University of New South Wales Law Research Series

The Draft Korea Adequacy Decision: Submission to European Union Authorities

Graham Greenleaf

[2021] *UNSWLRS* 52

UNSW Law
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

The draft Korea adequacy Decision: Submission to European Union authorities

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

16 August 2021

This paper has been provided to various EU authorities as a Submission.

Contents

---

* *A shorter version of this paper was published as 'The meaning of 'adequacy': Implications of the draft Korea decision' (2021) 172 Privacy Laws & Business International Report 1, 3-7.*

Valuable comments have been received from Prof KS Park, Korea University (with permission to quote), Prof Douwe Korff, London Metropolitan University, Kwang Bae Park, Lee&Ko Seoul, and one anonymous commentor, but responsibility for all content remains with the author.

The author was one co-author of a 'self-assessment' report on the adequacy of Korea's data privacy laws, commissioned by the Korean Government, in 2016 (prior to major legislative changes). The author has periodically prepared commissioned reports for the European Commission on adequacy issues concerning various countries, but no such commissions are currently active.

The draft Korea adequacy Decision: Submission to European Union authorities

The European Commission's draft adequacy Decision concerning the Republic of Korea[1] will be the third such decision under the GDPR, once finalised. (It follows those concerning Japan (2019) and the United Kingdom (2021)). The decision is significant not only for its practical implications for Korea, but also for what it adds to our emerging understanding of how 'adequacy' is being interpreted under the GDPR. The CJEU's decision in *Schrems II* and the EDPB's Adequacy Referential[2] must also be considered.

The draft Decision is positive, in that it 'has the effect that transfers [from a controller or processor in the EU] to personal information controllers in the Republic of Korea may take place without the need to obtain any further authorisation' (Rec. 7 – indicating recital number of the draft Decision). The scope of the Decision is broad (Rec. 5), covering all information controllers in Korea bound by the Personal Information Protection Act (PIPA), with the exception of missionary activities, political party nominations, and most credit transactions.[3] So almost all processing of personal information by the private sector, and all processing by the public sector, is within the Decision. This contrasts with the Japan decision, which did not cover the public sector.

The Korea Decision will be subject to a first review within three years after its entry into force (unless the final Decision changes this). The review will, in particular, consider compliance by Korean authorities with the safeguards and representation set out in Annexes 1 and 2 mentioned below (Rec. 220).

The Decision is lengthy, comprising 66 pages of recitals, two pages of formal Decision, and approximately the same amount again of the two Annexes by Korean authorities. This article surveys those key aspects of the Decision and Annexes which should be most important in providing essential equivalence, and therefore most likely to be relevant to future adequacy Decisions. It highlights aspects which may be criticised either as falling short of a level of protection 'essentially equivalent' to that provided by the GDPR, or of being insufficiently documented in the Decision to justify a conclusion of essential equivalence.

Why is it valuable for independent third parties to critique draft adequacy Decisions? First, if third countries with sub-standard protections are held to provide adequate protection, then the rights of EU citizens under the GDPR are diminished when their data is exported. Second, NGOs and other parties in third countries need to know the standards to which their countries should be held if they apply to the EU for an adequacy assessment, so they can put their knowledge and experience to the Commission to assist it to reach its Decision – and probably to pressure their own governments to achieve higher standards of protection. Third, these

---

[1] [Draft] 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 the Republic of Korea under the Personal Information Protection Act

[2] European Data Protection Board, Adequacy Referential, WP 254 rev. 01. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 ('EDPB Referential').

[3] Korean controllers processing credit information pursuant to the Credit Information Act and under the oversight of the Financial Services Commission.

Decisions are, in practice, a major source of interpretation of the provisions of the GDPR, but as we know from the *Schrems* cases, they are interpretations that can be challenged.

What additions to Korean law did the Commission require?

The Commission negotiated with Korea two key documents additional to existing Korean law:

(i) The additional safeguards set out in Notification No 2021-1 of the Personal Information Protection Commission (PIPC) (Annex I of the Decision, hereinafter 'Additional Safeguards'); and

(ii) Concerning criminal law and national security matters ('government access'), there are official representations, assurances and commitments by Korean government authorities[4] to the Commission (Annex II of the Decision, hereinafter 'Government Assurances').

Both documents have similarities with, but significant differences from, documents contained in the Japan adequacy Decision. It seems that such 'Additional Safeguards' and 'Government Assurances' are becoming a standard part of adequacy decisions under the GDPR.

