

Japan and Korea: Different paths to EU adequacy

Graham Greenleaf



Japan and Korea: Different paths to EU adequacy

The first two adequacy assessments of countries under article 45 of the GDPR are now at critical points. By **Graham Greenleaf**.

The European Commission will receive the Opinions and Resolution of other relevant EU bodies concerning its draft Decision on Japan by mid-December. It will then either make a final adequacy Decision this year, or take time to revise its draft Decision. The Korean legislature now has Bills (see p.12) before it to comprehensively restructure Korea's data protection system, which may result in it applying in 2019 for a much more comprehensive adequacy finding from the EU.

JAPAN: COMMISSION FAILS TO DEMONSTRATE ADEQUACY?

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) has resolved,¹ on the basis of the European Commission's draft Decision concerning Japan, and further communications with the Commission, that it is necessary for the Commission "to provide further evidence and explanation regarding [a list of criticisms], in order to demonstrate that the level of protection afforded by the Japanese data protection legal framework ensures an adequate level of protection". In short, it implies that the draft Decision fails to justify a positive adequacy finding. LIBE adopted the proposed Resolution by a 28 votes to 9 majority (with 7 abstentions). It will be put to the vote of the whole Parliament by mid-December, ahead of the final Adequacy Decision to be adopted by the Commission. The Parliament's Resolution is not binding on the Commission.

The LIBE Committee's main criticisms of the draft Decision are as follows (with paragraph numbers of the proposed Resolution in square brackets):

1. The Decision does not specify with sufficient clarity which transfers of EU personal data are within its scope, due to exclusions from Japan's law [7].
2. Japan's Supplementary Rules only apply to personal data transferred from the EU, so business operators in Japan who process both Japanese-sourced and EU-sourced personal data will therefore have to implement measures to identify such personal data throughout its life cycle (either technical tagging or organisational segregation). LIBE is concerned that operators may attempt to circumvent these obligations by transferring data via third countries, and says the Commission will need "to monitor the situation" [12]. However, unlike its draft version, LIBE's Resolution did not raise the question of whether having different sets of rules for EU-sourced and for Japan-sourced data meant that EU and Japanese laws were not "essentially equivalent".
3. The Commission should consider whether Japanese exceptions for data prescribed as having "little possibility of harming individuals' rights" are compatible with EU law [13].
4. The Commission should clarify whether all "personal data" within the GDPR usage of the term will come within Japan's definition of personal data [15], and if necessary seek further Supplementary Rules from Japan [16].
5. The Commission should demonstrate how Japan's limited sectoral rules on automated decision-making and profiling meet EU requirements [17].
6. The Commission should provide "in depth clarifications" in relation to Japan's lack of direct marketing provisions (considering EDPB adequacy referential) [18].
7. LIBE considers that the draft Decision's solution to the problem of onward transfers (namely "requiring prior consent on the part of EU data subjects for approval of onward transfer to a third party in a foreign country") lacks certain essential elements that would enable data subjects to formulate their consent, as it does not expressly define what is covered by the notion of "information on the circumstances surrounding the transfer necessary for the [data subject] to make a decision on his/her consent", in line with Article 13 of the GDPR, such as the third country of destination of the onward transfer; and does not explain the consequences of refusal of consent [19].
8. The Commission should further assess and demonstrate whether Japan's DPA (the PPC) "fully complies" with the independence required by the GDPR and CJEU decisions. [20]
9. LIBE "regrets" that "the level of possible fines ... is insufficient to ensure effective compliance with [Japan's] Act, as it does not seem to be proportionate, effective or dissuasive". The Commission should "provide information on the actual use of administrative fines and criminal sanctions in the past". [21]
10. LIBE is concerned that Japanese law provisions that "business operators can ... hand data over to law enforcement authorities on a 'voluntary basis'" "is not foreseen in the GDPR or the Police Directive" and might not be compliant with the GDPR's essentially equivalent standard [23].
11. The Commission should "provide more information about Japanese mass surveillance", because LIBE is "seriously worried" that "this mass surveillance will not stand the test of the criteria established" by the CJEU in *Schrems* [24].
12. LIBE 'regrets' that the draft Decision Annex II on law enforcement and national security protections "does not have the same legally binding effect as the

Supplementary Rules” [25].

