



UNSW Law & Justice Research Series

Global Data Privacy Laws 2023: International Standards Stall, but UK Disrupts

Graham Greenleaf

[2023] *UNSWLRS* 50
(2023) 183 *Privacy Laws & Business
International Report* 8

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@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 laws 2023: International standards stall, but UK disrupts

[Graham Greenleaf](#), Professor of Law & Information Systems, UNSW Australia

(2023) 183 *Privacy Laws & Business International Report* 8-15

Since 2020 there has been very limited progress in the development of international data privacy standards. This contrasts with modest progress in 2019-20 ('Uncertain paths for international standards' (PL&B Int, Feb 2021, pp. 23-27) and with the watershed period of 2017-18 ((PL&B Int, Feb 2019, pp.19-20). Developments in 2021 to mid-2023 are analysed in this article, and the changes to the countries affected are detailed in my *2023 Global Tables of Data Privacy Laws and Bills*¹.

EU GDPR-created standards (emulation and adequacy)

To refer to the EU's General Data Protection Regulation (GDPR) is ambiguous. The GDPR, in force since 25 May 2018 in fact created two international data privacy standards: the first through informal emulation, and the second through formal 'adequacy' mechanisms. First, new laws enacted or revised in 2021-22² confirm that the GDPR has established a new 'global benchmark' (often called a 'gold standard') for data privacy protection, to which non-EU countries very often aspire to align their laws, in very varying degrees. Only some of the innovations in the GDPR are being widely emulated, and it is too early to assess which ones will eventually be fully part of this '3rd generation' of data privacy standards.

The GDPR coming fully into force in 2018 created a second, more legally significant, 'GDPR standard' which must be met by those countries which wish to obtain or retain unhindered transfers of personal data from the EU. They must obtain a finding by the European Commission that they 'ensure an adequate level of protection' (GDPR art. 45), but the precise content of that 'adequacy standard' (including which of the GDPR's 18 innovations are required) can only emerge from Decisions of the European Commission, Opinions of the European Data Protection Board (EDPB), and (most important) decisions of the Court of Justice of the EU (CJEU). These texts are as yet few and far between.

Considerable uncertainty about adequacy was created by the CJEU decision in 'Schrems II' (2020) that 'certain programmes enabling access by US public authorities' did not satisfy the requirements for essentially equivalent protections as are provided under EU law and did not 'grant data subjects actionable rights before the courts against the US authorities'.³ Adequacy decisions by the Commission since 2020 have to meet these requirements.

¹ *Global Tables of Data Privacy Laws and Bills (8th Ed) 2023* < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4405514>

² G. Greenleaf 'Global data privacy laws 2023: 162 national laws and 20 Bills' (2023) 181 163 *Privacy Laws & Business International Report* 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146>

³ European Data Protection Board 'Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*' 13 July 2020.

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

By the end of 2022, the EU Commission has adopted only three positive assessments under the GDPR: Japan (2019), Korea (2021) and the United Kingdom (2021).⁴

- A positive adequacy decision by the Commission concerning **Japan**, and a ‘mutual’ positive decision on EU protections by Japan, required re-assessment in two years (i.e. by 2021). Japan passed new legislation in 2020 to further align its laws with the GDPR. Japan and the European Commission met to successfully conclude the first ‘mutual adequacy’ review in April 2023.⁵ Consideration was not given as to whether the scope of the Commission’s adequacy finding could be extended to the public sector, now that the public sector has come under the jurisdiction of Japan’s DPA, or to academia, but it was agreed that these expansions could be considered in future.
- A positive adequacy decision by the Commission concerning **Korea** (public and private sectors) was announced on 17 December 2021. It followed Korea’s major reforms in 2020,⁶ and additional reforms in 2021. The UK government has also passed legislation allowing personal data transfers between the UK and Korea with no additional safeguards, the UK’s first adequacy decision since leaving the EU.⁷
- A positive adequacy decision by the Commission concerning the **United Kingdom** was announced on 28 June 2021 and will expire on 27 June 2025. A similar decision was made under the Law Enforcement Directive.

The most important unresolved data transfer problem remains EU transfers to the US. The Commission and the US announced on 25 March 2022 an agreement in principle on a new *Trans-Atlantic Data Privacy Framework* which would be consistent with the July 2020 CJEU decision in *Schrems II*.⁸ Under the Framework, the US is to ‘put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight...’⁹ To implement this, President Biden signed an Executive Order on 7 October 2022 and the Attorney General issued regulations. In response the Commission released a positive draft adequacy decision on 13 December 2022.¹⁰ The European Data Protection Board (EDPB) issued its opinion on 28 February 2023,¹¹ ‘welcoming

⁴ See the European Commission ‘Adequacy Decisions’ website for all official decisions and press releases concerning adequacy <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>

⁵ European Commission ‘Japan: EU and Japan conclude first review of their bilateral mutual adequacy arrangement’ 4 April 2023 <https://www.eeas.europa.eu/delegations/japan/japan-eu-and-japan-conclude-first-review-their-bilateral-mutual-adequacy_en?s=169>

⁶ Park, KB et al ‘Korea amends Personal Information Protection Act’ (2020) 163 *Privacy Laws & Business International Report* 21-3.

