University of New South Wales Law Research Series

QUESTIONING 'ADEQUACY' (PT II) – SOUTH KOREA

GRAHAM GREENLEAF

(2018) 151 *Privacy Laws & Business International Report*
[2018] *UNSWLRS* 5

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

Questioning 'adequacy' (Pt II) – South Korea

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

15 January 2018

A shorter version of this article will be published in (2018) 151 *Privacy Laws & Business International Report*, February 2018.

The first part of this article provided a summary of the criteria and procedures by which the European Union has in the past assessed the 'adequacy' of data protection in third countries, and considered, in light of those criteria, what might be some of the issues which will arise in relation to Japan's current application. This second part considers similar questions in relation to South Korea's current application, and concludes with implications for the future of adequacy.

South Korea – Issues for adequacy assessment

In a 2014 comparison of all Asian jurisdictions, I considered Korea's data protection system to be the strongest.[1] Its enforcement aspects have grown much stronger since then, as noted below. However, there are issues both old and new that must be addressed in an adequacy assessment of Korea.

General or sectoral assessment?

Korea was initially seeking a 'whole country' adequacy assessment, under the *Personal Information Protection Act* (PIPA) including the Personal Information Protection Commission (PIPC) created by PIPA among a number of data protection authorities. EU concerns over whether the PIPC yet had sufficient enforcement powers of its own[2] led Korea to temporarily scale back its ambitions and to propose instead a sectoral adequacy assessment which would cover only those parts of the private sector subject to the 'Network Act', which is administered by the Korean Communications Commission (KCC). This decision was contentious.[3] Such assessments of 'specified sectors' are specifically allowed under the GDPR (art. 45(1)), and apparently permissible under the Directive (for example, for passenger name data (PND)). KCC is both independent of government and has strong regulatory powers. The Network Act covers the online-related activities of almost all major businesses, including any business that conducts online transactions, both telecommunications providers and those providing content and services via networked services (collectively described as 'ICSPs'). Other aspects of Korea's data protection system, not only KCC's role, will still be relevant to an

* Prof Whon-il Park, Mr Kwang Bae Park, and other Korean experts have provided valuable comments, but all responsibility for content remains with the author. Declarations of interest: in 2016 I carried out a consultancy assignment for a Korean agency, KISA, to assist it to prepare for Korea's application to the EU for an adequacy assessment; in 2012 I received a three month fellowship from a Japanese academic fund to research Japanese and other Asian data privacy laws, in Japan.

[1] Greenleaf *Asian Data Privacy Laws*, Chapter 5 'South Korea – The Most Innovative Law'.

[2] Whon-il Park 'South Korea's GDPR preparation: Hurdles ahead' (2017) 149 *Privacy Laws & Business International Report*, 23o 24.

[3] Under PIPA, the public sector including the resident registration number control is administered by PIPC as well as MOI (Ministry of the Interior). Korean experts advise that MOI is not ready to yield its authority of law enforcement to PIPC owing to the statutory restriction of the Government Organization Act and complexities of management of the national ID number databases. In November 2017, PIPC issued its objection to the proposed sectoral adequacy assessment by recommending MOI and KCC make a combined application for a 'whole country' adequacy assessment (PIPC Decision 2017o 25o 198 decided November 13, 2017). This advice was not followed.

adequacy assessment. For example, PIPA covers the non-network activities of businesses which are under the Network Act, and civil rights of action, and constitutional protections underpin KCC's powers.[4]

Legislative scope: Non-identifying and de-identified data

The definitions of 'personal information' in both the Network Act and PIPA say that it means 'any information which relates to a living natural person who can be identified or identifiable from those data … (including the information that does not, on its own, permit direct identification of a specific individual, but that does identify specific individual when it is *easily* combined with other information'.[5] The inclusion of the word 'easily' means that, like Japan, Korea does not have a conventional definition of 'personal information'.[6] Instead, it has a more narrow definition because if a data item cannot be 'easily' combined with other data to identify an individual,[7] then it is not 'personal information', and it remains unregulated by Korean data privacy laws. This difference is important to Korea's current policies on 'big data'. Whether information subjected to de-identification processes is still classified as personal information has not yet been determined by the Korean courts.[8]

In 2016 a consortium of Korean ministries and commissions[9] including KCC, the Financial Services Commission (FSC) and Ministry of the Interior and Safety (MOIS) (but not including the PIPC), released the *Guidelines for De-identification of Personal Data,*[10] replacing earlier guidelines[11] and repealing them.[12] The Guidelines do not have any clear legal status,[13]

---

[4] Greenleaf *Asian Data Privacy Laws*, pp. 127-132.

