University of New South Wales Law Research Series

JAPAN'S PROPOSED EU ADEQUACY ASSESSMENT: SUBSTANTIVE ISSUES AND PROCEDURAL HURDLES

GRAHAM GREENLEAF

(2018) 154 *Privacy Laws & Business International Report*
[2018] *UNSWLRS* 53

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

Japan's proposed EU adequacy assessment: *Substantive issues and procedural hurdles*

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*

25 July 2018 A shorter version of this article will be published in (2018) 154 *Privacy Laws & Business International Report.*

Abstract: On 17 July 2018 the European Commission announced that it had successfully concluded with Japan 'their talks on reciprocal adequacy', and that the Commission would adopt its adequacy finding once 'relevant internal procedures are complete'. The draft decision is not yet available. This article commences by noting seven such procedures, and the numerous EU bodies that could have a substantive influence on the final decision, including the European Data Protection Board (EDPB) and the LIBE Committee of the European Parliament. The draft 'Supplementary Rules' by Japan's DPA (the PIPC), on which the decision is substantially based, is explained. Four aspects of the Rules which will benefit European data subjects, by strengthening aspects of Japanese law, are set out. The article then examines the following issues which EU bodies will need to consider: (i) the transparency of adequacy assessment processes; (ii) the applicability of the decision to Japan's public sector; (iii) whether some personal information transferred from the EU might fall outside Japan's definition of what is protected; (iv) whether the enforcement of Japan's data privacy laws does or can meet the standards of the GDPR; (v) whether, even though the Commission is preventing APEC-CBPRs compliance being a basis for onward transfers, its proposed replacement with an almost entirely consent-based mechanism is protective enough; and (vi) whether a law where the key elements of adequacy can benefit only Europeans can be 'essentially equivalent'. The path to the EU's decision on whether Japan's privacy protections are adequate has many rivers to cross.

Contents

* This paper is based in part on presentations at Privacy Laws & Business 31st Annual Conference, St Johns, Cambridge, 3 July 2018, and at the Brussels Privacy Hub 'Meet the Author' series, 26 June 2018. A number of European and Japanese experts have provided valuable assistance or comments, but all responsibility for content lies with the author.

On 17 July 2018, the European Commission announced[1] that:

> 'The EU and Japan successfully concluded today their talks on reciprocal adequacy. They agreed to recognise each other's data protection systems as 'equivalent', which will allow data to flow safely between the EU and Japan. Each side will now launch its relevant internal procedures for the adoption of its adequacy finding. ... Once this procedure will have been completed, the Commission will adopt the adequacy decision on Japan.'

Many rivers to cross

Although this announcement was couched in the certainty that the EU and Japan had 'agreed to create the world's largest area of safe data flows', the 'relevant internal procedures' at the EU end include the following:

1. Proposal of a draft adequacy decision by the Commission, following its approval by the College of Commissioners (28 members).[2] Only at that point will there be any legal certainty about what is proposed, as distinct from what is in a press release.

2. An opinion from the European Data Protection Board (EDPB), comprised of the head of the data protection authorities of each of the 28 EU member states, and the European Data Protection Supervisor (EDPS);

3. A comitology procedure;[3]

4. Provision of details to the LIBE Committee (Committee on Civil Liberties, Justice and Home Affairs) of the European Parliament, which may at any time 'request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the [GDPR]'.[4]

5. Approval from the representatives of the 28 EU member states;

6. Adoption of the adequacy decision by the College;

---

[1] European Commission - Press release 'The European Union and Japan agreed to create the world's largest area of safe data flows', Tokyo, 17 July 2018 <http://europa.eu/rapid/press-release_IP-18-4501_en.htm>.

[2] 'The Commission is composed of the College of Commissioners of 28 members, including the President and *Vice-Presidents*. The Commissioners, one from each *EU* country, are the Commission's political leadership during a 5-year term. Each Commissioner is assigned responsibility for specific policy areas by the President.' <https://ec.europa.eu/commission/commissioners/2014-2019_en>.