⁷ Oliver Bray (RPC law firm) ‘UK’s first adequacy decision since leaving EU permits data transfers to South Korea’ *Lexology*, 31 March 2023

⁸ ‘European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework’ 25 March 2022 <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087>

⁹ *ibid*

¹⁰ Joint Press Release ‘Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US’ 13 December 2022.

¹¹ Summary of EDPB Opinion 5/2023, 28 February 2023 <https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

substantial improvements such as the introduction of requirements embodying the principles of necessity and proportionality for US intelligence gathering of data and the new redress mechanism for EU data subjects. At the same time, it expresses concerns and requests clarifications on several points. These relate, in particular, to certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism.’ The European Parliament has resolved that the European Commission should not grant the United States an adequacy decision. The non-binding resolution was by 306 votes in favour, 27 against, and 231 abstaining. ‘MEPs note that the framework still allows for bulk collection of personal data in certain cases, does not make bulk data collection subject to independent prior authorisation, and does not provide for clear rules on data retention.’¹² MEPs were also concerning that the Data Protection Review Court lacked both transparency and independence.

Countries already held ‘adequate’ under the 1995 Directive¹³ were supposed to have this status renewed under the GDPR within four years (i.e. by 2022),¹⁴ but the decisions remain in force after that time until the European Commission decides otherwise.¹⁵ Of these jurisdictions, Uruguay, Jersey, Guernsey, Argentina and New Zealand all had substantially updated their laws by 2021. Canada and Israel have reform Bills in progress. Whether any of these reforms will meet the ‘adequacy standard’ of the GDPR remains unknown, but the Commission’s decisions on these seven jurisdictions (plus the UK, Korea, Japan and perhaps the US) should shed considerable light on which elements of the GDPR are necessary (or at least important) for a positive adequacy assessment. Except for one country where discussions continue, the Commission’s reports on the continuing adequacy of all these countries are complete, subject to final checking, and await publication. It is a very slow process.

The UK has also made provisional post-Brexit arrangements so that EEA countries and ‘all countries covered by the EU’s adequacy decisions pre-Brexit are also considered adequate for the purposes of the UK GDPR’.¹⁶ The activity of Japan and the UK in starting their own adequacy decisions means that the ‘adequacy landscape’ is rapidly becoming more complex.

Convention 108 & 108+: Ratifications and accessions

The ‘modernisation’ of Council of Europe data protection Convention 108 was completed, by the parties to the existing Convention agreeing to a Protocol amending it, on 18 May 2018. The new version (called ‘108+’ to distinguish it) will not come into force before October 2023) and requires at least 38 ratifications to do so.¹⁷ New parties must simultaneously accede to both Convention 108 and to its amending Protocol (i.e. to 108+). The Convention’s Consultative Committee has nearly completed a detailed procedure for assessing substantive compliance with the requirements of

¹² European Parliament Press Room ‘MEPs against greenlighting personal data transfers with the U.S. under current rules’ 11 May 2023 < <https://www.europarl.europa.eu/news/en/press-room/20230505IPR85012/meps-against-greenlighting-personal-data-transfers-with-the-u-s>>

¹³ See discussion of Bills relevant to such assessments in Greenleaf ‘Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR hegemony’ < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348>

¹⁴ EU GDPR art. 45(3). See also art. 45(4) requiring the Commission to monitor developments in third countries with adequacy decisions.

¹⁵ Article 45(9) of the EU GDPR says that decisions adopted under the Directive shall remain in force until amended, replaced or repealed by a new decision. In the absence of such a decision, they could have ‘indefinite adequacy’.

¹⁶ Bray, op cit

¹⁷ For details see G. Greenleaf (2018) ‘Modernised’ data protection Convention 108+ and the GDPR’ 154 *Privacy Laws & Business International Report* 22-3 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

108+, both for accessions and continuing assessments.¹⁸ However, it is unknown what level of substantive compliance with the standards of 108+ countries must meet in order to accede.¹⁹ An accession request to 108+ by Costa Rica is progressing but has not yet resulted in an invitation to accede.

The requirement of continuing assessment of compliance with 108+ may prove challenging for some countries. For example, changes to the UK's definition of 'personal data' in its new law are arguably inconsistent with the Convention.²⁰

Argentina and Morocco have since 2018 completed their accessions to Convention 108, bringing its current number of Parties to 54 (including the suspension of Russia's membership in 2022). Burkina Faso remains the only country which had commenced but not completed the accession process, and is still able to accede to 108 alone.²¹ Forty-four of the existing Parties have now signed Convention 108+,²² but only 23 have ratified it (an increase from 11 in 2020). There are three ratifiers from outside Europe; Mauritius (2018), Uruguay (2021) and Argentina (April 2023) being the most recent to join.. Only 9 of the 27 EU Parties have yet ratified the Convention. Out of Council of Europe Member States, 27 have not yet ratified 108+, and only 10 did so in 2021-22. All in all, while progress on Convention 108+ ratification has doubled in 2021-22, the lack of ratifications by EU Member States is particularly disappointing.

