Japan: EU Adequacy Discounted

GRAHAM GREENLEAF

(2018) 155 *Privacy Laws & Business International Report* 8
[2019] *UNSWLRS* 5

UNSW Law
UNSW Sydney NSW 2052 Australia

Japan: EU adequacy discounted

The first adequacy decision under the GDPR will be watched carefully all over the world as to what 'GDPR-adequate' means. By **Graham Greenleaf**.

The European Commission formally commenced EU procedures for the adoption of a positive adequacy decision concerning Japan under the GDPR – potentially the first such decision – on 5 September 2018.[1] Its draft adequacy Decision[2] includes additional measures which Japan has committed to implement – a set of Supplementary Rules issued by Japan's Personal Information Protection Commission (PPC), applicable only to personal data transferred from the EU, and binding on companies in Japan importing such data.[3]

This article focuses on these aspects of the draft Decision concerning the private sector, arguing they do not contain sufficient justification that Japan meets the EU's criteria for adequacy, described in the Decision as requiring that Japan "guarantees a level of protection 'essentially equivalent' to that ensured" within the EU.[4]

Public sector access

The draft Decision also includes a set of assurances ("signed representation") by Japanese government authorities, described as "regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms";[5] and "a complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities", a new mechanism to be administered by the PPC.[6] These provisions on public sector access to personal data transferred to Japan[7] are complex and beyond the scope of this article.

Issues insufficiently addressed by the draft

Some of these criticisms have been raised by me previously, at greater length.[8] The draft Decision does not sufficiently dispose of them. They are discussed here in approximate order of importance.

1. How is Japan's enforcement regime 'essentially equivalent' to the EU? GDPR art. 45 explicitly requires "effective and enforceable data subject rights" and "effective judicial and administrative redress". The EDPB states that these are "of paramount importance" and that infringements "should be punished in practice" and compensation awarded.[9] Despite it being clear that enforcement and redress must be demonstrated in practice, and not only exist on paper, the draft Decision ignores this. It lists many examples of where the PPC or the courts can, in theory under legislative provision, take enforcement actions, but it does not give any examples of specific penalties issued or compensation granted, either administrative or judicial.[10] If this legislation is being enforced, why are there no concrete examples of fines and compensation? Before Japan's 2015 amendments and creation of the PPC, there were no such examples. On the evidence provided by the draft Decision, there have been none since then. It is no explanation to say that Japan relies on criminal prosecutions (unlike the EU), because there are no examples of those either.

A related issue is whether, even if it was enforced, a law which has maximum penalties for breaches of under US$10,000 in the Act (or US$3,000 in the Supplementary Rules) is capable of being "essentially equivalent" to the GDPR where penalties are some orders of magnitude higher? Suggested cultural differences might help explain differences in the quantum of penalties, but cannot explain complete non-enforcement. Nor are they convincing when penalties must dissuade companies with global operations from breaches, not just Japanese companies. The draft Decision does not address these significant questions.

2. Is consent a sufficient basis for an onward transfer regime? A strong aspect of the draft Decision is that it makes it clear that the "Japanese back door", which allows personal data exports from Japan to overseas companies merely because they are certified under the APEC CBPRs scheme, has been shut in relation to any data originating from the EU.[11] Such onward transfers now require the consent of the individual data subject in the EU. I have criticised this on three grounds.[12] First, the draft Decision claims that they will be "particularly well informed" because Supplementary Rule (4) requires that the individuals concerned shall be "provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent".[13] However, there is no obligation to tell the person that their data will be transferred to a country with very weak privacy laws such as the US. Second, the Supplementary Rule is under Japanese law, so there is no obligation to comply with GDPR requirements for consents, and no GDPR enforcement provisions will apply. The third, broader, issue is whether consent should be the principal basis for an onward transfer regime. Under the GDPR, consent is not a basis for transfer to third countries, but is only a very constrained derogation, which the EDPB considers must remain the exception not the rule.[14] These issues are not discussed in the draft Decision.

3. Can an "essentially equivalent" law exclude Japanese citizens? The PPC's Supplementary Rules only apply to personal data originating from the EU (thus probably primarily affecting EU citizens), and do not operate to provide their higher level of protections to personal data sourced from Japan, or from other foreign countries. The question of whether the concept of "essentially equivalent" protections, as required by the GDPR and the CJEU, can be satisfied by laws which, in effect, give a lower level of protection to Japanese citizens, is not addressed in the draft Decision. Is such an approach more suited to BCRs or standard contracts than to adequacy? The Commission

says it is "Japan's choice" to take this approach,[15] but it is ultimately a question of the CJEU's interpretation of the GDPR. If insistence on changes which are not restricted to EU-sourced data is considered to be likely to breach the EU's GATS art. 14 obligations, the Decision should state this.

