in similar terms to the GDPR (cl. 3.1(11)-(12));
- Data portability (cl. 3.1(14)-(15)).

Other provisions also create rights for data subjects, including to opt-out of processing for marketing and other purposes (cl. 2.8).

Data transfers

The NITDA decides whether a foreign country "ensures an adequate level of protection", but this is subject to the "supervision" of the Attorney-General, who is to take into consideration much the same factors as are stated in GDPR art. 45 (cl. 2.11). It is also implied that the Attorney-General can make such decisions independently of NITDA. If no positive decision concerning adequacy has been made, exceptions allow transfers on various grounds (cl. 2.12), similar to GDPR art. 49 derogations. There are no "appropriate safeguards" as alternatives (BCRs etc).

Conclusions

This law has more common features with the GDPR than most of the other 23 data privacy laws in Africa. However, it has many significant limitations. Its validity is questionable. A major deficiency is that it does not provide any protection to foreign-sourced data processed in Nigeria. Its enforcement measures might not be a significant deterrent to breaches of its principles. Its provisions for Compliance Organisations could result in conflicts of interest. This Regulation may not be Nigeria's final data privacy law, but it is a notable step in that direction, and because of the importance of Nigeria, a significant step for Africa.

INFORMATION

Bertil Cottier provided valuable information, but responsibility for all content remains with the author.

REFERENCES

1 Nigerian Data Protection Regulation 2019
2 'Buhari declines assent to Digital Rights and Freedom Bill, four others' *The Guardian* (Nigeria) 20 March 2019 guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/
3 African Union Convention on Cyber-security and Personal Data Protection, open for signature in 2014.

Serbia enacts new data protection law

GDPR-style law enters into force in August 2019. By **Goran Radošević**, **Sanja Spasenović**, and **Milica Filipović** of Karanovic & Partners, Serbia.

Serbia enacted a new Data Protection Law on 9 November 2018 to follow the EU GDPR, with its applicability postponed until 21 August 2019. The new law was long-awaited: it has been ten years since the existing law was passed; a law that even at that moment was already outdated (for example, it recognized only consent in written form and almost completely restricted data transfers to non-European countries).

The new law is a copy of the GDPR to a large extent – perhaps too large, as the critics of the new law (including the Serbian Data Protection Authority, DPA) argued that implementation of the GDPR was performed badly, without the much-needed harmonization with Serbia's legal framework. In addition, the GDPR's recitals (all 173 of them) were not copied or otherwise implemented in the new law, potentially creating a number of issues in its future interpretation. The new law also failed to regulate certain important data protection aspects, such as video surveillance, which are regulated in the EU via other community and national pieces of legislation.

That being said, the new law undoubtedly marks a revolution in the way personal data should be handled in Serbia, similarly to what GDPR did for the EU – and perhaps even more so, since the EU's previous data protection framework was far less outdated than that of Serbia. It is therefore expected that Serbian companies will have to adjust many of their operations, not just legal but also technical and organizational ones, in order to prepare for the comprehensive changes that will be introduced in a few months.

Some of the most important changes are summarised below.

The scope of the new law

The new law will not apply only to the processing of data carried out by Serbian controllers and processors, but also to the controllers based outside Serbia if their processing activities relate to the offering of goods or services (even for free) or monitoring the behaviour of Serbian data subjects within Serbia. For example, a company outside of Serbia targeting consumers in Serbia will be subject to the new law, which was not the case so far. As a result, a number of these controllers and processors will need to appoint their representatives in Serbia, to be addressed by the DPA and the data subjects on all issues related to processing.

Consent: New forms and stricter requirements

Compared with the existing law, which recognizes only consent in written form - creating significant issues in the digital age – the new law explicitly introduces other forms as well, such as online and oral consent, or consent by other clear affirmative action, provided that the controller is able to demonstrate that the data subject has indeed consented.

On the other hand, the conditions for obtaining consent have become much stricter – it must be freely given, specific, informed and unambiguous. For example, there is a presumption that consent will not be valid unless separate consents are obtained for different processing operations, where appropriate. In addition, the request for consent – when presented in a written document – must be clearly distinguishable from all other matters, using clear and plain language. Catch-all clauses will not be valid. In addition, consent will not be considered freely given if the performance of a contract is conditional on the consent to the processing of personal data that is not necessary for its performance.