Additional Safeguards: Six 'Supplementary Rules'

The 'Additional Safeguards' are a 'Notification' made by Korea's Personal Information Protection Commission (PIPC) based on articles 5 and 14 of PIPA. They provide 'clarifications that apply to any processing of personal data under PIPA as well as additional safeguards for personal data transferred to Korea based on this Decision'. The Commission is satisfied that they are 'legally binding on personal information controllers and enforceable by both the PIPC and courts' (Rec. 12, and see Annex 1, part I[5]). The PIPC says it has 'adopted the Notification based on Article 5 (Obligations of State, etc) and Article 14 (international Cooperation)' of PIPA, but neither of these provisions, on their face, gives PIPC explicit authority to make such delegated legislation.[6]

Constitutional law Professor KS Park, Executive Director of NGO Open Net Korea[7] argues that the validity and enforceability of the 'Additional Safeguards' is not as clear as the Commission and the PIPC assert:[8]

> 'Korean constitutional law has the requirement of clarity and the principle of prohibiting blanket delegation to lower laws such as administrative regulations, which together require that a statute abridging basic rights be sufficiently clear *in its text* to inform the public of the scope of abridgement sufficiently so that they can predict generally how the law will be enforced or interpreted. If the unclear or blanket-delegating statute is found unconstitutional, the lower

[4] National Intelligence Service, Ministry of Justice, National Human Rights Commission of Korea, National Counter Terrorism Center, and Korea Financial Intelligence Unit

[5] The PIPC states that 'As this notification has the status of an administrative rule … it has legally binding force on the personal information controller in the sense that nay violation of this Notification may be regarded as a violation of the relevant provisions of PIPA. In addition… individuals are entitled to obtain redress from the [PIPC] or the courts.'

[6] PIPA art. 14 does mention cross-border transfers, which is the subject matter of one Supplementary Rule.

[7] Open Net Korea website <http://opennetkorea.org/en/wp/about-opennet>

[8] Personal communication with the author, held on file.

> regulations such as these Additional Safeguards become automatically void. Furthermore, Korean courts tend to interpret law in a manner grounded in the texts of the statute, often not accepting the administrative regulations issued to interpret the statute. The Commission should demand that the substance of the Supplementary Rules be converted into relevant statutory amendments. The problem is especially acute for pseudonymity provisions, discussed later, where the constitutional validity of some provisions in PIPA is questionable.

There are six 'Supplementary Rules' in the Additional Safeguards, each of which is discussed in this article. Only one (Rule #3 concerning notifications where the data has not been collected from the data subject) applies solely to personal information transferred from the EU pursuant to the adequacy decision.[9] The other five Supplementary Rules are of general application, so that the additional protections or clarifications they provide are equally available to persons located in Korea, or whose data has been transferred to Korea from somewhere other than the EU. It is unclear why Supplementary Rule #3 could not apply generally, and it would be better as a matter of principle if the EU aimed wherever possible to avoid the result of a higher standard of data protection law for EU citizens, and a lower standard for local citizens. The Japan Decision had this defect in relation to all its Supplementary Rules,[10] but the Korea Decision does so in only one of its six Rules.

The Commission asserts that 'an adequacy finding exclusively concerns the level of protection afforded to personal data transferred from a controller/processor in the Union to an entity in a third country (here: The Republic of Korea)' (Rec. 25). Even if this is so, where the process of negotiating an adequacy decision results in changes to the law of a third country, it is consistent with the EU's advocacy of global adoption of high data protection standards that it should aim to have the laws of countries held to be adequate align as closely as possible with core aspects of EU law such as onward transfer rules.

Rights of foreign nationals

The Commission finds that Korea's data protection framework, including both constitutional rights, and rights provided by statute, apply to 'all individuals, irrespective of their nationality' (Rec. 9-10). This finding is necessary, because the Commission must ensure that EU citizens are protected under Korean law. Supplementary Rule #1 (iv) states that other provisions in that Rule 'shall be applied equally to the processing of all personal information received within the area of Korea's legal jurisdiction from a third country, regardless of the nationality of the data subject'. This universality of application is somewhat at odds with Supplementary Rule #3 (discussed above) and its limited application only to data received from the EU (and therefore in most cases applying only to EU citizens).

Which GDPR rights and obligations does the Commission emphasize?

The Commission finds that all the key definitions in Korea's law align with those under the GDPR (Rec. 15-23). The categories of 'sensitive data' also now align with the GDPR's categories (Rec. 50). It finds that Korean law protects individual rights in ways equivalent to the GDPR, in relation to rights to information and access, correction or erasure, and

---

[9] Another very minor EU-specific clarification is in Rule #6, allowing EU citizens to submit complaints to the PIPC via their local (EU) DPA, or via the EDPB.

[10] G. Greenleaf 'Japan: EU Adequacy Discounted' (2018) 155 *Privacy Laws & Business International Report* 8-10, <https://ssrn.com/abstract=3276016>; G. Greenleaf 'Questioning 'Adequacy' (Pt I) – Japan' (2017) 150 *Privacy Laws & Business International Report*, 1, 6-11, <https://ssrn.com/abstract=3096370>

suspension of processing (including for direct marketing), and that controllers must establish and announce measures for such protection (Rec. 73-83).

