DATA PRIVACY AUTHORITIES (DPAS) 2017: GROWING SIGNIFICANCE OF GLOBAL NETWORKS

GRAHAM GREENLEAF

(2007) 146 *Privacy Laws & Business International Report*,14 [2017] *UNSWLRS* 44

UNSW Law
UNSW Sydney NSW 2052 Australia

Data privacy authorities (DPAs) 2017: Growing significance of global networks

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*
(2007) 146 *Privacy Laws & Business International Report*, 14-17

Data Protection Authorities (DPAs) and (as they are sometimes called) Privacy Enforcement Agencies (PEAs) have expanded in numbers and activity, including through their various networks, over the past two years. This article analyses the details of those network set out in the 2017 Global Tables of Data Privacy Laws (*Privacy Laws & Business International Report*, Issue 145, pp. 14-26). The last two columns of the Table identify the DPA/PEA, where one exists, in each of the 120 countries that now have data privacy laws, and each network of which they are a member. Background on the DPA/PEA associations discussed in this article can be obtained from the 2015 analysis.[1]

Deficiencies in DPA appointments

Before considering the growing networking and cooperation of DPAs, in relation to both policy and enforcement, it is necessary to consider that some legislation does not create a specialised, independent, DPA, or perhaps any DPA at all, or perhaps does so in theory but one has not been appointed.

The near-deserted 'Hall of Shame'

The DPA Hall of Shame is reserved for countries which, having undertaken in their data privacy legislation to appoint a data protection authority, fail to do for more than the year or so normally required to put a new Act into operation. They are DPAs 'missing in action'.

There are three important recent escapees from the Hall of Shame. The Philippines National Privacy Commission, which existing in theory their law was enacted in 2012, was finally appointed in mid-2016 by the outgoing President. It has moved rapidly to undertake its duties, such as by enacting the Act's Implementing Rules and Regulations, and by recommending prosecutions for major data breaches), and has become a member of international DPA organisations. It has also ignored attempts by the country's new and homicidal President to force its members to resign. South Africa's Information Regulator under its 2013 Act was finally appointed by the President in late 2016, and has also moved quickly to announce plans for the establishment of her office. Mali's DPA has also now been appointed under its 2013 Act, and has been very active since appointment. Another relatively recent African DPA appointment in is Ghana's Data Protection Commission,[2] whose activities include an annual public conference.

Other countries with new laws have promptly established DPAs, including the appointment of the final members of Turkey's Data Protection Authority in January 2017. Bermuda's

* The assistance of Marie Georges, Blair Stewart, Sophie Kwasny, Hannah McCausland, Alain Kapper and Pablo Palazzi, is gratefully acknowledged. Responsibility for all content remains with the author. Separate acknowledgments accompany the Tables.

[1] 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>

[2] Data Protection Commission (Ghana) < https://www.dataprotection.org.gh/>

legislation was only enacted in 2016, and that of Chad in 2015, so it is too early to consider the appointment of their DPAs overdue.

Unfortunately, a few countries are still in the Hall of Shame, with no appointments of DPAs under legislation which is at least four years old. In some cases it seems that the Acts have also not been brought into force. The government of the Seychelles is the worst offender, having not appointed a DPA – or brought its Act into force – since its enactment in 2003. The others, and the dates of their relevant legislation, are the Dutch Caribbean territories (Aruba, Curacao and Sint Maarten) with Acts since 2010 but Data Protection Committees not yet appointed, Angola (2011), and Nicaragua (2012). Angola is reported to be taking steps toward establishing its DPA. Perhaps 2017 will see the corridors of the Hall of Shame empty of occupants. All-in-all, countries have improved their record in timely appointment of DPAs in recent years.

Absence of a DPA, and non-independent DPAs

Twelve data privacy Acts don't provide for a specialised data protection authority at all, but leave data privacy enforcement up to other State institutions: Azerbaijan; Colombia; India; Indonesia; Kyrgyz Republic; Kazakhstan; Malawi; Paraguay; Qatar; St Vincent & Grenadines; Taiwan: and Vietnam. While such enforcement may sometimes be vigorous, the provision of a specialist DPA is generally regarded as essential for a first-class data privacy law.[3]

In a somewhat different category are Acts that 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, Singapore and Macau (the establishment law for its DPA has never been enacted). Singapore and Malaysia do not have public sector jurisdiction, which removes that conflict of interest. There is considerable evidence of independent action by at least Singapore and Macau's DPAs.

Conclusions

Only 10% of national laws do not create specialised DPAs. This is so in all Central Asian laws, common in the rest of Asia, and sometimes the case elsewhere, but never the case in Europe nor in Africa. In Africa there is too high an incidence of DPAs theoretically created but not appointed - this is rare elsewhere. Appointment of specialised DPAs explicitly subject to government control does occur, but is rare. Despite all this, over 80% of the more than 120 countries with data privacy laws have them administered by appointed and functioning, independent, specialised DPAs. How well they do their job as regulators is another question, but they are the rule, not the exception.