Although LIBE does “welcome the substantive improvements” [6] made to Japan’s data protection law in 2015 (in force in 2017), its Resolution does not endorse or reject the draft Decision, but instead calls on the Commission to provide the further evidence it has identified as lacking [26], and authorises LIBE to continue to monitor developments [28]. My interpretation is that LIBE implies that the Commission has failed to demonstrate adequacy.

Several amendments tabled² by different political groups of the LIBE Committee had similar if not identical wordings to the final LIBE motion, which lowered the level of some criticisms of the draft motion tabled on 19 November³. It is reasonable to assume that other political actors interested in the swift adoption of the adequacy decision influenced several of the amendments tabled by these political groups, although with only partial success.

The European Data Protection Board (EDPB) has as yet only released brief details of the Opinion it finalised at its December Plenary Meeting.⁴ It welcomes that the Supplementary Rules “bridge some of the differences” between the Japanese and EU frameworks. However, “the EDPB notices that a number of concerns remain, such as the protection of personal data, transferred from the EU to Japan, throughout their whole life cycle” (similar to LIBE criticism (2) above). The EDPB also wants the Commission to “address the requests for clarification made by the EDPB, to provide further evidence and explanations regarding the issues raised and to closely monitor the effective application.” To what extent these issues will overlap those raised by LIBE is unknown. EDPB considers that this adequacy decision “is of paramount importance” because as the first adequacy decision under the GDPR, “it will set a precedent”.

At the time of writing, the opinions on the draft Decision of the relevant EU bodies (European Parliament and EDPB⁵), and the approval of the relevant committee⁶ established under the comitology procedure, will not be publicly available until mid-December.

If they are as critical as the LIBE Resolution, this will make it difficult for the Commission to achieve its goal of a final Decision during 2018 without appearing to be dismissive of the views of other EU bodies.

KOREA: A MORE COMPREHENSIVE ADEQUACY APPLICATION

Bills to comprehensively amend Korea’s four main data privacy laws⁷ were introduced into Korea’s National Assembly jointly by fourteen Members on 15 November 2018. The key Bill is the Partial Amendment to the Personal Information Protection Act.⁸ The Bills are the result of an agreement between the ruling party in the Assembly and the executive government, and so have good prospects of enactment, possibly quickly. As outlined by Kwang Bae Park and colleagues in ‘Korea’s Proposed Overhaul of Data Protection Laws’,⁹ the Bills have three main purposes, each of which is discussed further here.

Comprehensive adequacy? Korea’s previously proposed scope of an adequacy decision was limited to those parts of the private sector under the ‘Network Act’ and the jurisdiction of the Korean Communications Commission (KCC). This was primarily because the Personal Information Protection Commission (PIPC), while independent in its decision-making, did not have any independent powers to enforce its decisions but had to rely upon enforcement by the Ministry of the Interior and Safety (MOIS).

The Korean government and the European Commission have agreed that this approach was too narrow to provide meaningful benefits to EU-Korean trade, from either the Korean or EU perspectives. Korea is now proposing to make the PIPC a “central administrative agency” under the Prime Minister, with independent authority over all situations of processing of personal information, and to transfer to it all powers and functions of the MOIS under PIPA, and of KCC under the Network Act. PIPC is also to be empowered to investigate violations and to impose administrative fines up to 3% of turnover, which was previously a power held by KCC but not by PIPC. The European Commission will have to assess whether these

no doubt welcome proposals will meet the GDPR’s technical standards for the necessary powers and independence of a DPA.

“Big data”: Anonymised and pseudonymised data: Similar to Japan, Korea is now proposing to deal with aspects of “big data” processing directly in PIPA, rather than under the 2016 ‘Big Data Guidelines’, which had no clear legal status. The PIPA Bill distinguishes personal information, pseudonymized information and anonymized information.