[3] 'Comitology refers to a set of procedures through which EU countries control how the European Commission implements EU law. Broadly speaking, before it can implement an EU legal act, the Commission must consult, for the detailed implementing measures it proposes, a committee where every EU country is represented. The committee provides an opinion on the Commission's proposed measures.' Comitology Register <http://ec.europa.eu/transparency/regcomitology/index.cfm?do=implementing.home#2>

[4] European Commission 'Adequacy of the protection of personal data in non-EU countries' , 17 July 2018 <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>

7. Once adopted, adequacy decisions may also be challenged by individuals before national data protection authorities, and subsequently through national courts and potentially to the CJEU, as in *Schrems*.[5]

Once the proposed decision is approved (step 1 above), the Commission proposes to make public the text of the draft decision, and supporting documentation, by the time the draft goes to the EDPB. Therefore, from that stage the process will become more transparent, and the views of many stakeholders may be put to the various EU bodies. In relation to the US Privacy Shield decision, such inputs led to a re-opening of negotiations and amendments to the draft decision.

The role of the EDPB under GDPR art. 70(1)(s) is of particular importance, since it must make an independent assessment, which may 'identify insufficiencies' and 'propose alterations' to the Commission's proposals:

> '… the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country. The EDPB will provide an opinion on the European Commission's findings in due time and, identify insufficiencies in the adequacy framework, if any. The EDPB will also endeavor to propose alterations or amendments to address possible insufficiencies.'[6]

Given these numerous procedural steps, and the independent EU bodies involved, it is possible that substantive objections to the Commission's current plans (and the substance of the agreements it has obtained from Japan) may still require amendments to the proposal before it is finalized.

Japan's initial request for a positive EU adequacy assessment was made when the EU Directive was still in force, but it is now to be decided under the GDPR. In December 2017, I identified four potential problems with Japan's case for adequacy:[7] (i) uncertain scope; (ii) exemptions for some EU personal data (including 'anonymous' data); (iii) weak and untested enforcement mechanisms; and (iv)'onward transfers' based on APEC-CBPRs. Adequacy decisions are very complex and lengthy, so I did not suggest any conclusions on Japan's adequacy. This was not a comprehensive assessment, and it noted that the European Commission was likely to also focus on other issues, which it has done with at least (v) sensitive data; (vi) retention of data; (vii) secondary uses; and (viii) law enforcement access.

---

[5] GDPR Art. 58(5); see Article 29 Working Party *Adequacy Referential*, 6 February 2018 (18 EN WP 254 rev. 01), Chapter 2, which notes that in Case C- 362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015 (§ 65) the CJEU found that it was incumbent upon national legislatures to provide legal remedies enabling such challenges.

[6] Article 29 Working Party *Adequacy Referential*, 6 February 2018 (18 EN WP 254 rev. 01), Chapter 2.

[7] Greenleaf 'Questioning 'Adequacy' (Pt I)- Japan' (2017) 150 *Privacy Laws & Business International Report*, 1, 6-11 <https://ssrn.com/abstract=3096370>. A subsequent analysis was made of the same issues in relation to Korea: Greenleaf 'Questioning 'Adequacy' (Pt II) – South Korea' (2018) 151 *Privacy Laws & Business International Report* <https://ssrn.com/abstract=3102070>.

Japan's proposed Supplementary Rules, and their enforceability

Japan's DPA, the Personal Information Protection Commission (PIPC) responded to some of these issues by proposing to make a set of Supplementary Rules[8] under its *Act on the Protection of Personal Information* (Japan) (PPIA). They are a major factor on which the European Commission has concluded that Japan's legal system can be considered to provide adequate protection under the GDPR. The draft Rules were available for comment, in Japanese, from 25 April 2018, but had not been made available for public distribution in English before the announcement on 17 July. They are included in the Appendix to this article.