DPA/PEA policy-oriented networks

Networking between DPAs is good policy, due to the common nature of the issues they must deal with, the global nature of many of the issues that they must confront, and the isolation within their country's policy environment they often feel (particularly when newly-established). Networks can also be of particular value when some countries in a region have no data privacy law, but have common cultural values with neighbouring countries. It is then worth asking which networks exist, and which (by implication) are missing, and then whether those that exist are successful in attracting the involvement of all of their possible pool of membership. No doubt the networks consider this internally, but some external scrutiny is also needed, and this article aims to assist that to occur.

[3] C. Bennett and C. Raab *The Governance of Privacy* (MIT Press, 2006), p. 134; G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 62-75.

ICDPPC – More structure, increasingly global

The **ICDPPC** (International Conference of Data Protection and Privacy Commissioners) is the longest established (since 1979) DPA organisation, and accredits as members DPAs from any country with the requisite role and independence, as well as sub-national and supra-national DPAs. The eight new members of ICDPPC since 2015 are the DPAs of Armenia, Benin, Cape Verde, Cote d'Ivoire, Georgia, Mali, the Philippines and Ukraine. It is likely that Japan's DPA will become a member in 2017, when it is fully operational. ICDPPC now has 70 national members. Of the 84 countries that have specialised DPAs (and have appointed them), 83% are therefore members of ICDPPC.[4] A few of those missing might not be eligible for membership for lack of requisite independence (e.g. Malaysia, Singapore, Macau, Zimbabwe), and a few are only very recently appointed or not fully established (Japan, South Africa, Turkey). Once these are taken into account, ICDPPC can now claim to be a comprehensive national network of independent DPAs with 90% of its potential membership.

Another important global policy-oriented grouping, **IWGDPT** (International Working Group on Data Protection in Telecommunication, or 'Berlin Group') was created in 1983 by Berlin's DPA. It meets twice a year, once in Berlin, once in another country, and does not have a fixed membership list. Its draft common positions[5] are presented to members of ICDPPC, APPA and other networks before adoption.

Africa – the new RAPDP

A new African DPA association, **RAPDP** (Réseau Africain sur la Protection des Données Personnelles – African Personal Data Protection Network), was established in 2016 with 3 categories of members (i) DPAs of UA member states, are members with voting rights; (ii) representatives of UA member states with a data privacy law but not yet a DPA, may be observers; and (iii) representatives of UA member states that wish to enact a data privacy law may be observers. The eleven current members with laws and DPAs in category (i) are listed in the Table of Data Privacy Laws plus Niger as an observer in category (iii) in the Bills Table. The current president is from Benin, and RAPDP works in English, French, and Portuguese.

Other regional and global associations thrive

AFAPDP, the Francophone Association of DPAs,[6] now has twenty full members with voting rights, Kosovo; and Mali being the most recent members, and many other observer members. It aims to promote data protection cooperation and training initiatives between French-speaking countries. Its General Secretary is based in France, and its executive positions aim to achieve geographical balance.

RedIPD (La Red Iberoamericana de Protección de Datos, also called the RedIberoamericana or Latin American Network)[7] has 22 members and consists of all the Latin American countries, plus Spain, Portugal and Andorra. However, only six of the Latin American members are DPAs, the rest are from government agencies.

---

[4] The 2015 version of this analysis noted that ICDPPC had 70% (63/90) of national DPAs as its members. This figure was an under-estimate, because it did not take into account that some countries had not appointed DPA provided for in their Acts.

[5] Berlin Group 'Common Positions' <https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>

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

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

APPA, the Asia-Pacific Privacy Authorities now has 18 members from 10 countries (largely the same as countries in APEC), as shown in the Table, with Japan's DPA being its most significant new member.

Anglophone DPAs: CTN and BIIDPA

The Common Thread Network (CTN or CommTN) is a Commonwealth-wide DPA association,[8] formed in 2014, but launched in 2016 at the Morocco IDPPCC conference. Its current members include the DPAs from Australia (including the Victorian office), the Bahamas, Canada (including the BC, Nova Scotia and Yukon offices), the Channel Islands (i.e. Guernsey and Jersey), Ghana, the Isle of Man, Malta, Gibraltar, Mauritius, New Zealand, and the United Kingdom, as well as the following observers: Bermuda, the Cayman Islands, India, Trinidad and Tobago, the Seychelles and Uganda.