[5] Art. 2 in each Act. The English translation of PIPA on the English language portal of KISA now includes the phrase 'when it is easily combined with', but until March 2017 it instead stated 'if combined with'. Pre-2017 commentary must therefore be read with care. The Ministry of Government Legislation (MoLeg) had previously provided an English language translation of PIPA, with wording similar to 'when it is easily combined with' <http://law.go.kr/engLsSc.do?menuId=0&subMenu=5&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95>.

[6] For example, the 1995 EU data protection Directive, Art. 2(a) states " 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity;"

[7] The 2016 *Guidelines for De-identification of Personal Data* say "'easy combination with other data' means that it should be possible to obtain other information to be combined and there is a high possibility of combining with other information," and this 'does not include data that can't be legally collected and requires irrational amount of time or costs for collection' (II-2(1)B(e)).

[8] In the absence of the Supreme Court ruling on the interpretation of 'personal information', a district court held the USIM card serial number and the IEMI (International Mobile Station Equipment Identity) number of a mobile phone are information capable of identifying the individual. Seoul Central District Court 2010GoDan5343 decided February 23, 2011.

[9] Office for Government Policy Coordination; Ministry of Interior; Korea Communications Commission; Financial Services Commission; Ministry of Science, ICT and Future Planning; and Ministry of Health and Welfare

[10] Interdepartmental Joint Announcement *Guidelines for De-identification of Personal Data* (Korea), 30 June 2016 *<https://www.privacy.go.kr/eng/news_event_view.do?nttId=7585>*

[11] KCC had released 'Big Data Guidelines for Data Protection' in December 2014. In July 2014, the Personal Information Protection Commission (PIPC), had advised KCC that the draft guidelines did not conform to existing law, and advised reconsideration. For a summary of these 2014 Guidelines, see Kwang-Bae Park and Hwan-Kyoung Ko, 'Highlights of the "Big Data Guidelines for Data Protection" ', Lee & Ko Data Protection / Privacy Newsletter, January 2015 <http://www.leeko.com/data2/publication/Newsletter%20-%20January%202015(4).htm>;

[12] The 2014 Guidelines, and a number of ministerial regulations, were repealed. Details are in Whon-il Park 'Big Data Guideline' (KoreanLII) < http://www.koreanlii.or.kr/w/index.php/Big_Data_Guideline> .

unlike Japan's legislative provisions concerning 'Anonymously Processed Information'.[14] The purpose of the Guidelines includes to 'provide standards for businesses which intend to use or provide de-identified personal data' (II-1), which they do in considerable detail. The Guidelines do not only focus on the process of de-identification, because, even when personal data is held to be de-identified, numerous obligations in relation to its management are intended to continue. How such Guidelines can alter some obligations under PIPA, but not others, is not clear, and civil groups have claimed that processing according to the Guidelines is illegal.[15] The details of the Guidelines are discussed elsewhere.[16]

Broadly put, the issue for an adequacy assessment raised by both the definition of 'personal information' that completely excludes from protection data which cannot be 'easily' combined to identify and by the 'de-identification' Guidelines, both of which also have parallels in Japan, is whether, in comparison with the requirements of the Directive, they result in exempting from data privacy laws too broad a class of what would be personal information under EU requirements, particularly in light of *Schrems*.