Korean law does not have specific provisions concerning automated processing, but the Commission has not considered that this affects the level of a protection afforded to data transferred from the EU. It decided this on the pragmatic grounds that if personal data is collected in the EU, any decisions concerning automated processing will 'typically' be taken by the controller in the EU, so the absence of specific Korean rules on automated processing 'is unlikely to affect the level of protection of the personal data transferred' (Rec. 81). Perhaps this is correct 'typically' where an EU controller exports data to a Korean processor, but it might not be correct if the controller was Korea-based and receiving personal data from its EU offices or affiliates (or directly from EU individuals). Examples could be a Korean company providing video or computer games or equipment, some financial services, or travel services for use by EU individuals. How likely would such Korean companies be to use AI or other automated processing in order to make decisions affecting EU individuals in such transactions? This is difficult to answer, but the argument that automated processing is not relevant to an adequacy decision, based on the assumption that automated processing with take place at the EU end, calls for more discussion and precision. Perhaps the Korean company would come within the GDPR's extra-territorial jurisdiction (art. 3, and then art. 22), but if so this needs explanation in the Decision. On the basis of this Decision, it is difficult to see how the absence of automated processing protections could ever adversely affect an adequacy decision, an odd result given the increasing global prominence of AI. The EDPB's adequacy Referential also lists automated decision making as one of the principles considered necessary for 'essential equivalence', and sets out a list of matters which the 'law of a third country should … provide'.[11]

There is no specific discussion in the Decision of the following rights under the GDPR:

- the 'right to be forgotten' (GDPR art. 17), although PIPA does provide the more general 'right of erasure'.
- the right of data portability, although it is noted that the Credit Information Act provides such a right (Rec. 110).

Data portability is also omitted from the principles considered necessary for 'essential equivalence' in the EDPB's adequacy referential,[12] but the 'right to be forgotten' is arguably included.[13]

Onward transfers

If there are to be onward transfers of personal data received from the EU, the further recipient must be subject to rules 'affording an adequate level of protection'[14], so that the level of protection is not undermined by the further transfer.

---

[11] EDPB Referential, Ch 3, B(3).

[12] EDPB Referential, Ch 3, A(7).

[13] EDPB Referential, Ch 3, A(8): 'when for example their processing is no longer necessary'.

[14] EDPB Referential, Ch. 3 A(9).

PIPA distinguishes various types of onward transfers, and provides differing protections (Rec. 85-90). Generally, PIPA does not require notice to be given of transfers, but does require transfer matters to be disclosed in the company's privacy policy (PIPA Art 30). However, consent of the data subject must be obtained for some transfers to third parties and for some outsourcing.

1. *Outsourcing by a Korean controller to a processor in a third country* – There must be a legally binding outsourcing contract with the controller, imposing obligations on the processor, and the controller remains vicariously liable for any damage caused by the outsourcing (PIPA, art. 26). Such a contract cannot protect the data (and the data subject) against undue access by authorities of the other third country (*Schrems II*). Supplementary Rule #3 (ii) requires that the data subject be given notice of such transfers, including the country to which data is to be transferred, and their rights if any damage does result.

2. *Transfer to a third party located outside Korea, with consent of the data subject* – The controller must obtain the data subject's consent, after providing notice in considerable detail of the proposed transfer, including the third country involved, and that the data subject may deny consent (PIPA art. 17(2), plus clarifications in Supplementary Rule #3 (ii)). The Decision is, however, ambiguous concerning whether this consent must always be obtained, or only 'in principle' except for 'always' being required by information and communication service providers (Rec. 88). This ambiguity is significant and should be clarified. As in (1) above, Supplementary Rule #3 (ii) requires that the data subject be given notice of such transfers, informed of their rights etc.[15]

3. *Transfer without the consent of the data subject, but 'within the scope reasonably related' to the purpose of collection* – Such transfers are allowed under PIPA (art. 17(4)), thus exposing data subjects to risk if the laws of the third country do not provide adequate protection. Supplementary Rule #2 attempts to remedy this by requiring that the controller and the third country recipient 'through a legally binding instrument (such as a contract), ensure a level of protection equivalent to PIPA, including with respect to data subject rights' (Rec. 89). Again, the individual is provided with notice, prior to the transfer, under Supplementary Rule #3 (ii).

4. *Transfer without the consent of the data subject, for a new unrelated purpose* – Various grounds under PIPA allow such transfers (art. 18), and Supplementary Rule #2 requires a similar 'legally binding instrument' (Rec. 90), with notice, prior to the transfer, under Supplementary Rule #3 (ii).

The Commission concludes that these provisions, as modified by the Supplementary Rules, 'ensure continuity of protection' in the event of onward transfers, 'in a way that is essentially equivalent' to the GDPR (Rec. 91). Of course, it must be remembered that Supplementary Rule #3 (ii) only applies to personal data sourced from the EU, and therefore the crucial

[15] The GDPR provides that in transfers to a third country based on consent in absence of an adequacy decision (derogations under GDPR art. 49(1)(a)), individuals who are asked to consent to such transfers must be informed of the risks involved.

protection that notice of an overseas transfer gives is lacking in at least situations (3) and (4), where locally acquired data is concerned.