There is also a smaller organisation, BIIDPA (British, Irish and Islands' Data Protection Authorities). The DPAs of the UK, Ireland, Cyprus, Jersey and Guernsey, the Isle of Man, Malta, Gibraltar and Bermuda meet annually at the invitation of one of the respective authorities (Malta in 2016, Gibraltar in 2017). Comparative normative background, historic ties and (in most cases) proximity, explain BIIDPA's continuing existence, as an informal forum for members of the Commonwealth. Cyprus is a member, although not of the broader CTN, but perhaps this is just a matter of time. Also, BIIDPA can include Ireland, but CTN cannot.

Some DPAs in Commonwealth countries are not members or observers of either association: Malaysia, Singapore, Antigua & Barbuda, St. Lucia, and (the newest) South Africa. Hong Kong is not eligible. All in all, the Anglophone DPAs are still developing, but CTN has had a strong start.

European associations

The European-wide association of DPAs (**EDPA** or 'Spring Conference'), meeting since 1990 in anticipation of the coming EU Directive, in 2016 accredited Armenia, Hungary, Gibraltar, the Canton of Basel-Stadt- Switzerland, and Monaco as new members. Armenia's Personal Data Protection Agency also became the 20th member of the Central and Eastern Europe Data Protection Authorities (**CEEDPA**). It also joined GPEN and AFAPDP, thus becoming the year's most enthusiastic new DPA network participant (slightly ahead of the Philippines' DPA). The **Nordic DPA group** has met at least annually since at least the 1980s.

In December 2016, the Regional Network of Data Protection authorities in Eastern Partnership Countries (**RNDPAEPC)** was formed at a meeting in Tbilisi, Georgia. The members are Armenia, Georgia, Moldova and Ukraine (all represented by their DPAs), Azerbaijan (which has a law but no DPA) and Belarus (with no law as yet) represented by other public bodies than a DPA. This network is not in the table as it is only recently known.

Missing associations

Not all regions or language groups have DPA/PEA association where they might be expected. For example, there is no Caribbean organisation, nor one for Portuguese-speaking countries. A 'Greater China' privacy conference for Chinese-speaking authorities and academics has been held, but there is no formal association.

[8] Common Thread Network website https://commonthreadnetwork.org/: 'a forum for data protection and privacy authorities of Commonwealth countries'. See lists of Members and Observers.

DPA/PEA enforcement networks

As with policy networks, there is an increasing likelihood of cross-border enforcement issues being dealt with by DPAs and PEAs, so international networks to facilitate cross-border resolution are *prima facie* desirable. But which networks are these, and do they complement or compete with each other for any reasons? To what extent does national legislation give DPAs/PEAs sufficient powers and obligations to cooperate, particularly in information exchange? And which DPAs do not become involved in these networks? Most of these questions are beyond a brief survey such as this, but details of extent of membership are provided below. Further details of these networks are in the 2015 article.

ICDPPC's **Enforcement Arrangement**[9] established by resolution of the 2014 ICDPPC Conference in Mauritius now has members from ten countries (both national sub-national DPAs in some cases). They are listed in the Table.

GPEN, the Global Privacy Enforcement Network[10] has included 6 new members since 2015,[11] so that it now has members from 47 countries (plus sub-national and supra-national members).

GPEN Alert is a separate network within GPEN, and administered by the US Federal Trade Commission (FTC) on behalf of it nine participants as yet (listed in the Table). It facilitates information sharing on individual investigations, and therefore has high security requirements.[12]

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.[13] It has members from nine countries.[14]

UCENet is the new name for what was referred to as the "London Action Plan" (on spam). Participation is not limited to DPAs, and it is not included in the Table, but a number of DPAs are members.[15]

Missing DPAs/PEAs

Some DPAs/PEAs are just not 'joiners', they are not members of any associations of DPAs/PEAs which they are eligible to join: Antigua & Barbuda; Equatorial Guinea; Faroe Islands; Lesotho; Malaysia; San Marino; and Sao Tome & Principe. In some cases, lack of funds might be a reason, but not in some of these instances. If involvement in networks is a sign that

---

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

[10] GPEN < https://www.privacyenforcement.net/>

[11] 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.

[12] '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)

[13] APEC-CPEA <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>

[14] APEC-CPEA members: Australia, NZ, USA, HK SAR China, Canada, Japan, Korea, Mexico, Singapore.

[15] See UCENet website <https://www.ucenet.org/member-organizations/.>.

a DPA really is alive, less benign reasons may explain non-engagement, and these DPAs need to be put on a watch-list for signs of life.

On the other hand, the lifetime achievement award for membership of the most networks goes to Canada for its membership of nine networks: ICDPPC; APPA; GPEN; APEC CPEA; AFAPDP; CommTN; GCBECA; GPEN-A (the acronyms are explained in the Table). Runners-up, Australia and the United Kingdom, each with only eight, may claim this is unfair because Canada is bilingual.