Data export restrictions: Consent and proposed reforms

Korea's existing data export restrictions are based on very weak consent requirements in PIPA,[17] and provisions in the Network Act, art. 63. The latter provide a stronger consent-based export requirement which requires disclosure to the data subject of the destination country of export, the recipient company, purpose of transfer and period of retention of data (art. 63(3)). There are no other requirements in relation to the extent of data protection laws in the destination country, or need to inform the data subject of those protections (or lack of them) and any consequent risks. The transferor must also 'have the recipient … take such security measures as stated by the Presidential Decree (art. 63(4)).[18] A Bill to amend art. 63 is currently before the National Assembly, but may well be amended in the course of passage.[19] If enacted, the overseas recipient will then (purportedly) bound by similar requirements if it proposes to re-export the data (draft art. 63(8)), but this raises difficult issues of extra-territorial enforcement. KCC will have authority to order suspension of cross-border transfers '[w]hen it is apprehended that user's rights are severely violated' (draft art. 63(5)), with the

---

[13] It does not appear that the Guidelines are legally binding, nor that they would in themselves protect organisations against possible actions for breaches of any of Korea's data protection laws. However, given that the Guidelines have been issued by all of the main organisations enforcing these laws – KCC, FSC and MOI – companies operating in Korea may reasonably question whether any enforcement actions would be taken against them for following the Guidelines by these bodies. Nevertheless, there is still the possibility of court actions independent of these enforcement bodies. The legal effect of the Guidelines is therefore unresolved.

[14] See G. Greenleaf 'Questioning 'adequacy' (Pt I) – Japan'.

[15] De-identification processes pursuant to the new Guideline have concerned civic groups including the People's Solidarity for Participatory Democracy and the Korean Federation of Trade Unions. On November 9, 2017, they demanded prosecution of four de-identification agents including KISA, the Financial Security Institute and the Korea Credit Information Services, and the big data user corporations, on charges under PIPA of unconsented collection and de-identification of users' personal information. PIPA contains a number of penal provisions, so breaches may make data processors liable to punishment even though no actual damage to data subjects can be shown. No prosecutions have resulted as yet.

[16] See G Greenleaf, G, *2014-2017 Update to Asian Data Privacy Laws - Trade and Human Rights Perspectives* (July 12, 2017) UNSW Law Research Paper No. 47, 2017, pp. 13-14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000766> .

[17] Greenleaf *Asian Data Privacy Laws*, p. 147.

[18] Implemented by Presidential Decree of the Network Act, art. 67(2) (Protective Measures in Transferring Personal Information Abroad)

[19] It has been reported that KCC may modify the proposed amendment, following the ongoing negotiations with the EU Commission, domestic developments, and Korea's steps to join APEC CBPRs (as yet incomplete).

exporting ICSP having a right of appeal (draft arts. 63(6)-(7)). Amendments in 2016 to the Network Act mean that any ICSPs responsible for provision of personal data to foreign countries without the required consent of users shall be subject to the penalty surcharge by KCC up to a maximum of 3% of sales related to such violation.[20] Other draft amendments to art. 63 are discussed below.

The EU Directive requires Member States to allow 'derogations' from adequacy of 'a transfer or a set of transfers' where 'the data subject has given his consent unambiguously to the proposed transfer' (art. 26(1)(a)). While this already implies that subject consent is only an exceptional measure, the GDPR is far more explicit, classifying subject consent under 'derogations for specific situations', which are to take place '[i]n the absence of an adequacy decision … or of appropriate safeguards' (art. 49). Furthermore, the GPDR requires that 'the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards' (art. 49(1)(a)).

The issue for Korea's proposed reforms is whether adequacy requirements can be satisfied, in relation to onward transfers from a third country, by reliance primarily on consent requirements (albeit backed with security requirements, and heavy penalties for breach), even though consent is only an exceptional measure in relation to exports from the EU, and where restrictions on further transfers may be unenforceable. The residual capacity of KCC to terminate transfer arrangements (if it knows of them) where data subject interests are 'severely violated' (provided in the draft art. 63 amendments) is to some extent similar to the law New Zealand enacted in order to obtain an adequacy assessment, but that was in relation to a less significant EU trading partner,[21] and prior to the GDPR or *Schrems*, so the position of Korea is different.

APEC CBPRs: Potential back doors for onward transfers

In December 2016 South Korea lodged its *Notice of Intent to Participate in the CBPR System*, and APEC's Joint Oversight Panel (JOP) has approved its participation.[22] However, Korea has not yet appointed an Accountability Agent, and is not yet fully involved in APEC CBPRs.[23] Its involvement will not of itself adversely affect the assessment of its adequacy.