4. "Readily collated" personal information: The requirement that information be "readily collated" (or "easily collated" in some translations) in Japan's definition of "personal information" could mean that some data which is protected as "personal information" under the GDPR is not protected under Japan's law.[16] The draft Decision quotes the PPC's Guidelines to the effect that the test is what collation could be performed by the average or normal business operator,[17] but does not set out what the GDPR requires (primarily in art. 4(1) and Recital 26), nor assess whether the Japanese approach is consistent with this.

5. 'Sectoral' exclusions from PPIA: The Decision will not apply to a very broad range of categories of business operators when they are processing personal data for specified purposes, as defined by art. 76 of Japan's law.[18] The Decision will still apply to the same business operators processing information for other purposes.[19] The draft Decision does not evaluate which of the art. 76 exclusions have parallel GDPR exemptions (some may). To the extent they do not, this device deals with divergences between Japanese and EU law simply by the Decision not applying to some processing. It raises another question of what "essentially equivalent" means.

6. Reliability of translations: It is essential that translations on which an adequacy Decision is based are as reliable as possible. The translation of the PPIA states that it has "neither had its texts checked by a native English speaker nor legal language editor, and thus may be subject to change", and that only the "Japanese original legal texts" are in force.[20] While "official" English translations, with equal standing to the Japanese text, are not possible, the Decision should state what the Commission has done to ensure the translation is accurate (including reliance on expertise available to it[21]). This also applies to the Japanese version of the Supplementary Rules, which are presumably authoritative. The authority given for the Supplementary Rules being legally binding and enforceable is that the Rules themselves say so, as does the PPC,[22] but since this has been questioned by some Japanese experts,[23] it would be appropriate for some independent expert opinion to be cited in the draft Decision.

7. Other gaps between Japanese and EU laws: The draft Decision is very thorough in explaining where and why Japan's laws meet GDPR standards. Nevertheless, there remain apparent "gaps" between the GDPR and explicit provisions of Japan's laws, including: requirements for data protection by design and by default; data portability; mandatory DPIAs; mandatory DPOs; and de-linking ("right to be forgotten"). There is mention of very weak protections for automated decision-making, with very limited scope,[24] and data breach notification requirements which are voluntary and cover only some industries.[25] While it is clear that "essentially equivalent" protection does not require the inclusion of every GDPR innovation, the draft Decision does not explain why those omissions and weaknesses should not prevent a positive adequacy assessment here. For the first adequacy Decision under the GDPR, this approach does not result in a convincing case for Japan's adequacy, nor give a valuable guide to what is required for "essentially equivalent" protection.

"I'll have what Japan's having": Adequacy discounted

Some of the above questions are very difficult, and it is no discredit that the draft Decision does not provide fully satisfactory answers to all of them. However, the first adequacy decision under the GDPR will obviously be watched carefully all over the world as to what "GDPR-adequate" means, and to what extent that can fall short of full "GDPR-compliance".

If the draft Japanese Decision was adopted "as is", what conclusions might be drawn by some governments in other countries that are planning to amend or enact data privacy laws with adequacy in mind? A legal adviser taking a resolutely cynical view could argue that the Japanese Decision suggests the following:

1. While "essentially equivalent" must be recited in various formal parts of a Decision, it does not carry its ordinary meaning, nor have any obvious operational effect in Decisions.[26]
2. A Decision will repeat statements from the applicant country's government or DPA, without documenting any expert independent substantiating advice, although such advice would be possible, may have been obtained, and would increase confidence in the Decision.
3. Deficiencies in a country's data protection law can be overcome by a regulation which applies only to personal data originating from the EU, but in effect has no application to the country's own citizens or residents.
4. Import of data from the EU for processing not permitted under EU law can be removed from the scope of a Decision, thus reducing the Decision's "sectoral" scope in very complex ways.
5. Enforcement only requires formal provisions on paper, without need for evidence of enforcement in reality.
6. Very small maximum penalties (administrative fine or criminal offence) are acceptable, despite the administrative fines in the GDPR being orders of magnitude higher.