Networks under international agreements

A different category of networks, because their membership is not so much DPAs/PEAs, but rather the representatives of countries that are parties to international data protection agreements. DPAs/PEAs are sometimes those representatives, but not usually.

The largest such grouping is the **Consultative Committee of Council of Europe Convention 108**. It includes representatives of the 50 Member States of the Convention (three from outside Europe), the four countries that have part-completed the accession process,[16] and six further non-European countries who are observers.[17] This means that 60 states participate, half of the 120 countries that now have data privacy laws, plus various supra-national organisations and NGOs. The Committee's membership is likely to expand further, with pending requests for observer status by Japan and the Philippines, and Argentina having indicated its interest in the Convention. CoE 108 Consultative Committee meetings are therefore one of the largest regular 'network' meetings in relation to data protection. The Committee meets in Plenary twice per year in Strasbourg, and has bureau meeting three times per year in various places. The Committee prepares draft legal instruments for the Committee of Ministers (for example, Recommendation of 2015 on Employment) or adopts as its own reports, opinions or guidelines (for example, the PNR Opinion and the Big Data Guidelines). The texts adopted by the Committee apply to all 50 Parties, now a broader group than CoE Member States.

The most significant grouping resulting from an international agreement is undoubtedly the EU's **Article 29 Working Party** (A29WP), with membership comprising the DPAs of all 28 EU Member States (at least until Brexit occurs). It has various formal roles under EU privacy Directives, including in adequacy assessments. Since 1997 it has issued a continuous stream of significant joint policy documents, and has increasingly become engaged in joint enforcement activities.

The other such network of significance arising from an international agreement is the **Data Privacy Sub-group (DPS) of APEC's Electronic Commerce Steering Group (ECSG)**, which has as members representatives of the 21 APEC economies, and meets twice per year. It does not have a process for other economies to become observers. The Privacy Sub-group does significant policy work such as recommendations to APEC for revision of the APEC Privacy Framework, and in relation to administration of APEC's Cross-Border Privacy Rules system (CBPRs).

The African Union Convention on cybercrime and data protection is not yet in force, so no such network yet exists under that agreement.

---

[16] CoE 108 Members: Uruguay, Mauritius, Senegal; CoE accessions part-complete: Morocco, Tunisia, Cape Verde TBC, and Burkina Faso.

[17] CoE 108 Observers: Australia, Canada, Indonesia, Korea, Mexico, and the US

Conclusions: DPA/PEA accountability

This survey looks at some of the more obvious questions concerning DPAs/PEAs, because that is where it is necessary to start: do data privacy Acts require their appointment?; are they appointed?; do they show signs of life by being active in DPA/PEA networks?

There are more questions that need to be asked about DPAs/PEAs on a periodic basis, and the answers compared across jurisdictions according to some global performance standards. Most of these questions come down to two fundamental concerns: do they have the resources (within the capacity of their country) to carry out their mandate to a reasonable extent, and can they demonstrate that they are accountable for carrying out that mandate? Three key aspects of that accountability are the publication of annual reports; the publication of a reasonable number of cases studies (usually anonymised) of how they apply the law to resolve disputes; and the publication of statistics concerning their use of their powers to resolve complaints, and what remedies or other outcomes result.

On a global basis, these are tasks far beyond the capacity of academic or NGO analysts. For that reason, it is particularly encouraging to see that the ICDPPC is this year conducting an extensive survey of its member DPAs, which will cover many aspects of their work including the above questions. It will be launched in late March. The ICDPPC Secretariat intends to make the results public, not only in aggregate but also to share source data with researchers and other networks. This work is buttressed by the resolution adopted by the 38th ICDPPC at its 2016 meeting in Marrakesh which recommends that DPAs 'play a part in helping to develop internationally comparable metrics in relation to data protection and privacy'.[18] The 2013 revised OECD privacy Guidelines and the 2016 revised APEC Framework also contain recommendations supporting such metrics, and APPA has also endorsed similar measures.

DPAs and PEAs must be accountable for their work to achieve their missions, as well as being supported to do so. It is possible that 2017 will see concrete advances in achieving this.

***Update**: It was noted in the previous article (Issue 145, p. 10) that the APEC Privacy Framework was being revised, probably to keep it consistent with the 2013 OECD Guidelines revision. The revision was in fact completed and endorsed, along these lines, in November 2016.*[19]

[18] 'Resolution on developing new metrics of data protection regulation' <https://icdppc.org/wp.../Developing-new-metrics-of-data-protection-regulation.pdf>

[19] *Updates to the APEC Privacy Framework*, APEC 2016/CSOM/012app17, November 2016 <http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf>. See also APEC ECSG: 'The ECSG-DPS recently completed its update of the APEC Privacy Framework which was endorsed by the Ministers in November 2016.' <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>