The proposed amendments to Article 63 of the Network Act include two exceptions from the consent requirement for data exports which could be interpreted to raise the same issues of 'back door' re-exports as Japan's Rules and Guidelines concerning CBPRs.[24] The first (draft art. 63(2)1) is where Korea is a party to 'other international agreements' which include 'special provision concerning cross border transfer of personal information'. While this could be interpreted to refer to APEC CBPRs, the required 'special provisions' may be missing. The steps involved in a country (say, Korea) 'joining' CBPRs do not involve it agreeing that

---

[20] Whon-il Park 'Recent amendments to the Network Act' (on KoreanLII) <http://koreanlii.or.kr/w/index.php/Recent_amendments_to_the_Network_Act >.

[21] G Greenleaf and L Bygrave ' Not Entirely Adequate but Far Away: Lessons from how Europe Sees New Zealand Data Protection' (2011) 111 Privacy Laws & Business International Report, 8-9 :< https://ssrn.com/abstract=1964065 >

[22] APEC CBPRs JOP JOP Findings Report regarding Korea's intent to participate in the CBPR system, 1 June 2017 <https://cbprs.blob.core.windows.net/files/JOP%20Findings%20Report_Korea_FINAL.pdf>.

[23] It is reported that KISA may be designated as Korea's Accountability Agent, commencing as such in 2019, in addition to its role in operating the Personal Information Management System (PIMS): "MOI and KCC to participate in APEC CBPRs", *Digital Times*, June 12, 2017. <http://www.dt.co.kr/contents.html?article_no=2017061202109960041003>.

[24] See G. Greenleaf 'Questioning 'adequacy' (Pt I) – Japan'.

companies within that country can export person information to another country by means outside the requirements of Korea's law.

The second exception (draft art. 63(2)3) is where the recipient of the transfer (in the overseas country) has been certified by the Personal Information Management System (PIMS),[25] a certification mark provider created under the Network Act by the KCC.[26] It is unclear whether this would facilitate KCC certifying individual overseas companies that were APEC CBPRs-compliant, or a whole class of companies (such as 'all CBPRs-compliant US companies'), or neither, if APEC standards are lower than PIMS standards. This needs clarification before an adequacy assessment is made.

Both provisions in proposed art. 63 are ambiguous (and not yet enacted), but they (and possible amendments during enactment) need to be considered in the context of an adequacy application, as potential methods by which onward transfers to CBPRs-compliant companies could be authorised. In Japan, such a situation has in fact arisen. Each draft provision also needs to be consistent with one of ways by which the EU recognises that data exports may take place.

Compliance and remedial mechanisms in place

Korean authorities, including KCC, have a long history of relatively vigorous enforcement of privacy laws.[27] Since 2014 Korea has strengthened significantly the penalties which can be applied by KCC, as well as other authorities.[28] Amendments to the Network Act in May 2014 provide that ICSPs may be required by a court to pay statutory damages of up to KRW 3 million (around US$3,000) to each affected user for a negligent or wilful violation of a data protection requirement that causes data loss, theft, or leakage, without the user having to prove actual damage resulting from such violation. Also, ICSPs may be required by KCC to pay increased administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover related to the violations for failure to obtain user consent prior to the collection and use of personal information, and the cap of KRW 100 million (around US$100,000) for administrative fines previously applicable to data leaks resulting from failure to comply with technical and managerial protection measures was removed.

The first major application of these penalties was in relation to the 'Interpark data leak'[29] which resulted in KCC imposing an administrative surcharge of 4.5 billion won (around US$4.5 million) on one of the largest Korean online shopping malls. In 2016 cyber criminals, allegedly associated with North Korea, fraudulently obtained personal information of 10.3 million customers, and attempted to blackmail the company for KRW 3 billion (around US$3 million). The fine was imposed by KCC for negligent failure to protect customer data, and was 60 times higher than previous fines.

---

[25] For explanation, see Whon-il Park KoreanLII: Personal Information Management System <http://www.koreanlii.or.kr/w/index.php/Personal_Information_Management_System>

[26] Network Act, art. 47-3(1).

[27] The history of enforcement to mid-2014 is detailed in Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 149-155.

[28] Details concerning other authorities are in G Greenleaf, G, *2014-2017 Update to Asian Data Privacy Laws* -, (cited above) pp. 15-17.

[29] Whon-il Park 'Interpark data leak' (KoreanLII, 2017) < http://koreanlii.or.kr/w/index.php/Interpark_data_leak> ; The 3% penalty rule had previously been imposed by KCC on a small internet company..