Anonymized information is excluded from the scope of PIPA, because PIPA “will not apply to information which cannot identify an individual anymore even if other information is used when all the means, which can be utilized by the personal information controller, are taken into consideration reasonably, e.g. time, cost and technology” (art. 58-2). This appears to be consistent with the GDPR exclusion of data where “the data subject is not or no longer identifiable” (GDPR recital 26 concerning art. 4(1) ‘personal information’).

To accommodate “big data” processing, the Bill provides that a controller “may process pseudonymized information without the consent of the data subject for the purpose of statistics, scientific researches, public-interest archiving, etc.” (art 28-2(1)). “Process” includes disclosure to third parties, so this is an area of considerable privacy dangers. “Statistics” and “scientific research” are ambiguous terminologies, and it is not clear whether they would encompass “statistics for commercial purpose” or “research for industrial purpose” (which business organisations prefer) or be limited to “academic research” (which some civil society groups prefer). Even before safeguards are considered, the scope of this exception for processing of personal data will raise significant issues in adequacy discussions with the EU.

Numerous other provisions in art. 28-2 place restrictions on such processing of pseudonymised data. Where a controller provides such information to a third party, it “should not include information that can be used to identify a specific individual”. Further, any “combination of sets of information between personal information controllers” for the approved purposes must also be

“done by a specialized institution with security facilities according to the standards prescribed by [a] Presidential Decree.” At this and other points, the substance of these protections will be in a Presidential Decree, delegated legislation. This approach might raise significant issues for discussion with the EU, at least and until such standards are prescribed.

Other reforms towards GDPR standards: There are various other provisions in the Bills which, if enacted, will move Korea’s laws closer to the GDPR. The Bill to amend the Credit Information Act introduces a data subject right to request transmission of a person’s credit information to another provider, a “data portability” right. It also includes limits on automated decision-making. These rights are not included in the PIPA Bill discussed above but have been included in a Bill to further amend PIPA, so it is possible that they will become part of Korea’s uniform data protection regime.

As Park and colleagues point out, “special provisions regarding (i) safeguards to be implemented for the cross-border transfer of personal information, (ii) restrictions on the onward transfer of personal information, [and] (iii) the designation of a local representative” have been added to the PIPA by the Bills. These provisions were previously intended to be included in the Network Act, and are due to perceived weaknesses in Korea’s current laws concerning data exports, compared with GDPR standards.

Overseas providers of information and communications services within Korea, to a degree of significance specified by Presidential Decree, will be required to nominate a “domestic agent” (local representative) to carry

out duties of a chief privacy officer and reporting obligations. The overseas provider will be liable for their failures to do so (art. 39-12).

Transfer of personal data overseas will generally require the consent of the data subject, based on notifications, including of the data to be transferred, the country of the recipient, the recipient’s identity, the purpose of transfer and the duration of retention of data (art. 39-13(3)), and the transferor must take any other protective measures required by Presidential Decree (art. 39-13(4)). The same restrictions purport to apply to any further onward transfers by that recipient (art. 39-13(5), (6)), but whether such an exercise of extra-territorial jurisdiction will be effective is questionable. To what extent these data export restrictions will meet EU requirements cannot be clearly assessed until the EU’s final Decision concerning Japan is made, and its effect as a precedent considered.

CONCLUSIONS: A BROADER KOREAN APPROACH?

At this stage, Korea’s approach is different from that taken by Japan, because there is no equivalent to Japan’s Supplementary Rules which apply stronger GDPR-like provisions only to EU-origin personal data but not to Japan-origin data. The Korean approach has been to strengthen its law through legislation applying to all personal data, irrespective of its source. It is likely that Presidential Decrees will be needed to clarify some issues between Korea and the EU, once adequacy negotiations advance further. It will be very valuable to the privacy of the Korean people, and also to the future of the EU concept of adequacy, if Korea continues its

inclusive approach by making such Decrees apply to all personal data, irrespective of its source, and rejects Japan’s insular approach.