The preamble to the PIPC's Supplementary Rules asserts that the PIPC has the necessary legislative power to make them (particularly art. 6); that they 'are binding' on data controllers in Japan receiving personal information from the EU based on an adequacy decision; and that the PIPC can treat breaches of the rules 'without legitimate ground' as a 'serious infringement' (PPIA, art. 42(2)). However, the rules cannot be enforced if the data controller 'has taken alternative action that fully remedies the violation', because this is 'legitimate grounds' for non-enforcement.[9]

Despite these assertions, some Japanese experts question whether the Supplementary Rules are binding.[10] EU authorities will need expert independent Japanese advice on this question, including relevant case law.

Improving transparency

The non-availability of Japan's draft Rules in English prior to the EU Commission proposing an adequacy decision was unfortunate in this instance. Third parties (academics, NGO's, business organisations) can raise problems that it may be difficult for the Commission to state publicly during its discussions with countries applying for adequacy findings. They may identify issues that the Commission has not understood fully. These benefits can only be realised in full if key documents (particularly draft legislation) are made available in commonly-understood languages prior to adequacy findings being announced.

Although the Commission proposes to make information about proposed adequacy decisions available at the time the draft decision is announced publicly and goes to the EDPB, this is too late to be optimally useful. Ideally, the Commission could make key documents (including key legislation in English), and a list of differences between the GDPR and the laws of the candidate country (without needing to label them as 'issues') once the adequacy process is officially underway but before a draft decision is made. This is particularly relevant to situations such as this one, where a press release announces the substance of a draft decision before the draft decision and supporting documents are available.

---

[8] PIPC (Japan) [Draft] *Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision*, 25 April 2018..

[9] PIPC Supplementary Rules, p4, footnote 2.

[10] For example, see Professor Shizuo Fujiwara 'Comparison between Japan and EU in the Personal Information Protection Legal Regimes' *Jurist* vol. 1521, July 2018, pp.14-19. (in Japanese). 藤原静雄「日本とEUの個人情報保護法制の比較」ジュリスト1521号（2018年7月）14-19ページ。

Unknown scope of adequacy in relation to the public sector

It has been assumed that Japan is only seeking an adequacy assessment for its private sector because the PIPC does not have powers over the public sector.[11] The Supplementary Rules have no application to public sector bodies. Under Japan's 2015 revisions to the PPIA, supervision of the public sector is by the Ministry of Internal Affairs and Communications (MIC), except that the PIPC can ask for reports to be made to MIC, so there is no independent DPA in relation to the public sector.[12] A comprehensive adequacy assessment for both private and public sectors is therefore unlikely without amendments to the PPIA..

However, the Commission states that there will be a 'complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities' and that this 'new mechanism will be administered and supervised by the Japanese independent data protection authority'[13] (the PIPC), reiterating that this will 'ensure that potential complaints from Europeans as regards access to their data by Japanese law enforcement and national security authorities will be effectively investigated and resolved'.[14] It is not clear where in PIPA the PIPC's authority for such regulation is found. The Commission also states that 'personal data exchanged for law enforcement purposes between EU and Japanese authorities' will be covered 'ensuring that in all such exchanges a high level of data protection is applied'.[15] EU law requires that there must be some independent oversight mechanism, with effective remedies to individuals, operating there as well.[16]

Details of these new mechanisms are unknown, another instance of it being impossible to assess whether these claims are realistic on the basis of a press release. Neither the Commission nor Japan has made a formal announcement about the scope of Japan's application, so at this stage it is uncertain to what extent (and how) an adequacy proposal will go beyond Japan's private sector. Exactly what has the Commission decided has adequate protection will not be known until the draft decision is released.

Benefits for 'Europeans' (only) from the Supplementary Rules

Because the PIPC has legislative authority to make 'stricter rules that supplement and go beyond those laid down' in the PPIA,[17] it is able to make 'the present Supplementary Rules providing for a higher level of protection of an individual's rights and interests regarding the handling of personal data received

---

[11] Effect of PPIA art. 2(5) definition of 'business operator handling personal information', which excludes public sector bodies.