Regional agreements in Africa: AU Convention and ECOWAS Supplementary Act

Africa has the only two binding regional agreements concerning data privacy, one of which is in force. The *African Union Convention on Cyber Security and Protection of Personal Data* (2014), also known as the Malabo Convention, has relatively high data protection standards, and a potential membership of 55 African countries. It is the most significant data privacy Convention other than the increasingly global Convention 108. Thirteen countries have ratified²³ this AU Convention²⁴ and eleven more countries have signed but not ratified.²⁵ Some countries without data privacy laws have signed or ratified,²⁶ possibly because the Convention also covers cyber-crime. Fifteen ratifications are required for the Convention to enter into force (art. 36), so only two more ratifications from the 11 unratified signatures are needed, indicating that it is likely that the

¹⁸ The *Evaluation and follow-up mechanism under Convention 108+* (T-PD(2018)20rev6, T-PD(2018)21rev6) are to be finalized by the Convention's Bureau.

¹⁹ G. Greenleaf 'How Far Can Convention 108+ 'Globalise'?: Prospects for Asian Accessions' *Computer Law & Security Review*, Special Issue on the 40th Anniversary of Convention 108, January 2021 <<https://www.sciencedirect.com/science/article/pii/S0267364920300194>> or <<https://ssrn.com/abstract=3530870>>.

²⁰ See Pounder, C 'Definition of "personal data" in DPDI No 2 Bill results in non-compliance with CoE Convention No.108 in PL&B UK, May 2023, p. 9.

²¹Greenleaf 'Modernised' data protection Convention 108+ and the GDPR', cited above.

²² Council of Europe *Chart of signatures and ratifications of Treaty 223*, as at 19 February 2023 <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures>>.

²³ AU Convention ratifications: Angola, Cape Verde, Congo, Mozambique, Niger, Togo. Senegal, Mauritius, Guinea (Conakry), Ghana, Mozambique, Namibia and Rwanda.

²⁴ This Status List to 18/6/2020 (current as at February 2023) is at <<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>>.

²⁵ AU Convention signatures without ratifications: Benin, Cameroon, Chad, Comoros, Gambia, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Tunisia

²⁶ Five countries without data privacy laws have signed the AU Convention (Comoros, Guinea-Bissau, Cameroon, Sierra Leone, and Zambia). Three countries without a law have ratified in 2021-22 (Namibia, Mozambique and Rwanda).

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

Convention may soon enter into force. The majority of African countries with data privacy laws have as yet neither signed nor ratified the Convention, increasing this feasibility. Ratifying states Mauritius, Senegal and Cape Verde are also Parties to Convention 108.

The fifteen member states²⁷ of the Economic Community of West African States (ECOWAS) adopted the *Supplementary Act on Personal Data Protection within ECOWAS* (2010)²⁸ to the ECOWAS Treaty, to establish the content required of a data privacy law in each ECOWAS member state, including the composition of a data protection authority. It may be enforced by the ECOWAS Court of Justice.²⁹ The ‘ECOWAS laws’ are among the strongest data privacy laws in Africa. Eleven of the fifteen ECOWAS states have enacted data privacy laws,³⁰ with none of the remaining four doing so in 2021-22.

Non-binding agreements and declarations

Africa apart, no other region outside Europe has a binding agreement on data privacy (whether in force or awaiting ratifications). However, these developments in standards, both regional and global, are worth mentioning:

- The *Standards for Personal Data Protection for Ibero-American States* (‘RIPD Standard’) was finalized in 2017 by the 20-country network of Latin American data protection authorities (abbreviated as RIPD or RedIP), at the request of the XXVth *Ibero-American Summit of Heads of State and Government* in 2016. The RIPD Standard is a measure against which laws in Latin American countries can aim for consistency and can demonstrate that they are meeting regional and global standards. This RIPD Standard’ has a strong consistency with the EU’s GDPR and with Convention 108+. However, it has no legal force, and there is no obvious treaty-making body.
- The *RIPD network’s model contractual clauses for international transfers*³¹ are based on these RIPD standards.
- A draft *Statement of Principles for Privacy and Personal Data Protection in the Americas* was prepared in 2012 by the Organisation of American States (OAS), which includes all 35 independent states in the Americas (including the Caribbean, and the US and Canada). It comprises 12 principles,³² of standards closer to the OECD Guidelines than the GDPR, and thus weaker than the RIPD Standard. The OAS has not yet adopted the Standard. An OAS initiative to develop a model law does not seem to have progressed. OAS does have the capacity to create treaties.

²⁷ ECOWAS Member States: Benin, Burkina Faso, Cape Verde, the Ivory Coast, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo. Mauritania is an associate member.

²⁸ *Supplementary Act on Personal Data Protection within ECOWAS* <<http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf>>

²⁹ So far, no data privacy case has been submitted to the ECOWAS Court.

³⁰ ECOWAS member states with laws: Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Guinea, Ivory Coast, Mali, Niger, Nigeria and Togo.