A PIPA amendment bill proposed by PIPC in early 2021 will allow Korea to make adequacy decisions concerning other countries. Once enacted, it would further alleviate risks in transfers to 'adequate' countries, and such transfers would not require notifications.

Processing pseudonymised information

PIPA allows the (further) processing of pseudonymised information without the consent of the concerned individual for the purpose of statistics, scientific research[16] and archiving in the public interest ('ARS processing') (art. 28-2). A variety of safeguards and penalties are provided, primarily to prevent and penalise the processing of the pseudonymous information for the purpose of identifying an individual (art. 28-3 – 28-6). The Commission concludes that the combination of these safeguards ensures 'essentially equivalent protections compared to those that would be required in accordance with' the GDPR (Rec. 43).

The consistency with the GDPR of Korea's pseudonymisation provisions was contested, in a letter to the Commission in March 2021,[17] by one of Korea's leading privacy NGOs, Open Net Korea. OpenNet's most significant criticism is that 'Under GDPR, it is ARS processing that triggers exemption from data subjects' access and other rights: in contrast, under [PIPA article] 28-7, it is pseudonymization that triggers the same exemption. The first problem is that any data controller can evade the duty to afford data subjects access, erasure, and objection simply by pseudonymization of the data even if it is NOT planning to use the resulting data for any socially beneficial purposes such as ARS purposes. This goes against GDPR's tenet that 'pseudonymized data are still personal data.' Open Net considers that there is a 'fundamental question: why should data subjects' access, erasure, and objection rights be abrogated simply because data are pseudonymized?'. These problems, if they exist, would apply to the personal data of EU citizens, unless the Supplementary Rules rectify this.

The GDPR does allow derogations (GDPR art. 89(2)) from the data subject's rights concerning access, rectification, restriction, notification, portability or objection (GDPR arts. 15, 16, 18, 19, 20 and 21), but it specifically requires that 'the derogations shall apply only to processing for the purposes of [scientific or historical research purposes or statistical purposes – 'ARS purposes']', and not for 'some other purpose' served at the same time by the processing (GDPR art. 89(4)). So, in the EU, even where data is processed for scientific purposes, relying on these derogations, subsequent use of the results for commercial or other non-scientific, purposes would not benefit from the derogations,[18] and restrictions on the use of the data in the GDPR would still apply.

In contrast, PIPA article 28-7 provides that all the following articles concerning user rights do not apply to 'the' pseudonymized information: articles 20 (destruction), 21 (notification of sources), 27 (notification of business transfers), 34 (1) (data breach notification), 35 through

---

[16] Considered by the Commission to comply with GDPR Recital 159 (Rec. 42, fn 59).

[17] OpenNet 'March 2021 Letter to EC and EDPS on Korea's GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions' <http://opennetkorea.org/en/wp/3239>.

[18] C W Svanberg 'Article 89', p. 1246 in Kuner, Bygrave & Docksey (Eds.) *The EU General Data Protection Regulation (GDPR) (A Commentary)* (OUP 2020)

37 (access, rectification or erasure, suspension), 39-3, 39-4, 39-6 through 39-8 (all special rights of users of ICSPs).

The key question is whether these Article 28-7 derogations from data subject rights occur irrespective of whether the pseudonymised data is being used for ARS purposes, and notwithstanding the fact that it remains personal data despite pseudonymisation. Such wholesale derogations of data subject rights, even though PIPA requires extensive protective measures to be taken, would be difficult to reconcile with 'essentially equivalent protections'. The pseudonymised data could not be provided to others, or re-identified, or severe penalties could apply (PIPA art. 71(4-2), (4-3)), but many (non-ARS) uses could still be made of the personal data provided they comply with the parts of PIPA that still apply.

The alternative view, that the derogations only apply when the pseudonymised data is used for ARS processing, is the view of the Commission, and the PIPC. The view that Article 28-2 places limits on the scope of Article 28-7 is supported by the fact that both Articles fall within Chapter III 'Section 3 Special Cases concerning Pseudonymous Data', so the reference in Article 28-7 to its provisions applying to 'the pseudonymous data' can logically be interpreted as referring to the data processed for ARS purposes only under Article 28-2.[19] The Commission considers that Supplementary Rule #4 'confirms' this interpretation of PIPA (Rec. 82 and footnote 108), implying that it accepts that PIPA has this meaning.

In addition, Supplementary Rule #4 (ii) provides that arts. 28-2 to 28-7 'shall not apply to cases where pseudonymised information is processed for purposes other than [ARS purposes]'. Any other processing of pseudonymised data will require consent, because article 28-2 authorising processing without consent will not apply. Also, because article 28-7 will not apply, the derogations listed above will also not apply to any such processing for non-ARS purposes, irrespective of the whether the pseudonymisation was originally done for ARS purposes. Supplementary Rule #4 is not limited in its scope to personal data imported from the EU, so it will benefit all data subjects. It is therefore intended as a notable strengthening of Korea's data privacy law.