[12] Japan's public sector privacy legislation, the *Act on the Protection of Personal Information Held by Administrative Organs*, is enforced in relation to security breaches, and is effective in giving individuals access to their own records, where there is a well-used Review Board: see Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 252-3.

[13] European Commission, Press Release, 17 July 2018.

[14] European Commission Fact Sheet 'Questions & Answers on the Japan adequacy decision' Tokyo, 17 July 2018.

[15] European Commission, Press Release, 17 July 2018.

[16] Article 29 Working Party *Adequacy Referential*, 6 February 2018 (18 EN WP 254 rev. 01), Chapter 4.

[17] Supplementary Rules, preamble, referring to art. 6 PPIA.

from the EU based on an adequacy decision.'[18] In other words, it can make special rules that only benefit the data subjects of data received from the EU (roughly speaking, 'Europeans') and which do not benefit those whose data is collected in Japan ('Japanese') or those whose data is received from elswhere ('other foreigners').

However, if personal data is received from the EU by means other than an adequacy decision (under GDPR art. 45), for example by transfers subject to appropriate safeguards (GDPR art. 46), then the Supplementary Rules do not apply. Any transfers from the EU to Japan (under agreements between public bodies, standard clauses or BCRs etc), will therefore need to include special protections equivalent to those in the Supplementary Rules (since the Commission has found such protections to be necessary), or they will be in breach of the general principles for transfers in GDPR art. 44. They will no longer be 'standard' clauses or BCRs, but special Japanese-flavoured ones. It may be simpler not to use such clauses or BCRs, and to rely on the adequacy decision instead.

Taking this approach, four Supplementary Rules provide 'Europeans' with four significant extra protections.

(i) ***Additional special categories*** – Data concerning a natural person's sex life or sexual orientation or trade-union membership, which are defined as special categories of personal data under the GDPR art. 9, are now given the same extra protections as special categories of personal data in PPIA art. 2,[19] although these are rather limited.[20]

(ii) ***Preservation of protections*** – In general, data received from the EU under an adequacy decision is categorised as 'retained personal data' irrespective of when it is scheduled to be deleted, and therefore the protections in PPIA arts. 27-35 (many of the most important in the Act) will continue to apply with no time limit.[21]

(iii) ***Limits on purposes of use of received data*** – One of the weakest aspects of PIPA is the exception allowing disclosure of personal information to third parties, simply by a business giving notice of such disclosure via a website, with an option to the data-subject to opt out. This was strengthened only slightly in the 2015 amendments, with businesses now required to notify the PIPC when they do this, and the PIPC must 'publicly announce' that it has occurred. The Supplementary Rules revoke this in relation to data received from the EU under an adequacy decision, to the general effect that the original

[18] Supplementary Rules, preamble.

[19] Supplementary Rules, Rule 1; For the limited extra protections provided in PPIA,

[20] see G Greenleaf 'Japan: Toward international standards – except for 'big data'' (2015) 135 *Privacy Laws & Business International Report* 12-14 <https://ssrn.com/abstract=2649556>

[21] Supplementary Rules, Rule 2.

purpose for which data was collected in the EU sets the limit on the purposes for which it can be used in Japan.[22]

(iv) ***'Anonymously processed information' (API)*** – In an effort to give wide scope to the use of 'big data', the 2015 version of PPIA, art. 2(9), defines 'anonymously processed information' (API) as data which has supposedly been de-identified by following one of two procedures. However, it is contentious whether they would achieve the desired result. PPIA then provides much less protection to this API than is provided to 'personal information' (PI).[23] Defining anonymous information via a process to be followed, rather than by a result to be achieved (GDPR Recital 26: 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'), is not compatible with the GDPR because it can result in data which would be PI under the GDPR not being so protected under PPIA. The Rules remedy this by redefining art. 9(2), in relation to data received from the EU under an adequacy decision as requiring that the controller 'takes measures that make the de-identification of the individual irreversible for anyone', including by the two methods specified in PPIA (assuming they are effective in achieving irreversibility). In other words, a procedure has been replaced by a result, so Japan is providing the same level of protection as the EU.