³¹ Guía De Implementación De Cláusulas Contractuales Modelo Para La Transferencia Internacional De Datos Personales (TIDP).

³² http://www.oas.org/es/sla/ddi/docs/CJI-RES_186_LXXX-O-12.pdf (in Spanish)

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

- ASEAN Ministers for digital affairs have approved **Model Contractual Clauses for Cross Border Data Flows** (MCCs).³³ The MCCs are based on³⁴ the 2016 **ASEAN Framework on Personal Data Protection**³⁵ a non-binding ‘record of Participants’ intentions’ with no practical effects, which in turn refers to, and has principles similar to, the APEC Privacy Framework, plus principle on cessation of retention of personal data. These are less demanding standards, comparable to those proposed for the OAS.³⁶
- An EU/OECD **Declaration on Government Access to Personal Data Held by Private Sector Entities** was made on 14 December 2022³⁷ by the EU and by 14 non-EU member states of the OECD.³⁸ This Declaration by 41 economically advanced countries, though non-binding, is one of the most substantive privacy policy statements by such a globally large and diverse group of countries. It is intended to confirm that state access to data held by the private sector must be consistent with democratic values. The Declaration elaborates principles of (i) Legal basis; (ii) Legitimate aims; (iii) Approvals; (iv) Data handling; (v) Transparency; (vi) Oversight; and (vii) Redress. It claims that ‘As the first intergovernmental agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, it seeks to promote trust in cross-border data flows, a critical enabler of the global economy’. This reflects the ‘Data Free Flow with Trust’ slogan promoted by the OECD, Japan, and others.
- The **Commonwealth’s Model Provisions on Data Protection**³⁹ was adopted in November 2022 by Commonwealth Law Ministers meeting in Mauritius, after all 56 Commonwealth Member States⁴⁰ were asked for final comment. It could be of future significance, particularly in the Pacific Islands where no countries have data privacy laws. This depends on whether Commonwealth countries decide to adopt the Provisions.

Regions such as the Caribbean and Central Asia have not developed any standards of their own. The OECD is proposing to complete a revision of its privacy *Guidelines* (1980/2013), but it is very unlikely to involve changes to their core principles.

³³ 1st Association of Southeast Asian Nations (ASEAN) Digital Ministers’ Meeting (ADGMIN), 22 January 2021; see Press Release <<https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meeting>>;

³⁴ PDPC (Singapore) *Guidance For Use of Asean Model Contractual Clauses For Cross Border Data Flows in Singapore* 22 January 2021

³⁵ Telecommunications and IT Ministers of the ASEAN member states ‘ASEAN Framework on Personal Data Protection’ <<http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>> November 2016.

³⁶ G. Greenleaf ‘ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards’ (2021) 174 *Privacy Laws & Business International* Report 22-24,

³⁷ OECD Legal Instruments *Declaration on Government Access to Personal Data Held by Private Sector Entities*, 14 December 2022 <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>>

³⁸ Non-EU OECD members: Australia, Canada, Chile, Colombia, Costa Rica, Israel, Japan, Korea, Mexico, New Zealand, Switzerland, Türkiye, the United Kingdom, the United States.

³⁹ Commonwealth Secretariat *Model Provisions on Data Protection* 2023 <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-02/ROL%20Model%20Law%20Provisions%20on%20Data%20Protection.pdf?VersionId=Fpgmtvhd6E3dm3JfQiEVp8IP0zO_mGy0>

⁴⁰ Member States of the Commonwealth <https://en.wikipedia.org/wiki/Member_states_of_the_Commonwealth_of_Nations>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts CBPRs (APEC and ‘global’): Impact continues to be negligible

To participate fully in the Asia-Pacific Economic Cooperation's **Cross-Border Privacy Rules System (APEC CBPRs)**, a country's laws must be approved by APEC's Electronic Commerce Steering Group Joint Oversight Panel (ECSG-JOP), and the country must appoint ‘Accountability Agents’ (AAs), so that companies in their jurisdictions can apply to be certified as CBPRs-compliant. As of February 2023, only five countries have appointed AAs.⁴¹ They have certified 60 companies:⁴² US (42 companies since 2013⁴³); Japan (6 companies since 2016⁴⁴); Singapore (10 companies since 2019⁴⁵); Korea (2 companies since 2019) and Taiwan – no certifications apparent). Therefore, after ten years of operation, APEC CBPRs only involves engagement by a tiny number (60) of US, Japanese, Singaporean and Korean companies. APEC CBPRs is therefore of negligible practical significance as yet, and there is no sign of this changing.

‘Participation’ without appointment of an AA is illusory, with no practical effect. In 2021-22 no new countries were approved to ‘participate’ in APEC-CBPRs. ECSG-JOP has held previously that the laws of ten countries met APEC requirements: US (2012); Japan, Canada and Mexico (2014); Korea (2016); Singapore (2017); Taiwan and Australia (2018) and the Philippines (2019). Only half of these countries have as yet appointed an AA,⁴⁶ It seems that some countries (6 so far) say they wish to participate in APEC CBPRs, and take preparatory steps, but then do not do so. A minority of ‘participants’ (4 so far) go further, appointing AAs and certifying a few companies.