However, whether PIPA itself, or Supplementary Rule #4, will have this effect is contested by Open Net. While welcoming Supplementary Rule #4, Open Net argues that both enforcement and constitutionality are in issue:[20]

> The statutory provision 28-7 abrogates the rights without any reference of ARS purposes. As discussed earlier, courts often interpret and apply law regardless of how administrative bodies interpret the law. In this instance, where the statute 28-7 clearly notes that pseudonymity without any ARS purposes still abrogates rights, Korean courts will find it difficult to enforce the Supplementary Rule #4 which unpredictably restricts the scope of Article 28-7.
>
> What is more important, Article 28-5 sets up an absolute ban against re-identification of pseudonymized data, without leaving any exemption. Therefore, even if a data subject demands vindication of, for instance, his right to access his personal data, data controllers cannot fulfil those rights of that data subject because they have to re-identify the data. It is for this reason that

[19] This division of PIPA into Chapters and Sections is found in the official Korean version of PIPA, and in the English language translation provided by the Ministry of Legislation. It is anomalous that the English translation provided by the Korean Legislation Research Institute (KLRI) provides no such division into Chapters and Sections.

[20] Prof KS Park, personal communication with the author, held on file.

> Open Net's constitutional challenge against Article 28-7 now includes a challenge against Article 28-5 as well.[21] Actually, PIPC itself has used Article 28-5 as a reason why they could not afford data subject rights with respect to pseudonymized data. It is a positive development that PIPC has changed its position on this but such benevolent intent must be reflected in the statute and carried out together with statutory amendment of the deeply related Article 28-5.

The Commission's rejection of this view can be assumed to be similar: Article 28-5 refers to '*the* pseudonymized information' (emphasis added) and is therefore limited to processing for ARS purposes, by Article 29-2.

The position taken by PIPC and the Commission concerning Articles 28-7 and 28-5 is persuasive, but it rests on questions of statutory interpretation practices concerning Korean language laws, which must be left to Korean-speaking experts. It cannot be ignored that two well-respected Korean NGOs take a different view and have commenced constitutional challenges[22] to Articles 28-5 and 28-7 of PIPA, on the basis of Korea's constitutional protection of the right to self-determination concerning personal information. European experience also indicates that NGO criticisms of adequacy Decisions need to be considered with care.

Unless and until there is a court decision to the contrary (to which the Commission could then respond), it is reasonable to assume that the position taken by the PIPC and the Commission is correct. However, the Decision needs to explicitly state the Commission's view on the relationships between Articles 28-2, 28-5 and 28-7, which it only implies at present. In some instances it would strengthen a Decision if it made clear that the Commission had considered but rejected significant domestic opinions contrary to a position taken in the Decision. Where such opinions have resulted in constitutional challenges, a Decision should mention this.

Oversight and enforcement – Theory and evidence

Until the major amendments to Korean privacy laws in 2020, the main impediment to Korea obtaining a positive adequacy assessment was that the PIPC did not hold sufficient enforcement powers that it could exercise independently of a Ministry, the scope of its powers was too limited in the private sector (the Korean Communications Commission was responsible for most of the telecommunications sector), and it did not have jurisdiction over the public sector. The 2020 amendments relocated the necessary enforcement powers with the PIPC.[23]

The Commission finds that the PIPC acts with complete independence, guaranteed by numerous provisions in PIPA (Rec. 113-116), and that the delegation of some of its tasks to the Korea Internet and Security Agency (KISA) and its Privacy Call Centre, does not detract from this (Rec. 117).

---

[21] For Open Net's constitutional challenge, see https://opennet.or.kr/19909 (Korean only)

[22] Korean civil society's objections to the PIPA provisions concerning pseudonymised information in arts. 28-5 and 28-7 are the subjects of constitutional challenges initiated by Open Net and another NGO (Solidarity for Participation Public Interest Law Center). See <https://www.hankyung.com/society/article/202011025040i> and <https://opennet.or.kr/19909 (Korean only).

[23] Park, Kwang Bae and others 'Korea amends Personal Information Protection Act' (2020) 163 *Privacy Laws & Business International Report*

The numerous enforcement powers in PIPA are reviewed by the Commission (Rec. 118-127), and their cumulative effect and actual use are summarised as follows:

> 'The Korean system therefore combines different types of sanctions, from corrective measures and administrative fines to criminal sanctions, which are likely to have a particularly strong deterrent effect on controllers and the individuals handling the data. Immediately after its establishment in 2020, the PIPC started to make use of its powers. For example, the PIPC imposed a fine of 6.7 billion won in December 2020 on a company for violating different provisions of PIPA (including security requirements, requirements for consent for third party provision and transparency)[152] and a fine of 103.3 million won on 28 April 2021 on an AI technology company for violating, amongst other provisions, the rules on lawfulness of processing, in particular consent, and the processing of pseudonymised information[153]' (footnotes omitted) (Rec. 128).

These examples are recent enforcement actions by the PIPC since it obtained its new powers in 2020, and the Commission notes that effective enforcement actions in Korea are of much longer duration and more diverse than these examples suggest.