Must personal information be 'readily' collated under the GDPR?

A related issue is that Japan's definition[24] of 'personal information' says that it includes information 'containing' specified items 'whereby a specific individual can be identified (including those which can be *readily collated* with other information and thereby identify a specific individual)' (emphasis added). Other translations refer to '*easy* reference.' If information in two documents cannot be 'readily' (or 'easily') collated/cross-referenced, the information is not personal information, and is outside the scope of the PPIA or any privacy controls. So if such data was imported from the EU, it is not personal information, and no restrictions apply. There are no cases or guidelines known on what 'readily/easily' means.

The GDPR's definition of 'personal data' in art. 4(1) refers to a person 'who can be identified, directly or indirectly' without any qualifier such as 'readily', and Recital 26 says that in order to determine whether a person is identifiable, 'account should be taken of all the means reasonably likely to be used' (including all 'objective factors' such as costs, time, and technology). This appears to be a broader definition than Japan's requirement that persons be 'readily' identifiable, so there is a risk that what would be 'personal data' in the EU will not be 'personal information' when it is exported to Japan. This is not addressed

---

[22] Supplementary Rules, Rule 3.

[23] Greenleaf 'Japan: Toward international standards – except for 'big data', section titled " 'Anonymous processed information': Trying to define 'big data' processing".

[24] Act on the Protection of Personal Information (Japan) (PPIA), art. 2(4); Taken from the most authoritative translation of PPIA (Translation date: December 21, 2016), on *Japanese Law Translation* website (operated by Nagoya University with government funding) <http://www.japaneselawtranslation.go.jp>.

by the Supplementary Rules. Perhaps the European Commission will explain in its draft decision which it considers this is not a problem for adequacy.

Enforcement effectiveness

The GDPR art. 45(2)(a) refers to the requirements of 'effective and enforceable data subject rights and effective judicial and administrative redress for the data subjects whose personal data are being transferred', and art. 45(2)(b) refers to the need for an independent supervisory body to have 'adequate enforcement powers'. The Article 29 Working Party *Adequacy Referential*[25] (now adopted by the EDPB[26]) states that 'efficient enforcement mechanisms are of paramount importance', and that 'the means for ensuring … effective application' are one of the 'two basic elements' of adequacy protection. The *Referential* states that infringements should be 'punished in practice' and that 'the data subject should be provided … with effective administrative and judicial redress, including for compensation for damages'. It describes this as 'a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate'.[27] The emphasis is on effectiveness, not mere paper compliance, and presumably it must be able to be demonstrated.

In a study of the enforcement of Japan's law in 2014, Prof. F Shimpo and I argued[28] that Japan's system 'does not provide evidence of its effectiveness'. We concluded that Japan's 'enforcement mechanisms are not used to any significant extent, and the mechanisms by which most of the enforcement measures work are obscure,' resulting in 'a system that asks observers to take it on trust that it is effective.'

The 2015 amendments to the PPIA strengthened its enforcement provisions, most notably by the creation of a data protection authority (the PIPC) with powers to investigate make recommendations and give directions to businesses (replacing similar powers previously held by individual Ministries in their sectors). The PIPC was given no powers to issue administrative penalties or fines. Some criminal penalties were added (arts. 82-88), but none exceed a trivially small maximum fine of ¥1M (US$9,900). There are no explicit provisions under PPIA for data subjects to seek financial compensation, either from the PIPC or from the courts. A 2017 report by a European Parliament delegation to Japan did not refer to any prosecutions or compensation actions in relation to the Japanese privacy sector.[29] The 2015 enforcement powers are

---

[25] Article 29 Working Party *Adequacy Referential*, 6 February 2018 (18 EN WP 254 rev. 01), Chapter 1.

[26] EDPB *Endorsement of WP29 Documents*, Endorsement 1/2018, 25 May 2018.

[27] Article 29 Working Party *Adequacy Referential*, 6 February 2018 (18 EN WP 254 rev. 01), Chapter 3 part C.