REFERENCES

- 1 LIBE ‘Motion for a Resolution of 03 December 2018 on the adequacy of the protection of personal data afforded by Japan (2018/2904(RSP))’ www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0561+0+DOC+PDF+V0//EN&language=EN
- 2 75 Amendments tabled on the draft motion for a resolution, available on the LIBE website: www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/AM/2018/12-03/1170096EN.pdf
- 3 Draft motion for resolution, available on the LIBE website: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/12-03/1169352EN.pdf
- 4 EDPB ‘Press release: European Data Protection Board - Fifth Plenary session: EU-Japan draft adequacy decision, DPIA lists (DK, HR, LU, and SI), and guidelines on accreditation’ 6 December 2018.
- 5 The European Data Protection Supervisor may also issue an Opinion, though it is not formally required, but has decided not to do so in this instance.
- 6 Art. 93, GDPR; see Commission’s draft adequacy decision, para. 191.
- 7 Personal Information Protection Act (‘PIPA’), Act on Promotion of Information and Communications Network Utilization and Information Protection (‘Network Act’), Act on the Protection and Use of Location Information (‘Location Information Act’), and Credit Information Use and Protection Act (‘Credit Information Act’).
- 8 All sections quoted are from an unofficial draft translation provided by the KCC.
- 9 See the accompanying article in this issue p.12.

EUROPEAN PARLIAMENT AND THE EDPB PUBLISH FINAL VIEWS ON THE DRAFT JAPAN DECISION

Both the European Parliament and the European Data Protection Board (EDPB) published on 13 December their final views on the draft Japan Decision. The Parliament has changed little in the LIBE proposed Resolution, summarised above. Criticism 1 (para. [7]) is omitted, but other amendments were rejected, except for some re-wording that was not substantive. Additional criticisms made by the EDPB have been adopted (para. 19). Without rejecting or endorsing the Decision, the Parliament nevertheless assumes (para.

[27]) that a positive Decision will be made. The EDPB’s 41 page Opinion cannot be summarised here. It also neither endorses nor rejects the draft Decision. It notices that “a number of concerns, coupled with the need for future clarifications, remain”, and it recommends that the Commission “provide further evidence and explanations”. Furthermore, it invites the Commission to review ‘this adequacy finding’ at least every two years, not four years (Opinion [30]). My interpretation is that both the Parliament

and the EDPB have now implied but not expressly stated that the Commission has failed as yet to demonstrate the adequacy of Japan’s protections. However, they accept the inevitability of a positive adequacy Decision.

The EDPB Opinion includes the new argument that Japan can find third countries’ protections ‘adequate’ under Japanese law, without any necessity for compliance with the Supplementary Rules, which would create dangers of an onward transfer weakness under the GDPR.



ESTABLISHED
1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Spain adopts GDPR implementing law

The new law entered into force on 7 December.

Rafael García del Poyo of Osborne Clarke reports from Spain.

Spain's Senate approved, on 21 November, the law that complements the GDPR, and the text of the law was published in the Official Gazette on 6 December¹. The adoption of the law was delayed because, among other reasons, Spain's legislature took the opportunity to add provisions that guarantee

citizens' "digital rights".

In general terms, the law closely follows the GDPR. But as the national law must avoid derogations or overlaps with the GDPR, subsequent interpretation will be made by Spain's DPA, as it is in their practical

Continued on p.3

How Ireland's DP Commission will exercise its powers

This will be a long process as many multinational cases need to go through the EDPB cooperation and consistency mechanism.

By **Helen Dixon**, Ireland's Data Protection Commissioner.¹

The GDPR has undoubtedly given rise to considerable additional work specific to EU Data Protection Authorities due to new obligations. Ireland's Data Protection Commission (DPC) has

had to introduce a new classification system internally to deal with cases that pertain to cross-border processing entities in order to ensure the cases are appropriately recorded on

Continued on p.5

Issue 156 **December 2018**

NEWS

- 1 - Spain adopts GDPR implementing law
- 1 - How Ireland's DP Commission will exercise its powers
- 2 - Comment
GDPR still not in force everywhere
- 8 - Q&A with Helen Dixon
- 16 - Norway's DPA and Consumer Council support each other
- 20 - Uruguay moves towards the EU GDPR standard
- 26 - DPAs: Ethics comes before, during and after law

ANALYSIS

- 9 - Japan and Korea: Different paths to EU adequacy
- 18 - Cathay's data breach catastrophe goes beyond Hong Kong
- 19 - The GDPR's extra-territorial effect is felt in Hong Kong
- 22 - Asia-Pacific free-trade deals clash with GDPR and Convention 108