However, Singapore has done something more significant, from the perspective of Singaporean companies wishing to legally export personal data outside Singapore: ‘Singapore recognises the APEC CBPR and PRP certifications for overseas transfers of personal data under the PDPA. This means that organisations in Singapore can easily transfer personal data to the overseas certified recipient without meeting additional requirements.’⁴⁷ At present, this only assists Singaporean companies wishing to export personal data to the 42 CBPRs-certified US companies.⁴⁸ It adds nothing to exports to Japan, which has a law stronger than Singapore's law, and in any event has only certified six Japanese companies. It is of benefit only to the US (which has no laws sufficient to meet export requirements), and the US companies that are CBPRs-certified.

⁴¹ APEC CBPRs Accountability Agents listing <<http://cbprs.org/accountability-agents/>> .

⁴² Company certifications are aggregated in the CBPR System Directory <<http://cbprs.org/compliance-directory/cbpr-system/>>., which is relied upon. Figures for the main AAs are also given.

⁴³ TrustAct *APEC CBPR Certified Companies* <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>> as at 21 February 2023.

⁴⁴ JIPDEC's APEC CBPRs Certified Companies list <https://english.jipdec.or.jp/protection_org/cbpr/list.html> (as at 21 February 2023).

⁴⁵ Singapore IDMC ‘APEC CBPR System’ <<https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification>> . See also (Singapore) Directory of APEC Cross Border Privacy Rules (CBPR) Certified Organisations <<https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification/CBPR-Certified-Organisations>>.,(as at 21 February 2023)

⁴⁶ Canada called for applicants to be AAs in 2017. See Gazette <<http://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/pdf/g1-15103.pdf>> at p. 242.

⁴⁷ IMDA (Singapore) ‘APEC Cross Border Privacy Rules (CBPR) System’ op cit; On 28 May 2020 PDPC amended the PDPA Regulations to recognise certification under CBPRs or PRP as compliant with s 26 of the PDPA (see Clarisse Girot *Transferring Personal Data in Asia: A path to legal certainty and regional convergence* Asian Business Law Institute May 2020 (‘ABLI Review’) <<https://info.sal.org.sg/abli/ebooks/privacy/>> , p. 56).

⁴⁸ *CBPR Compliance Directory* <<http://cbprs.org/compliance-directory/cbpr-system/>>.

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

The European Commission states in its Decision concerning Japan's adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate.⁴⁹ This will further diminish the business case for CBPRs.⁵⁰

A '**Global Cross-Border Privacy Rules Declaration**' (Global CBPRs) was announced on 21 April 2022 by the US Department of Commerce.⁵¹ It stated that Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the US, as 'current economies participating in the APEC CBPR System', had established 'the Global CBPR Forum'. Australia subsequently joined,⁵² and Mexico is listed as a member on the Global CBPR Forum website.⁵³ Since these are the nine 'economies' that have been approved to participate in APEC CBPRs,⁵⁴ the 'Declaration' adds nothing.

As of May 2023, more a year after the Global CBPR Forum was established, no additional countries from the other 121 non-EU/EEA countries with data privacy laws have applied to become a Member of the Forum⁵⁵ However, while chairing sessions in a global CBPR forum in London,⁵⁶ the UK 'submitted its application to join the [Global CBPRs] Forum *as an Associate*'⁵⁷ (emphasis added). All this means is that 'Associates participate in the Forum and its activities to prepare for their potential participation in the Global CBPR System and/or Global PRP System as Members', according to the CBPRs Terms of Reference (procedures).⁵⁸ The criteria for Associate status is that the applicant supports the principles and objectives of Global CBPRs, has laws or regulations protecting personal information, and has a public body responsible for enforcing them, and investigating.⁵⁹ Associate status will normally only be granted for two years, with an

⁴⁹ [European Union] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information < https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf >

⁵⁰ On the other hand, APEC CBPRs has been 'recognised' in the USMCA tripartite free trade agreement (see below), but with no obvious effect.

⁵¹ US Department of Commerce 'Global Cross-Border Privacy Rules Declaration' 21 April 2022 <<https://www.commerce.gov/global-cross-border-privacy-rules-declaration>>

⁵² Australia joins the Global Cross-Border Privacy Rules Forum, 17 August 2022 < <https://ministers.ag.gov.au/media-centre/australia-joins-global-cross-border-privacy-rules-forum-17-08-2022>>

⁵³ Global CBPR Forum website < <https://www.globalcbpr.org/>> undated

⁵⁴ APEC CBPRs System < <http://cbprs.org/>>

⁵⁵ The Forum website does not mention any (<<https://www.globalcbpr.org/membership/>>). The Privacy Commissioner of Bermuda has informally 'joined': 'PrivCom recognises APEC CBPR System as a certification mechanism for overseas data transfers' 2 March 2021 <<https://www.privacy.bm/post/privcom-recognises-apec-cbpr-system-as-a-certification-mechanism-for-overseas-data-transfers>>. See Bermuda's PIPA s. 15(4).