Consent is not the only legal ground for data processing – others exist as well, such as the performance of the contract, compliance with legal obligations or processing necessary for legitimate interests, and will in fact be used much more often than consent.

New and expanded data subjects' rights

The new law significantly expands the existing right of individuals to receive information about the processing of and access to their personal data. Data controllers must provide transparent information to data subjects in a more comprehensive manner, and in particular must inform data subjects of certain rights – such as the ability to withdraw consent, and the period for which the data will be stored. The information needs to be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language. However, this will be hard to achieve given the fact that the elements that need to be included in the information are quite excessive, which should be carefully addressed by companies when analysing and updating their existing information notices.

In addition, the new law introduces a new right to data portability, and provides additional details concerning the erasure of personal data. The right to data portability gives individuals the right to demand that the controller provides them with their personal data, or to transmit data directly to another controller, in a machine readable format, if the relevant processing was automatic and based on consent or the fulfilment of a contract. The right to erasure binds the controller to erase the data without undue delay upon the individual's request if the personal data is no longer necessary for the purpose of processing, if there is no legal basis for processing - including cases where consent has been withdrawn, or if the data is otherwise processed contrary to the law, and even requires that the controller uses reasonable measures to notify other controllers processing the same data about the received erasure request.

Removal of obligation to register databases

One of the important changes under the new law is the removal of the existing obligation to register personal databases with the DPA, which was so far mostly ignored in Serbia. Under the new law, controllers and processors will only be required to maintain a record of processing internally and, in certain cases, even that obligation will not apply to companies with fewer than 250 employees. The maintenance of the Central Register of Databases, established under the existing law, has been terminated with immediate effect.

Data Protection Officer

The controllers and processors will be required to designate a data protection officer (DPO), whose primary tasks will be to ensure compliance with the data processing legislation and to communicate with the DPA and the data subjects on all data protection matters. This obligation applies if: (i) the processing is carried out by a public authority, (ii) the core activities of the controller/processor require the regular and systematic monitoring of data subjects on a large scale, or the large scale processing of special categories of personal data, for example, health data or trade union memberships, or criminal convictions/offences data.

The DPO may be employed or engaged under a service contract, and in any case must have sufficient expert knowledge. A group of companies may appoint a single data protection officer, provided that this person is equally accessible by each company.

The controllers and processors are required to ensure DPOs' independence in the performance of their tasks, meaning that no instructions may be given to them, that they report directly to the manager of the controller/processor and that they may not be dismissed or penalised for performing their tasks.

Accountability, security and Privacy by Design

Similarly to the GDPR, the new law introduces burdensome accountability obligations on data controllers, which are required to "demonstrate compliance". This includes their obligation to: (i) implement, maintain and update appropriate technical and organisational measures to ensure a level of security appropriate to the risk - taking into account the state of the art, the associated implementation costs etc., (ii) have in place certain documentation, such as data protection policies and records of processing activities, (iii) implement data protection by design and by default, and, (iv) conduct a data protection impact assessment for processing operations which are considered a higher level of risk to the rights and freedoms of individuals.

Data protection by design requires the controllers to adopt, as well as maintain and update when needed, appropriate measures - such as pseudonymisation, data minimisation, etc., which will integrate the safeguards necessary for processing. Data protection by default, on the other hand, requires the controllers to adopt measures so that only the processing which is necessary for the specific purpose will be possible (e.g. that, by default, privacy settings on one's social network profile do not make one's data public).

Liberalised data transfer concept

The data transfer regime has been completely revamped and liberalised under the new law, which is a much-welcomed change from the current overly restrictive concept which requires controllers to obtain prior approval from the DPA for transfers to non-European countries. The new law explicitly applies to both direct and indirect data transfers.