Such a resolutely cynical assessment would unfairly gloss over the Decision's painstaking documentation of the numerous similarities between the Japanese and EU systems, and also omit the considerable improvements negotiated by the Commission (though only for the benefit of EU citizens). However, a Decision such as this may encourage other countries to prefer to obtain a "Japanese adequacy decision", rather than go to the trouble of enacting or amending data privacy laws so that they really are substantively similar to the GDPR and applied to all data processing within their borders. "I'll have what they're having" may be the response of some countries to such a Japanese adequacy Decision, if such a "work-around" is possible. Some business groups may

advocate such an approach. Under the Directive, the only country to obtain an adequacy assessment through comparable devices was the US, and that approach is still under challenge.

I previously concluded that "the best result will be a significantly strengthened adequacy decision". This would require Japan to strengthen the protections it provides, which the PPC appears to be able to do under the 25 April 2018 Cabinet decision, and to demonstrate a willingness to enforce. It would require the Commission to strengthen of the quality of its Decision, moving away from the rather passive approach of not engaging with issues it could have taken up in its draft Decision, even if a more explicit approach is less diplomatic. It would require all EU institutions to consider some fundamental questions about the meaning of both adequacy and "essentially equivalent", in the course of improving or rejecting this draft Decision. Drawn-out CJEU litigation is best avoided. It does not matter if these processes take longer than desired; the long-term integrity of the GDPR requires a Decision concerning Japan which is sound in both principles and details. It need not impede progress on other adequacy decisions, and there may be some advantages in Japan losing its "first mover advantage": hard cases make bad law.

REFERENCES

1 European Commission Press Release 'International data flows: Commission launches the adoption of its adequacy decision on Japan', 5 September 2018, available together with all supporting documents mentioned below at ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
2 'Draft adequacy decision - Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan'
3 'Annex I - 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'.
4 Draft Decision, para. (3), citing GDPR Recital 104.
5 'Annex II - Signed representation', as described in Press Release.
6 Set out in Annex II, pp. 17-19 (Part IIC(5)).
7 Draft Decision, paras. (113)-(170).
8 See G. Greenleaf 'Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles' (2018) 154 *Privacy Laws & Business International Report*, 1, 3-8; extended online version at ssrn.com/abstract=3219728; see also G. Greenleaf Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 *Privacy Laws & Business International Report*, 1, 6-11.
9 See Greenleaf, 2018, p. 7.
10 Draft Decision, paras. (95)-(112)
11 Draft Decision , para (79); see Greenleaf 2018, pp. 5-7 for reasons why this was necessary.
12 Greenleaf, 2018, p6.
13 Draft Decision , para (76).
14 Greenleaf, 2018, p.6.
15 Commission statement (B. Gencarelli) to the EU Parliament LIBE Committee, 26 September 2018.
16 Greenleaf, 2018, p. 7.
17 Draft Decision, para. (18).
18 'Those categories are defined by using a double criterion based on the type of data controller processing the personal information and the purpose of processing:' draft Decision para. 36.
19 Draft Decision, paras. (37)-38).
20 PPIA, available at www.ppc.go.jp/en/legal/
21 Commission statement to the LIBE Committee (above).
22 Draft Decision, paras. (15)-(16).
23 Greenleaf, 2018, p. 5, citing Prof. Fujiwara.
24 Draft Decision, paras. (93)-(94)
25 Draft Decision, paras. (7), (58), (73).
26 There are only four mentions of "essentially equivalent', all formal (paras. (3), (171), (176), 184)), none substantive.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Norway takes active role on the European stage

Norway adopted a GDPR-compliant national data protection law sooner than several EU countries. Its DPA actively participates in the EU mainstream. **Stewart and Merrill Dresner** report from Oslo.

Bjørn Erik Thon, Data Protection Commissioner, and Jørgen Skorstad, Head of the Legal Department at the Datatilsynet (the DPA) explained that although the new Personal Data Act, number 38, was adopted on 15 June this year, its entry into force was delayed until 20 July due to the need for coordination with its European Economic Area (EEA) partners, Iceland and Liechtenstein. The GDPR was formally adopted in the EEA by way of a Joint Committee Decision

Continued on p.3

US CLOUD Act creates global data access framework

US law enforcement agencies can compel tech companies subject to US jurisdiction to disclose communications data stored overseas. By **Kurt Wimmer** and **Katharine Goodloe** of Covington & Burling LLP.

In March 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act[1], a new statute creating a framework for government access to data held by technology companies worldwide.

The CLOUD Act has two distinct parts. Part I of the Act expands the geographic reach of certain US warrants issued to technology

Continued on p.5

Issue 155 **October 2018**