⁵⁶ UK government Press Release 'New data laws debated in Parliament' 17 April 2023 <<https://www.gov.uk/government/news/new-data-laws-debated-in-parliament>>

⁵⁷ International Trade Administration (US) 'Commerce Department Welcomes UK's Application to the Global CBPR Forum' 17 April 2023 < <https://www.trade.gov/press-release/commerce-department-welcomes-uks-application-global-cbpr-forum>>

⁵⁸ *Global CBPRs Forum Terms of Reference* (2023) < <https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Forum-Terms-of-Reference-2023.pdf>>

⁵⁹ CBPRs *Terms of Reference*, Appendix A, para. 4

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts application for membership expected within that time.⁶⁰ The Global CBPRs ‘Framework’ document⁶¹ does not mention an ‘Associate’ while in contrast it has many paragraphs on the expectations of a ‘Member’. Becoming an Associate therefore means nothing of substance, it is just a statement of future intentions. Most of the 162 countries with data privacy laws could apply to become a CBPRs Associate, but only the UK has done so.

If the UK decided (in the next two years) to apply to become a full Member of Global CBPRs, it is hard to see any advantages that could flow to UK companies from being ‘Global CBPRs-certified’, because the stricter standards of UK law would still apply to any UK exports, and companies importing into the UK would obtain higher protection from UK law, not from Global CBPRs standards.

The most significant change from APEC’s CBPRs is that Global CBPRs Membership can be based on legal recognition of Global CBPRs certifications ‘as a valid data transfer mechanism’, in which case the Member does not have to appoint AAs.⁶² Singapore already has such a provision (see above), as has Japan (with a crucial exception for EU-sourced data). How this change would work, and its significance for Global CBPRs, is yet to become clear. It is by itself unlikely to save Global CBPRs from failure, but it does make this less clear-cut than with APEC CBPRs’ manifest failure.⁶³

Asia-Pacific FTAs: Conflicting standards

In the Asia-Pacific there are a number of multilateral free trade agreements (FTAs) that have provisions limiting data export restrictions and data localisation. These provisions may (or may not) be inconsistent with provisions in the laws of some of these countries (including provisions necessary for EU adequacy), or with their other international obligations such as in Convention 108/108+.⁶⁴

The *US-Mexico-Canada FTA (USMCA)*, in force since January 2020, is the most restrictive. On data export restrictions, although it uses different terms, USMCA includes substantially the same ‘4 step test’ as in the CPTPP (see below), but has an outright ban on data localization.

The *Comprehensive and Progressive Trans Pacific Partnership (CPTPP)* came into force between its six ratifying parties on 30 December 2018,⁶⁵ and then Vietnam (January 2019), Peru (September 2021) and Malaysia (November 2022). The two other initial parties, Brunei and Chile, are yet to ratify. Any other country, or customs territory may also ratify, with the consent of all the parties, and subject to any conditions agreed (CPTPP, art. 5). Nine other APEC economies have announced interest in joining CPTPP.⁶⁶ The Biden administration has not yet sought to

⁶⁰ Ibid, paras. 10-13

⁶¹ *Global Cross-Border Privacy Rules (CBPR) Framework (2023)* <<https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf>>

⁶² CBPRs *Terms of Reference*, Appendix A, para. 3(c)

⁶³ G.Greenleaf ‘Global CBPRs: A recipe for failure?’ (2022) 177 *Privacy Laws & Business International Report* 11-13 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4180516>

⁶⁴ G. Greenleaf ‘Asia-Pacific free trade deals clash with GDPR and Convention 108’ (2018) 156 *Privacy Laws & Business International Report*, 32-34. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3352288>

⁶⁵ Australia, Canada, Japan, Mexico, New Zealand and Singapore – See DFAT Australia CPTPP site <<https://dfat.gov.au/trade/agreements/in-force/cptpp/Pages/comprehensive-and-progressive-agreement-for-trans-pacific-partnership.aspx>>.

⁶⁶ Colombia, Indonesia, South Korea, Taiwan, Thailand, Philippines, the US, and China, have expressed interest: see Wikipedia: Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts negotiate US accession to CPTPP,⁶⁷ which would increase the likelihood of enforcement of its data export and data localisation provisions. Of major importance, China has applied to accede, but its failure to comply with existing international trade rules may provide barriers to unanimous agreement (for example, by Australia or Canada – or potentially, the UK).

CPTPP includes two provisions which go beyond diplomatic means of enforcement: State party dispute settlement provisions (which can involve monetary payments); and investor-state dispute settlement (ISDS) provisions, which could apply in limited situations. CPTPP's provisions limiting data export restrictions and data localisation both impose a 'Four-Step-Test' for any exceptions to its prohibitions. States have the onus to prove that their legislation satisfies each of the four tests ('legitimate public policy objective'; not 'a means of arbitrary or unjustifiable discrimination'; not 'a disguised restriction on trade'; and not restricting 'transfers of information greater than are required').