> 'Also, already before the recent reform, South Korea had a strong track record of enforcement, with the responsible authorities making use of the full range of enforcement actions, including administrative fines, corrective measures, and 'naming and sharing' [sic] with respect to a variety of controllers, including communication service providers (Korea Communications Commission), as well as commercial operators, financial institutions, public authorities, universities and hospitals (Ministry of Interior and Safety)' (footnotes omitted) (Rec. 128).

This acknowledgment is important, but the Decision would be more convincing if examples of many other forms of enforcement were given, and some sense of their volume and history.[24]

'On this basis', the Commission concludes, 'the Korean system ensures the effective enforcement of the data protection rules in practice, thereby guaranteeing a level of protection essentially equivalent to' the GDPR (Rec. 128). It is important that this conclusion is based on 'effective enforcement' of 'rules in practice', not merely on what appears on the face of the legislation. Perhaps the most significant criticism of the Japan Decision is that there was no such finding of 'effective enforcement' supported by details of actual enforcement actions, primarily because little if any such evidence of actual enforcement existed.[25] For the Korean Decision to serve as a convincing example of what constitutes adequacy, this aspect of the Decision can be, and should be, strengthened.

Individual redress – Compensation

The Commission asserts the centrality of redress mechanisms to adequacy: 'In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages' (Rec. 129).

The Decision then outlines the various ways in which the Korean system 'provides individuals with various mechanisms to effectively enforce their rights and obtain (judicial) redress.' (Rec. 130-135). These include the obligations on controllers, and the operation of

---

[24] For example, see an account of Korea's enforcement history up to 2014 in G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 149-155.

[25] G. Greenleaf 'Japan: EU Adequacy Discounted' (2018) 155 *Privacy Laws & Business International Report* 8-10, <https://ssrn.com/abstract=3276016>

specialised remedial institutions (the 'Privacy Call Centre' operated by KISA, and the 'Dispute Mediation Committees' (PIDMC) appointed to mediate particular disputes). In addition, there are collective dispute mediation provisions, with potential class actions resulting. Finally, there are provisions in PIPA for remedial actions to be brought before a Court, which may result in compensation for actual damage (including punitive 'triple damages'), or alternatively 'statutory damages' of up to 3 million won (US$3,000) without need to prove actual damage. Some of these remedial techniques are novel, but the Commission does not note this.

The Commission's overall conclusion is that the Korean system 'offers various avenues to obtain redress, from easily accessible, low cost options (for instance by contacting the Privacy Call Centre or through (collective) mediation), to administrative (before the PIPC) and judicial avenues, including with the possibility to obtain compensation for damages' (Rec. 138). Once again, all of this is in marked contrast to the Japan Decision, where no such finding was made, nor was it possible. However, the Korean Decision would be improved by inclusion of details of compensation and other remedies that have actually been provided over the past decade in Korea. For example, details of PIDMC dispute resolutions are available.[26] If adequacy decisions are to be accepted as reflecting reality, not merely 'the law on the books', evidence is required.

Public sector access to private sector data

As required since *Schrems I*, the draft Decision examines at length (Rec. 139-208) the access to and use of personal data transferred from the EU by Korean public authorities, particularly those authorities involved in criminal law enforcement and national security. The test of 'essential equivalence' is stated as involving the following criteria (consistent with the EDPB,[27] but in more detail) (Rec. 141-143):

1. Limitations on protections must be provided by law, and the law providing the legal basis of processing must define the scope of the limitations.

2. The requirement of proportionality means that 'derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognized by the [EU]'.

3. There must be independent oversight of how these requirements are fulfilled.

4. The legislation's requirements must be legally binding under domestic law on all public authorities in the third country, and legally enforceable against them in its courts. Data subjects must be able to bring 'legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data.' Other remedies such as compensation are not mentioned, but the Decision gives details of compensation provisions that do apply to Korean public authorities.

---

[26] Greenleaf, *op cit*, p. 150.

[27] EDPB Referential, Ch. 4.

The Decision applies these criteria (and adds other details) to Korea's general legal framework (Rec. 144-150), and then in greater detail to access and uses in each of criminal law enforcement and national security. In relation to the general legal framework, the Decision highlights:

1. Korea has very strong constitutional protections of privacy, including individuals' rights of action 'before the Constitutional Court if they believe that they have been infringed by public authorities in the exercise of their powers', including 'a right to claim just compensation'.

2. These protections are reflected in the specific laws regulating criminal law enforcement and national security authorities.

3. PIPA's data protection rules apply to all public authorities. All of the GDPR's 'core principles', and other principles, apply to processing for law enforcement purposes. 'While the processing of personal data for national security purposes is subject to a more limited set of provisions under PIPA, the core principles, as well as the rules on oversight, enforcement and redress, apply'.

4. 'These general limitations and safeguards can be invoked by individuals before independent oversight bodies (e.g. the PIPC and/or the National Human Rights Commission, see recitals 177-178) and courts (see recitals 179-183) to obtain redress.'