[28] G. Greenleaf and F. Shimpo ' The puzzle of Japanese data privacy enforcement' (2014) 4(2) *International Data Privacy Law*,139–154 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3086490> ; see also G Greenleaf *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (OUP, 2014) Chapter 8 'Japan – The Illusion of Protection'.

[29] It did refer to one complaint against Police resulting in a 40,000 euros payment; European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) *AD-HOC DELEGATION REPORT following the mission to Tokyo (Japan) 30 October – 3 November 2017*, 5 December 2017 (32 pgs), Pt X,

essentially a continuation of the limited enforcement position since 2003, but with the PIPC now playing a central role.

Prior to the 2015 amendments, Japanese courts had refused to provide tort law remedies, including compensation, for breaches of the PPIA.[30] A 2007 Tokyo District Court decision held that a breach of the PPIA did not in itself give rise to a civil cause of action. It is unknown whether the PPIA 2015 changes could lead to a different result. Actions under Civil Code art. 709 have resulted in tort remedies analogous to some types of breaches of PPIA, but actions for most types of breaches would not be likely to succeed. It is a scatter-shot partial tort remedy only, providing few precedential examples.

This is again demonstrated in the June 2018 Tokyo District Court decision refusing compensation concerning one of the most significant data breaches in Japan, the 2014 Benesse leak of 35 million data items concerning customers and their children. The Judge held that details of names, birth dates and addresses of parents and children were 'not private enough' to have caused significant psychological distress, and there was no evidence of online circulation of the data.[31]

Also, since most new aspects of enforcement only came into effect in May 2017, there has as yet been only one year for the Japanese system to demonstrate the extent to which these limited mechanisms will actually be used, and that the failures of enforcement in the past have been reversed. Whatever may be the position in a few years time, given Japan's demonstrably poor record of enforcement in the past, it must be seriously questioned whether the GDPR's enforcement requirements have as yet been met. Perhaps they are not capable of being met given PPIA's continuing weaknesses in enforcement powers and remedies. Should an adequacy assessment take on trust that there will be future stronger enforcement? As yet, no information is available on what approach the European Commission has taken to this issue 'of paramount importance'.

Onward transfers – Closing the Japanese back-door

The GDPR art. 44 ('General Principles') singles out 'onward transfers' from a third country to another third country as a form of processing which requires compliance with the conditions of Chapter V. In other words, onward transfers must in themselves be the subject of an adequacy decision, or be protected by 'appropriate safeguards', or BCRs, or within arts. 48-50.

Restrictions concerning overseas transfers of personal data were added for the first time to Japan's law in 2015 (art. 24). There are two justifications for overseas transfers relevant here:[32] (i) the business can obtain the consent of the data subject to their personal data being provided to 'a third party located in a foreign country' (no notifications or other conditions are specified); or (ii)

[30] For details, see Greenleaf *Asian Data Privacy Laws*, pp. 258-9.

[31] Takuya Kitazawa 'Court: Data in Benesse leak not private enough for redress' *The Asahi Shimbun*, June 21, 2018 <http://www.asahi.com/ajw/articles/AJ201806210042.html>.

[32] Two other bases for exports are hypothetically relevant: (iii) a country included by PIPC Rules in a 'White List' of countries acknowledged as providing equivalent privacy protection to Japan's law (no list yet exists); or (iv) exceptions listed in art. 23(1), based on statute or the protection of others.

provision to overseas businesses that are 'establishing a system' complying with the PIPC Rules for a business to 'continuously take action' to provide equivalent protection.[33] The relevant PIPC Rules, art. 11(2) refer to when 'a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information', and the PIPC Guidelines[34] confirm that APEC's Cross-border Privacy Rules system (APEC-CBPRs) is such an 'international framework' under art. 11 of the Rules.[35]

Therefore, if a Japanese business proposes to export personal data to a CBPR-certified business in a country which participates in APEC CBPRs (only the US as yet), then it can do so, provided it complies with other aspects of Japan's PPIA. At present, this applies only to 19 businesses in the US.[36]