The UK made a formal accession request to the CPTPP as part of its post-Brexit trade arrangements. After 21 months of negotiation the CPTPP Commission agreed in March 2023 to accept the UK as a party,⁶⁸ but this must be ratified by both the UK Parliament and by the other 11 initial parties.⁶⁹ UK Unions have condemned the ISDS clauses in CPTPP which will allow companies to sue governments if they believe their profits have suffered from changes to laws or regulations. This could include the introduction or strengthening of data privacy laws.⁷⁰

The latest Asia-Pacific FTA, signed by 16 countries on 15 November 2020, is the **Regional Comprehensive Economic Partnership (RCEP)**, involving the 10 members of ASEAN⁷¹ plus the six countries with which ASEAN has free trade agreements – Australia, China, India, Japan, Korea, and New Zealand. The US, Canada, Mexico and other Latin American parties to CPTPP are not included. To come into force, RCEP required 9 ratifications (or equivalent domestic processes), from at least three non-ASEAN signatories and six ASEAN signatories. RCEP has entered into force between thirteen parties:⁷² Australia, Brunei Darussalam, Cambodia, China, Japan, Laos, New Zealand, Singapore, Thailand and Vietnam (on 1 January 2022), Korea (on 1 February 2022), Malaysia (on 18 March 2022) and Indonesia (on 2 January 2023). With China as a leading participant, India entitled to a fast-track accession process, and thirteen accessions already, RCEP is potentially much larger than CPTPP.

RCEP's electronic commerce chapter does contain limits on data export restrictions and on data localisation (requirements to use local computing facilities) which involve a 'four step test' which is superficially similar to exceptions in the CPTPP. However, the question of whether measures are those 'that [a Party] considers necessary to achieve a legitimate public policy objective' is to be

⁶⁷ The Trump administration pulled out of its proposed predecessor, the TPP, in 2017.

⁶⁸ UK government Policy Paper [on conclusion of negotiations] including agreement <<https://www.gov.uk/government/publications/comprehensive-and-progressive-agreement-for-trans-pacific-partnershipcptpp-conclusion-of-negotiations/conclusion-of-negotiations-on-the-accession-of-the-united-kingdom-of-great-britain-and-northern-ireland-to-the-comprehensive-and-progressive-trans-pac#the-agreement>>, 31 March 2023

⁶⁹ See also the collection of UK government documents at <<https://www.gov.uk/government/collections/the-uk-and-the-comprehensive-and-progressive-agreement-for-trans-pacific-partnershipcptpp>>

⁷⁰ Phillip Inman 'UK joins Asia-Pacific CPTPP trade bloc that includes Japan and Australia' *The Guardian* 31 March 2023

⁷¹ ASEAN members: Brunei-Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam.

⁷² DFAT RCEP page <<https://www.dfat.gov.au/trade/agreements/in-force/rcep>>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

decided solely by that Party, and measures that a Party considers necessary for ‘protection of its essential security interests’ also ‘cannot be disputed by other Parties’. These are significant reductions compared with the CPTPP restrictions.⁷³

The result is that these Asia-Pacific FTAs provide three different models for the permissible breadth of data export restrictions, and data localization: USMCA (most strict); CPTPP (possibly intermediate); and RCEP (most permissive). One or other of these models is being followed in many bilateral FTAs in the Asia-Pacific and elsewhere (e.g. UK-Japan FTA), but bi-laterals are not considered here.⁷⁴

It is arguable that Japan, New Zealand and Canada may already have made commitments under these FTAs that are inconsistent with being considered adequate by the EU; and Mexico may have done similarly in relation to its commitments under Convention 108.⁷⁵

‘Data Free Flow with Trust’ (DFFT) at G20 and G7: Still an empty slogan

During its G20 Chairmanship in 2021 Japan promoted the concept of ‘Data Free Flow with Trust’ (DFFT) and invited countries to join the Osaka Declaration on Digital Economy, and then to use the ‘Osaka Track’ to implement DFFT.⁷⁶ Since then there has been no obvious progress made on DFFT, and with India as the G20 Chair in 2023 it may remain an empty slogan. India was one of four countries in 2021 that did not join the Osaka Declaration, and is in favour of data localisation policies.

However, Japan seems to have now switched its institutional focus to the smaller G7. A G7 Ministerial Declaration⁷⁷ in April 2023 states that ‘the Digital and Tech Ministers of the G7’ ‘affirm our commitment to operationalise’ DFFT and ‘stress the need for tangible progress on advancing DFFT’, but does not include any concrete measures to do so. The Ministers ‘endorse the establishment of the Institutional Arrangement for Partnership (IAP)’ and will ‘endeavour to launch it in the coming months’ after discussions of what it might involve. Japan’s Digital Affairs Minister has announced a plan ‘to create a database that lists data regulations for each country’,⁷⁸ but this is insignificant. DFFT often appears to be led by wishful thinking by countries and organisations that would like to see data export limitations reduced to the lowest common denominator – an unrealistic goal.

⁷³ G. Greenleaf ‘Will Asia-Pacific trade agreements collide with EU adequacy and Asian laws?’ (2020) 167 *Privacy Laws & Business International Report* 18-21.

⁷⁴ Greenleaf ‘Asia-Pacific free trade deals clash with GDPR and Convention 108’ cited above.

