University of New South Wales Law Research Series

GLOBAL DATA PRIVACY 2019: DPAS, PEAS, AND THEIR NETWORKS

GRAHAM GREENLEAF

(2019) 158 *Privacy Laws & Business International Report* 11
[2019] *UNSWLRS* 68

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

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

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*
(2019) 158 *Privacy Laws & Business International Report*, 11-14

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 eleven countries have so far failed to appoint a DPA, as required by their law, including: the Dutch Caribbean territories of Aruba, Curacao and Sint

* 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.

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.

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.

---

[5] Information Regulator (South Africa) < http://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 <https://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 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641772>

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 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 7 non-European), plus 14 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

[7] EDPB membership <https://edpb.europa.eu/about-edpb/about-edpb_en>

[8] Appointed from the APEC Privacy Sub-group 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.

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 thirteen 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

[10] RAPDP articles of association <http://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 < https://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 <https://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 <https://idpc.org.mt/en/Pages/dp/int/bidpa.aspx>

[17] AFAPDP <http://www.afapdp.org/>

[18] RedIPD, list of members < http://www.redipd.org/la_red/Miembros/index-iden-idphp.php >.

[19] CEEDPA <http://www.ceecprivacy.org/main.php>, meeting since 2001.

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 eleven 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 5 new members in 2017-18[22] (Cayman Islands, Turkey, Ukraine, Abu Dhabi (UAE), 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 eleven 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.

---

[20] Enforcement Cooperation Arrangement FAQs <https://icdppc.org/participation-in-the-conference/enforcement-cooperation-arrangement-faqs/>

[21] GPEN < https://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 <https://www.privacyenforcement.net/content/gpen-sweep-2017-international-enforcement-operation-finds-website-privacy-notices-are-too>

[24] For results, see <https://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-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 <http://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 <https://www.ucenet.org/member-organizations/>.

[29] DPAs that are UCENet members – Canada, Ireland, Spain, UK, US

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.

[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.