The following parts of the Decision elaborate these protections in relation to criminal law enforcement and national security. The Decision gives details of the actual enforcement of PIPA provisions by the PIPC in relation to numerous aspects of criminal investigations. (Rec. 171). High volumes of both complaint-based and ex-officio investigations by the National Human Rights Commission are also cited (Rec. 172, and fn 269).

Voluntary disclosures to law enforcement authorities

One contentious provision is that Korean law enforcement authorities may request disclosures of subscriber data on a voluntary basis (art. 83(3) *Telecommunications Business Act (TBA)*), and telecommunications providers must comply with PIPA when processing such requests. There are believed to be millions of voluntary data disclosures made every year.[28] The Commission has negotiated adoption by PIPC of Supplementary Rule #3 which provides (in the Commission's words) that 'telecommunications providers in principle have to notify the concerned individual when they voluntarily comply with a request' (with very limited exceptions for jeopardising ongoing investigations and protecting superior rights of others) (Rec. 166). Similar notification requirements apply when there is a voluntary disclosure to a national security authority (Rec. 194). These notifications are because of Supplementary Rule #3 (ii), which applies to the discloser (the telecommunications provider or other Korean controller, not the law enforcement or national security authority).

Supplementary Rule #3 only benefits data subjects whose data has been transferred from the EU, not all data subjects. For example, those in Korea must request such notification (PIPA art. 20(1)). The EU data subject is also to receive notification of the *receipt* of his or her data by a Korean controller, when it is received from the EU, under Supplementary Rule #3 (i).

---

[28] According to Korea Internet Transparency Report 2020 < http://transparency.kr/notice/2447>.

Korean civil society is very sceptical of the likely effectiveness of Supplementary Rule #3 (ii), as explained by Prof KS Park of Open Net Korea:[29]

> Despite the Commission's view that Supplementary Rule #3 creates such a notification requirement, this issue has been so hotly debated until recently that it is unlikely that the present level of rule-making will suffice. There have been many failed legislative attempts to set up such affirmative notification requirements concerning article 83(3) data disclosure, aimed at obliging the government receiving the data, following civil society campaigns. It will not be constitutionally acceptable for PIPC to change all of this only for EU-originated data.[30]
>
> At present there are no affirmative notification requirements on any data controller (including telecommunication providers) when the disclosure is made according to article 83(3) TBA. PIPA art. 39-8, a special provision applicable only to information communication service providers, does require those providers to inform data subjects periodically of the instances of data disclosure but the data disclosure under art. 83(3) and data disclosure made under state surveillance laws are explicitly exempted from such notification obligation. In conclusion, there is no affirmative notification requirement on telecommunication providers or any other data controller after they fulfill government requests for user data, and PIPC's rule-making is unlikely to change the *status quo* just for EU-originated personal data.

Korean civil society is therefore questioning whether PIPC has authority to impose such a notification requirement. If such a requirement is successfully challenged in later court proceedings, this would give the Commission a basis to reconsider the Decision.

It must also be open to question whether it is sustainable for Korean controllers to effectively segregate EU-sourced data from all other data, just so that they can observe Supplementary Rule #3, if and when disclosure is required. If it is not realistically sustainable, this is a reason for the Commission not to accept provisions which only apply to EU-sourced data, because the interests of EU citizens may be damaged if those rules are ignored in practice.

Other Supplementary Rules applying only to public authorities

Supplementary Rule #5 concerns PIPA article 64, which prevents the PIPC from ordering many types of administrative agencies to take remedial measures. However, if PIPC makes a recommendation to an agency that it should take such remedial measures, it is legally required to implement the recommendation unless there are 'extraordinary circumstances' (PIPA art. 64(4)). The Rule provides that a public authority may only invoke such extraordinary circumstances if it clearly demonstrates that no infringement occurred (perhaps because of factual or legal circumstances of which PIPC was unaware) and the PIPC determines that this is indeed not the case. This clarification benefits all data subjects, not only those in the EU.

Supplementary Rule #6 applies to uses of personal information for national security purposes, and provides a detailed elaboration of what is otherwise briefly stated in PIPA or recognised by the Constitutional Court. The Rule covers (i) how national security authorities must ensure that processing implements principles of data minimisation, use limitation and data quality; (ii) the rights of data subjects in relation to confirmation of processing, access, obtaining copies, suspension of processing, correction, deletion or destruction; and (iii) how data subjects may exercise these rights, including via the PIPC or a representative, or take steps to

---

[29] Personal communication to the authore, held on file.

[30] There have been a series of lawsuits and campaigns for reform by civil society since 2009 to date; see "Ask Your Telco" Campaign <http://opennetkorea.org/en/wp/2087>.

obtain redress. This Rule benefits all data subjects, with the slight exception of a special provision specifying that EU data subjects can exercise these rights via their local (EU) DPA, or via the EDPB. There is no explicit equivalent provision in relation to DPAs in other countries.