⁷⁵ See articles cited in the two previous footnotes.

⁷⁶ G. Greenleaf ‘[G20 makes declaration on "Data Free Flow With Trust"](#)’ (2019) 160 *Privacy Laws & Business International Report* 18-19.

⁷⁷ *Ministerial Declaration - The G7 Digital and Tech Ministers’ Meeting 30 April 2023* <https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf>

⁷⁸ Shiko Ueda ‘Japan to push for guidelines on cross-border data flows at G-7’ *Nikkei Asia*, 23 February 2023 <<https://asia.nikkei.com/Editor-s-Picks/Interview/Japan-to-push-for-guidelines-on-cross-border-data-flows-at-G-7>>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts

UN privacy commitments: Most have ratified

Of the 17 new countries enacting data privacy laws in 2021-22, the majority⁷⁹ have ratified the International Covenant on Civil and Political Rights, 1966 (ICCPR),⁸⁰ but only three⁸¹ have ratified the 1st Optional Protocol to the ICCPR.⁸² This is similar to the other 145 countries with data privacy laws: almost all have ratified the ICCPR, but a significant minority have not ratified the Protocol.⁸³

Conclusions: No clear direction

Looking back over post-2020 development, the global adoption of international data privacy standards has been very limited, but new uncertain elements have emerged, resulting in no convincing trajectory. Three reasons are apparent from this article.

Progress is too slow In 2021-22 the development of international data privacy agreements slowed to a snail's pace, except in the Asia-Pacific. COVID-19 no doubt added to the complexity of tasks being undertaken. The European Union's assessments of 'adequacy' under the GDPR made very limited progress, due to the demands of Schrems II, Brexit, and the sheer complexity of GDP adequacy assessments. The transition from Convention 108 to 108+ seems stalled, particularly in the lack of ratifications to bring the new Convention into force. The OECD's privacy Guidelines are mid-way through a revision which will leave their fundamentals unchanged. APEC's CBPRs, despite ostensible participation, remains of negligible practical significance, and Global CBPRs have the same flaws but also new and uncertain elements. Cross-border transfers made under CBPRs (either one) could become a 'collision course' with EU adequacy decisions⁸⁴ and with 108+.

FTA uncertainty in Asia-Pacific On data export limits and data localisation, Asia-Pacific countries remain suspended (for other geopolitical reasons) between standards in two FTAs: CPTPP with more restrictive requirements; and RCEP with less restrictive requirements. USMCA, completely banning some forms of data localisation, also affects some bilateral FTAs. UK and Chinese proposed accessions to CPTPP add new uncertainties.

Will regional treaties be skipped in favour of 108+? Convention 108 already has 55 Parties, 8 from outside Europe (5 from Africa, 3 from Latin America), and is in force. Convention 108+, though not yet in force, is open to accession globally, has strong safeguards concerning access to personal data by public authorities, and its ratification assists with EU adequacy (GDPR Recital 105). This is in strong contrast with regional binding agreement, of which the only examples are the African Union

⁷⁹ No ratification of the ICCPR: Cuba; Belarus; Oman; Saudi Arabia; United Arab Emirates

⁸⁰ Article 17 of which requires privacy protections; *International Covenant on Civil and Political Rights* (signatures and ratifications) <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en> (as at 4 January 2019).

⁸¹ The exceptions are Sri Lanka, Mongolia and Ecuador (see Tables).

⁸² This allows individuals to make 'communications' (complaints) to the UN Human Rights Committee, including concerning state failures to implement ICCPR Article 17: ICCPR 1st Protocol, ratifications <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-5&chapter=4&clang=_en> (as at 4 January 2019).

⁸³ As documented in the 5th edition (2017) of this survey: by far the majority of countries with data privacy laws have ratified both the ICCPR and the 1st Protocol, and therefore participate fully in the UN human rights system.

⁸⁴ Christopher Kuner 'Op-Ed: "International Data Transfers after Five Years of the GDPR: Postmodern Anxieties" *EU Law Live*, 5 May 2023 <<https://eulawlive.com/op-ed-international-data-transfers-after-five-years-of-the-gdpr-postmodern-anxieties-by-christopher-kuner/>>

Greenleaf – Global data privacy laws 2021: International standards stall, but UK disrupts Convention (not yet in force) and the ECOWAS agreement (not of global significance). No data privacy treaties seem likely to arise in other regions. It is plausible that regional binding agreements could be largely ignored, or of secondary importance, as countries skip regional agreements in favour of the global scope and higher standards of Convention 108+, but since 2020 there is little evidence of this occurring.

See also the articles ‘Global data privacy 2023: 162 national laws and 20 Bills’ and ‘Global Data Privacy 2023: DPA networks almost everywhere’ in the two previous issues.

Information: Valuable information and comments for this article have been received from David Freeland (ICO), Hannah McCausland (ICO), Elizabeth Coombs (University of Malta), Bertil Cottier (University of Lugarno) and Stewart Dresner and Laura Linkomies (PL&B). They are acknowledged with gratitude, but responsibility for all content remains with the author.