The problem this raised for adequacy is that certification under the APEC-CBPRs system is based on standards which are unarguably weaker than those of the GDPR. Therefore, Japan's data export rules allowed a 'back-door' means of onward transfer of personal data to companies in the US (and eventually perhaps elsewhere) without the protection of adequate laws or appropriate safeguards. However, the European Commission has acknowledged that the APEC-CBPRs standards are too low to meet those of the GDPR, and has stated that an adequacy decision cannot include onward transfers based solely on APEC-CBPRs certification.[37] The Japanese back door has to that extent been shut.

The resolution of this problem, proposed in Japan's Supplementary Rules, and accepted by the European Commission, is to add a requirement of consent obtained from the EU data subject whenever the onward transfer is of data which has been received in Japan as a result of an adequacy decision. Supplementary Rule 4 requires that the Japanese controller 'shall obtain in advance [an EU data subject's] consent to the effect that he or she approves the provision to a third party in a foreign country pursuant to art. 24 [of PPIA] after having been provided information on the circumstances surrounding the transfer necessary for the [individual] to make a decision on his or her consent'. This will apply to both transfers which would have taken place under CBPRs and those which could otherwise have taken place simply by consent.

---

[33] Technically in the words of the section, 'as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section'; (Article 24 PPIA).

[34] PIPC *Guidelines on the Act on the Protection of Personal Information (Provision to the third party in a foreign country)* November 30, 2016 <http://www.ppc.go.jp/files/pdf/guidelines02.pdf>. The full Guidelines are available only in Japanese. Prof Hiroshi Miyashita has kindly provided an English translation of the Guidelines in relation to art. 11.

[35] PIPC Guidelines 3-3 I states in relation to Art 11 (2) of the Rules (from Prof Miyashita's translation): 'A recognition based on an international framework concerning the handling of personal information" means the one recognized by the competent accreditation organizations based on the agreed rules of the international organizations. This framework requires the continuous measures equivalent to the one that the personal operators have to take. This recognition applies to the certification of APEC CBPRs system of the third party as the importer in the foreign country.'

[36] TrustArc (formerly TRUSTe), *APEC Certified Companies* <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> (as at 19 July 2018, down from 21 as at 5 December 2017).

[37] Verbal comments by Mr Bruno Gencarelli, head of the International data flows and protection unit, European Commission, at Privacy Laws and Business Annual Conference, St Johns College, Cambridge, 2 July 2018, in the session on 'threats to adequacy'.

This proposed resolution can be criticised on three grounds: (i) the vagueness of the consent arrangements; (ii) the lack of GDPR remedies; and (iii) whether consent should be the only basis for onward transfers.

First, the obligations to inform the EU data subject about a transfer from Japan to a country with no meaningful data protection (ie the US) are vague: 'information on the circumstances surrounding the transfer necessary for the [individual] to make a decision on his or her consent'. There is no explicit requirement to inform the EU data subject that it is the US to which their data will be sent; that the US has no legislative protections; that other protections (contracts, BCRs etc) will not be required; nor that the data never need be destroyed. Of what they are to be informed is, and will remain, unknown. This vagueness falls short of GDPR requirements in comparable situations, such as the considerable details in notice on data transfers to third countries (GDPR art. 13(1)(e)); or the required unbundling of consents (art. 7(2)); or that the consent obtained must comply with the GDPR definition of 'consent' (art. 4(11)); or the requirement of warnings of possible risks of international transfers due to lack of adequacy decisions or appropriate safeguards (art. 49(1)(a)).

Second, even though the consent must be obtained in the EU, it is not a requirement of the GDPR that it be obtained, so why should the GDPR apply to it being obtained? Therefore, although the obtaining of the consent is carried out by an EU controller, it seems that no GDPR sanctions would apply because it is a requirement of Japanese law that the proper consent by obtained. It is hard to see that any sanctions under Japanese law could be effective against an EU controller. In short, this seems to be a requirement that is notional, with no enforceability.