Conclusions

Korea has had the strongest data privacy law in Asia for the past decade, together with the most effective enforcement. Once the 2020 legislative reforms remedied the mis-match between the EU's requirements for an independent DPA, and the distribution of enforcement powers within Korea, the country was well-positioned to be the subject of a positive adequacy Decision. The Commission's positive Decision concerning Korea's data protection system sets out a strong case for Korea providing adequate protection, but has shortcomings and ought to be improved before it is finalised (see below). It is unlikely that a stronger case could be made for any other country in the Asia-Pacific.

The Korea Decision, even without improvements to the draft, is far more convincing than the Commission's Japan Decision, which many considered was 'inevitable' due to the importance of trade between Japan and the EU. The credibility of the objectivity of the adequacy process is important to the EU in the long term, and for that reason the Korea decision is a much better example of what should be established in an adequacy decision. More so, if it is improved.

What appears necessary for adequacy?

The Korea Decision clarifies some aspects of what will be necessary for future positive Decisions.

It seems to be unavoidable, and is in fact desirable, that the Commission should negotiate the making of what is in effect delegated legislation by the country's data protection authority, such as the Supplementary Rules in the Japan and Korea Decisions, provided that such rule-making is constitutional and otherwise valid and enforceable. The purpose of such Supplementary Rules is to better (or more clearly) align with the GDPR the regime that is being found to provide adequate protection. Where the delegated legislative powers of a DPA are sufficient to achieve the desired changes, as they are claimed to be in Korea and Japan, this is a far more rapid and certain procedure than insisting on changes to primary legislation by the national legislature. However, if credible doubts are raised about the validity or effectiveness of aspects of such Supplementary Rules, then the Commission needs to amend the draft Decision either (i) to dispel such doubts without simply relying on the view of the government in question, or (ii) by obtaining an undertaking by the government concerned that it will propose legislation to remove any such doubts, prior to the first review of the Decision. The Decision already sets out the steps the Commission may take to suspend, repeal or amend the Decision if the Supplementary Rules (and other provisions) are not adhered to by Korean parties (Rec. 216-228).

One of main lessons for other countries considering applying to the Commission for an adequacy Decision is that their country (through its DPA and other public authorities) will almost certainly need to negotiate Supplementary Rules of a similar complexity to those found in the Korea and Japan Decisions, and those Rules will have to be enforceable within domestic law.

What factors does this Decision indicate may be significant in relation to future adequacy decisions concerning other countries?

- All data protection rights must apply to 'all individuals, irrespective of their nationality'.
- The importance of the independence of a data protection authority is re-affirmed, and that 'independence' requires that the DPA has the authority, of its own volition, to use every enforcement mechanism available under a country's law. Every country in Asia that aspires to a positive adequacy finding needs to consider this very carefully, as few existing laws or pending Bills would pass this test.[31]
- It appears that the absence of the following factors in a country's data privacy regime is unlikely to adversely affect an adequacy decision concerning it: automated processing protections (but see reservations below); explicit provision of a 'right to be forgotten'; and a right of data portability.
- The detailed explanation of how government access is to be analysed is, with the UK decision, valuable as the first example from the Commission since *Schrems II*.

Desirable improvements to the Decision

Other EU authorities (the EDPB, Parliament and Council) will now have the opportunity to provide input into the Decision before it is finalised. How could the final Korea decision be improved?

The argument that requirements for *automated processing* are not necessary, based on the assumption that automated processing will take place at the EU end when data is transferred, is not sufficiently justified.

In relation to *onward transfers*, Supplementary Rule #3 (ii) only applies to personal data sourced from the EU. Therefore the important protection that notice of an overseas transfer gives is lacking in some international transfers, where locally acquired data is concerned.

Concerning *pseudonymized personal information*, the Decision needs to explicitly state the Commission's view on the relationships between Articles 28-2, 28-5 and 28-7, which it only implies at present. It would strengthen the Decision if it acknowledge that differing views of these provisions have resulted in constitutional challenges.

The positive conclusions concerning *both enforcement powers and redress mechanisms* should be strengthened by inclusion of as much detail as is available of actual cases of enforcement, and of provision of remedies, even though many of these details will inevitably pre-date the 2020 reforms.

Supplementary Rule #3 (ii) concerning *voluntary disclosures by controllers to law enforcement authorities* requires notifications to be given to data subjects, but only for EU-sourced data. Korean civil society has questioned whether PIPC has authority to

---

[31] G. Greenleaf 'How Far Can Convention 108+ 'Globalise'?: Prospects for Asian Accessions' *Computer Law & Security Review* Volume 40, April 2021, 105414 <https://ssrn.com/abstract=3530870>

impose such a notification requirement. If such a requirement is successfully challenged in later court proceedings, this would give the Commission a basis to reconsider the Decision. The sustainability of the segregation of data by Korean controllers is also questionable. The Decision should explain why a rule applying only to EU-sourced data is necessary. While Supplementary Rule #3 applies only to personal data imported from the EU, the result will be a higher standard of data protection for EU citizens, and a lower standard for local citizens.