Both prior to 2014, and even more so since then, KCC and Korea's data protection system generally could be considered to have met the three elements of enforcement and remedial measures relevant to an adequacy assessment: 'a good level of compliance'; 'support and help to individual data subjects'; and 'appropriate redress to the injured parties'.

Conclusions: Questioning 'adequacy', and existential threats to it

This article (Parts I and II) does not attempt any comprehensive consideration of matters relevant to an adequacy assessment (for example, the content principles, or government access to private sector data). It does not attempt a comparison between the two countries currently seeking adequacy assessment, but points out that there are some similar issues requiring consideration in relation to each of them, and divergences on other aspects.

Of the issues relevant to adequacy assessment indicated by the Directive, *Schrems* and the A29WP Opinions, there is no formula that reveals which factors the A29WP regard as the most serious (or which the CJEU would so regard in light of Schrems, except government access), or how negative and positive factors may be balanced. 'Adequacy', while not a black box, is not very transparent in its principles or operation.

Independent analyses of issues requiring consideration by EU authorities in relation to their assessments of particular countries need to be made, as part of more general public debate. Adequacy discussion should not be limited to 'Commission to government' negotiations behind closed doors, because the public interest in these EU decisions is very high. This is not only so for EU citizens, but for people everywhere who need the EU to uphold a high level of data protection as the global standard for what is 'adequate' privacy protection.

APEC-CBPRs back doors: An existential threat to adequacy?

A country's membership of APEC-CBPRS is not in itself significant for adequacy assessments. However, if a significant number of APEC member countries start to join CBPRs, as is now starting to occur, this could change.

The EU's concept of adequacy is a means of protecting the rights of EU citizens by insisting upon a high standard of data protection in foreign countries where their data will be processed, if their data is to flow to those countries in a free and unrestricted fashion, without case-by-case controls. A by-product of this has been an overall rise in data protection standards globally.[30]

This will be threatened if the EU accepts that Japanese companies can export personal data of EU citizens to APEC CBPRs compliant companies overseas (currently 21 companies in the USA) solely because they supposedly adhere to a standard of privacy protection considerably lower than that of the EU and also lower than that of Japan. Article 24 of Japan's PIPA, and its implementing measures, are a back door to such onward transfers. Korea might do something similar, depending on the enactment and interpretation of its proposed amendment of art. 63 of the Network Act.

A possible consequence is that other APEC members that are considering joining CBPRs will follow the lead of Japan and/or Korea, and implement similar back doors, particularly if they know that this will not jeopardise a potential future adequacy application to the EU. At the

[30] G. Greenleaf, "'European' Data Privacy Standards Implemented in Laws Outside Europe" (2017) 149 *Privacy Laws & Business International Report* 21-23 <https://ssrn.com/abstract=3096314>.

same time it will serve to appease US business interests that want some means of legal transfer of personal data to them, from the growing number of countries with data export restrictions, and despite the lack of international standard US data privacy laws.

Although membership of APEC CBPRs should be meaningless to countries with strong data privacy laws, because they should have no problems importing personal data, the 'Japanese back door' is not meaningless to companies within those countries. Those companies want to eliminate restrictions on data exports to countries with lower privacy standards, such as the USA. As soon as some data exports are facilitated (such as from Japan or Korea), CBPRs has network effects on its side: every new country allowing exports to CBPRs-compliant companies should encourages more companies in any CBPRs member country with lower standards to seek certification to gain the benefit of exports (imports to them) from an ever-widening group of higher-standard countries. The propaganda value of this is likely to soon result in more certifications in higher standard APEC countries as well, even though they don't need it in order to obtain data imports.

The attractions might not be limited to countries within APEC, if countries such as India, South Africa, or Brazil see attractions in 'recognizing' APEC-CBPRs as an easy means to get the USA off their backs while at the same time doing something the EU has approved.

In relation to data protection, APEC has always wanted to become a bloc which would be a counter-weight to the EU and its 'adequacy' demands. If it accepts that the Japanese back-door is consistent with adequacy, the EU will have given APEC the 'interoperabilty' it has sought, while surrendering its insistence upon high standards of data protection at all links in the chain of data exports and onward transfers.