Under the new law, controllers will be entitled to transfer personal data abroad if one of the following conditions (amongst others) is met:

- personal data is to be transferred to a country that ratified the Council of Europe Convention 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data;
- data transfers are performed to a country included on the EU list or the Serbian Government's list of countries providing an adequate level of data protection;
- data transfers are performed to a country which has a bilateral agreement with Serbia regulating data transfers;
- the transfer is based on the standard contractual clauses prepared by the Serbian DPA;
- the transfer is based on Binding Corporate Rules or a code of conduct approved by the Serbian DPA, or on certificates issued in accordance with the new law;
- the Serbian DPA has issued a

specific approval for the transfer to be performed on the basis of an agreement between the data exporter and the data importer; and,
- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks.

This should enable many more options for the transfer of data to non-European countries, especially once the DPA prepares the standard contractual clauses – which should be based on the ones approved by the EU Commission. In addition, it is expected that the process of obtaining the DPA's approval for such transfers will be more efficient, and should be completed within 60 days – currently the procedure often lasts for more than one year.

Data breach notification duty: 72 hours

The new data breach notification obligations are a significant development as they previously existed only for controllers in specific sectors. Under the new law, data controllers will generally be required to document each data breach, as well as to notify the DPA of most of them, without undue delay and, when feasible, within 72 hours after becoming aware of the breach. In addition, data processors will have to notify the controllers of the breach without undue delay.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is also required to communicate the personal data breach to the concerned individual as well, without undue delay. However, this does not apply if the controller has implemented appropriate technical and organisational measures - e.g. encryption, which rendered the relevant data unintelligible to any unauthorised person, or if the notification would involve disproportionate effort, in which case a public communication or a similar measure must be made in order to properly inform the individuals.

Sanctions and enforcement

The new law is generally harmonised with the GDPR in almost all aspects, with certain local specifics, except with respect to sanctions – the maximum fines which may be imposed on companies are up to approximately €17,000, rather than GDPR's €20 million or 4% of the company's global annual turnover. As before, the DPA is authorised to issue warnings to data controllers and data processors, order the correction or deletion of the collected data, rectification of other detected irregularities etc., but is now also able to directly fine the controllers and processors in certain situations, with fines in the region of approximately €850 – currently, only the Court of Offences is entitled to impose fines.

However, formally speaking, under the Law on Administrative Procedure, the DPA is also authorised to enforce its orders by threatening the company with a fine of up to 10% of its annual income in Serbia, in case it fails to comply with the order. This is a relatively new option for Serbian authorities that has not yet been tested in practice, to the best of our knowledge.

What will the future bring?

Now, it is the controllers' and processors' turn: by summer 2019 they will have to ensure compliance of their data processing operations with the new law, which will not be a quick or easy task. At the same time, the DPA will also have a lot on its plate in order to prepare for the new law, especially with resolving a number of its ambiguities raised during the public debate, preparing the standard contractual clauses, and raising the public's awareness concerning the approaching data protection overhaul.

AUTHORS

Goran Radošević is Partner / Attorney at Law in cooperation with Karanović & Nikolić, Sanja Spasenović is Senior Associate / Attorney at Law in cooperation with Karanović & Nikolić (Serbia), Milica Filipović is Senior Associate / Attorney at Law in cooperation with Karanović & Nikolić (Serbia).
Emails:
goran.radosevic@karanovicpartners.com
sanja.spasenovic@karanovicpartners.com
milica.filipovic@karanovicpartners.com

INFORMATION

Serbia is not an EU Member State, but is a candidate country. The information in this document does not constitute legal advice on any particular matter and is provided for general informational purposes only.

Canada clarifies the concept of consent

The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioner of Alberta and British Columbia have jointly issued new guidance on obtaining meaningful consent. The guidance, inspired by the EU GDPR's new, higher consent requirement, provides practical measures regarding what organisations should do to ensure that they obtain meaningful consent.

The guidelines set out seven principles for a more transparent consent process. One of the suggestions is to consider the customer's perspective. Organisations may consider:
- Consulting with users and seeking their input when designing a consent process;
- Pilot testing or using focus groups to ensure individuals understand what they are consenting to;
- Involving user interaction/user experience (UI/UX) designers in the development of the consent process;
- Consulting with privacy experts and/or regulators when designing a consent process; and/or,
- Following an established 'best practice,' standard or other guideline in developing a consent process.

The Office of the Privacy Commissioner has applied these guidelines since 1 January 2019.

- *See www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#_determining*

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

"*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