These first two issues could be dealt with by the EU making the obtaining of consent for onward transfers required by the GDPR, with all desirable notice and consent requirements, and consequent enforcement for breach. This could be via a delegated act (GDPR Pt X), or it could be part of a more general technical revision regulation.

The third and separate issue is whether consent can be the sole basis for onward transfers, consistent with the letter and spirit of Chapter V? Consent is not in itself one of the bases for transfers to third countries in arts. 44-50, which is of concern given the emphasis on onward transfers in art. 45. The only appearance of consent in Chapter V is in art. 49(1)(a) which deals with consent as the basis of international transfers only 'in the absence of an adequacy decision' and (as above) requires 'explicit' consent involving warnings of risks. This is in the context of 'derogations for specific situations' and is to apply to 'a transfer or a set of transfers' (art. 49(1)). The EDPB says 'the derogations must be interpreted restrictively so that the exception does not become the rule'.[38] 'Consent' is therefore a constrained exception to the normal rules for transfers to third countries, and specifically where no adequacy decision is involved. It is hard to

[38] EDPB *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018, pg 4; See FN 7 for details of CJEU decisions to the effect that 'derogations … should apply only in so far as is strictly necessary'.

see how it can become the central rule for onward transfers as part of an adequacy decision, and a largely unconstrained rule at that.

The result is that, although it is the intention of the Commission to shut the 'Japanese back door' of onward transfers based solely on APEC-CBPRs certification (and it has succeeded in doing so, which is a considerable achievement), its replacement with a vague consent requirement has left the door half open to transfers to the US with insufficient protection.

Can 'essentially equivalent' protection apply only to Europeans?

As explained above, Japan's approach in the Supplementary Rules is to strengthen its law only in relation to data received from the EU, and thus primarily for citizens of EU countries, and not for the personal data generated in its own country and concerning its own citizens. Japan is taking the narrowest possible path to an adequacy assessment by making any strengthening of its law such that few Japanese citizens will normally benefit from these stronger provisions. This raises the question of whether laws can give 'essentially equivalent' protections (*Schrems*) within the meaning of the GDPR, while failing to provide such protections to their own citizens? *Privacy Shield* raises similar questions. Is such narrow protection for 'EU data only' more properly dealt with by contracts or BCRs rather than adequacy? It is also possible that such a discriminatory approach might not be popular in Japan.

Further, all five Supplementary Rules apply only to data 'received from the EU based on an adequacy decision'. If data is received from the EU based on Contractual Clauses or BCRs it will not receive 'EU-like' protections under these Rules. It will be necessary to look to the contract or the BCR to see exactly what protections apply. EU controllers may need to know not to use their usual Contractual Clauses or BCRs, but to rely on adequacy instead. The result may be confusion: will data users in Japan knows which rules apply to which data?

Conclusions

This short article, dealing primarily with developments in the past few weeks, has raised a number of issues which cannot be resolved without further consideration of fundamental questions about the purpose of 'adequacy', and the release of the draft adequacy decision and supporting documents by the Commission. However, these issues indicate that there are serious questions which EU bodies still need to consider in relation to the adequacy proposal concerning Japan, even though the Commission has made significant progress in obtaining stronger rights for EU citizens.

The trade agreement reached between the EU and Japan will deliver significant benefits to both, and if mutual adequacy decisions can also be reached they will complement that agreement. However, this is the first adequacy decision which has been proposed under the GDPR, and it is more important for EU institutions to reach a decision which is correct and defensible against possible claims of invalidity before the CJEU, and which will indicate good practices for future decisions, than it is to finalise a decision concerning Japan in a politically attractive short time-frame. The adequacy processes under the GDPR still have

some distance to run, and may prove valuable. The best result will be a significantly strengthened adequacy decision.

Appendix: PIPC (Japan) (Draft) Supplementary Rules

PIPC (Japan) [Draft] *Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision*, 25 April 2018