MANAGEMENT

- 25 - The role of legal protection insurance

LEGISLATION

- 12 - Korea's proposed overhaul of its data protection laws
- 14 - Finland's new Data Protection Act enters into force on 1 January

NEWS IN BRIEF

- 4 - EDPB issues guidelines on territoriality of the GDPR
- 13 - Windows 10 breaches Dutch law
- 15 - Facebook fined €10m
- 20 - Ethics research issued in HK
- 21 - EU Standard Contractual Clauses case imminent in Ireland
- 27 - EDPB under pressure to produce more GDPR guidance

www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Materials from PL&B events
- Special Reports
- Videos and audio recordings

See the back page or www.privacylaws.com/subscription_info

To check your type of subscription, contact
kan@privacylaws.com or telephone +44 (0)20 8868 9200.

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL
report

ISSUE NO 156

DECEMBER 2018

PUBLISHER**Stewart H Dresner**

stewart.dresner@privacylaws.com

EDITOR**Laura Linkomies**

laura.linkomies@privacylaws.com

DEPUTY EDITOR**Tom Cooper**

tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR**Professor Graham Greenleaf**

graham@austlii.edu.au

REPORT SUBSCRIPTIONS**K'an Thomas**

kan@privacylaws.com

CONTRIBUTORS**Ana Brian Nougères**

Estudio Jurídico BrianN and Associates, Uruguay

Rafael Garcia del Poyo

Osborne Clarke, Spain

**Jukka Lång, Tuomas Haavikko and
Kaisa Päivinen**

Dittmar & Indrenius Attorneys Ltd, Finland

Kwang Bae Park, Hwan Kyoung Ko,**Sung Hee Chae and Minchae Kang**

Lee & Ko Attorneys, South Korea

Helen Dixon

Data Protection Commission, Ireland

Allan Chiang

Hong Kong

Merrill Dresner

PL&B Correspondent

Published byPrivacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Fax: +44 (0)20 8868 5215****Email: info@privacylaws.com****Website: www.privacylaws.com****Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753

Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2018 Privacy Laws & Business

comment

GDPR still not in force everywhere

The GDPR adaptation laws were delayed both in Finland (p.14) and Spain (p.1) due to national legislative traditions, and ambitions to add extra provisions on digital rights. In Spain, the new law is now in force and Finland's law will follow on 1 January 2019. But there are still some EU Member States that have not yet managed to bring the GDPR's provisions into national law, for example Greece, Portugal and the Czech Republic.

The European Data Protection Board (EDPB) will now increase its work rate by meeting every month for three days and is trying to achieve consistency in GDPR implementation. The Board is now dealing with cross-border cases. Much pressure has landed on Ireland, and the Data Protection Commissioner, Helen Dixon, says that many complaints and cases on systemic issues about tech companies do not need to be led by her office alone, as they apply equally across the EU (p.1). She promises fines, but not yet – the correct procedures takes time.

The EDPB has issued opinions on national lists for Data Protection Impact Assessments. In December it evaluated the European Commission's adequacy opinion on Japan. Japan's adequacy decision is close but not there yet. Korea has decided to amend its laws to facilitate its entry to the club of adequate countries (p.9). Another regional development is the new Asia-Pacific free trade agreements that include strict limits on how legislation can restrict personal data exports or require data localisation (p.22).

In October, Stewart Dresner and I attended the Data Protection Commissioners' International Conference in Brussels. DPAs spent a few days discussing the importance of data ethics (p.26). A valuable message was heard and reported also by national media, at least in the UK, but my impression was that the real work took place behind closed doors and at 31 side events on one afternoon and more on another. We organised a very well attended event on the potential for collective action under the GDPR and will be returning to this theme both on these pages and at our future events.

Laura Linkomies, Editor

PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality

Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service

Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

Subscription Fees

Single User Access

International Reports £560 + VAT*

UK Reports £450 + VAT*

UK & International Reports £900 + VAT*

* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition

Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions

Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.

www.privacylaws.com/UK