Adapting Korean Data Protection Laws for the Fourth Industrial Revolution

July 2019

Prof. Nohyoung Park
Korea Univ. Law School

Talking Points

- Recent Amendments to the Network Act
- Proposed Amendments to the PIPA
- Proposed Amendments to the CIPA
- Adequacy Negotiation with the EU

Introduction

- The Rep. of Korea (Korea) is trying to adapt its data protection laws to cope with the fourth industrial revolution.
  - The current data protection laws have been strongly criticized for their severely strong data protection rules, which hinder the legitimate use of personal information by industries in the fourth industrial revolution.
  - The amendments and their proposals are the result of intensive consultation under the Presidential Committee on the Fourth Industrial Revolution taking place in April 2018.
  - However, the proposed amendments are still waiting for the adoption due to the political fights in the National Assembly.
  - The major data protection laws include the Personal Information Protection Act (PIPA), the Act on the Promotion of IT Network Use and Information Protection (Network Act), and Credit Information Protection Act (CIPA).
- Korea has made efforts to revise data protection laws by examining the General Data Protection Regulation (GDPR) as a benchmark.
  - Korea has also tried to secure an adequacy agreement with the European Union since 2015.

Data Protection as a Basic Right in Korea

- The Constitutional Court has recognized 'the right to control one's own personal information' as a basic right, although the right is not explicitly stated in the Constitution of Korea:
  - "The right to control one's own personal information is a right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, existing to protect the personal freedom of decision from the risk caused by the enlargement of State functions and information and communication technology." (Constitutional Court, 2005. 5. 26. 2004Hun-Ma190 (Consolidated))

Recent Amendment to the Network Act

- The Act on the Promotion of IT Network Use and Information Protection (Network Act), which protects personal information of the users of information and communications services, was recently amended to establish a representative for foreign companies.
  - The providers of information and communications services with no physical presence like "address or business offices" in Korea are required to designate in writing a domestic representative who deal with the task of data protection officers, notification and communication of a personal data breach, and the submission of documents relating to the violation of the Network Act. (Art. 32 *quinquies*)
    - A controller or processor not established in the EU, subject to the application of the GDPR in accordance with Art. 3(2), is required to designate a representative in the EU. (Art. 27)
    - However, Korean data protection laws do not yet provide for their extraterritorial application.

Recent Amendment to the Network Act

- The Network Act was recently amended to apply to onward transfer as follows: When those who to whom the personal information of the users of information and communications services are transferred in third countries transfer the personal information concerned to another third countries, paras. 1 to 4 of Art. 63 (the protection of personal information transferred abroad) apply *mutatis mutandis*. (Art. 63(5))
  - Thus, the onward transfer of Korean personal information from third countries to another third countries is in principle allowed based on the consent of the users of information and communications services after notifying the users of the information like the items of the personal information transferred and the name of those who to whom the personal information is to be transferred in advance.
  - Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may take place only if, subject to the other provisions of the GDPPR, the conditions laid down in Chapter 5 are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. (GDPR Art. 44)

Recent Amendment to the Network Act

- The Network Act was recently amended to provide for the reciprocity principle in relation to data localization as follows: The providers of information and communications services in the States which restrict the transfer of personal information abroad may be subject to the restriction corresponding to the level of those States (Art. 63 *bis*)
  - Thus, the transfer of Korean personal information to those countries that implement data localization requirements may be prohibited.
  - This reciprocity principle applies even when the consent of the users of information and communications services is obtained for the transfer abroad in accordance with Art. 63.
  - This reciprocity principle does not apply in the case of the implementation of treaties or other international agreements.

Proposed Amendment to the PIPA

- Amendments to the Personal Information Protection Act (PIPA) and the Credit Information Protection Act (CIPA) were expected to be adopted by the National Assembly as early as the first quarter of 2019 and to be effective around the second half of 2019.
  - The amendments would provide a much easier use of personal information by introducing new elements like the pseudonymised personal information.
  - The PIPA would become genuinely the leading general data protection law in Korea after successful amendments.

Proposed Amendment to the PIPA

- The proposed amendments to the PIPA and the CIPA would have provisions to facilitate the use of personal data:
  - (i) clarifying the meaning of personal information and adding a concept of pseudonymized information (PSI);
  - (ii) expanding the scope of usage of personal information that is permissible without individual consent, subject to the additional purposes being compatible with the original purposes of data collection, and subject to fulfillment of a minimum level of encryption or other security process, to be further stipulated in the Enforcement Decree; and
  - (iii) freeing up statistical output using PSI, along with further use of that data subject to security measures under the Decree.

Proposed Amendment to the PIPA

- The PIPA and the CIPA, if amended, would provide pseudonymized information (PSI) as a new category of personal information, which would facilitate further the usage and processing of personal information.
  - There would be no requirement of individuals' consent, which is generally required under the current rules.
  - PSI is defined as information that has been pseudonymized so that a specific individual is not identifiable by that information without using, or combining it with, additional information so as to restore it to its original state.
  - The definition of PSI is analogous to the pseudonymisation defined under the GDPR. (Art. 4)
  - The PIPA, if amended, would also clarify the element of "identifiable" for personal information so that this will involve issues such as the reasonableness of time and expense required for identification.

Proposed Amendment to the CIPA

- The CIPA, if amended, would provide new rules in relation to profiling as follows: Individual owners of credit information are to have the rights to access to the information on and object to the assessment through profiling in relation to personal credit information assessment companies and personal credit information users/providers. (Art. 36 *bis* and *ter*)
- Unlike the GDPR (Art. 22), however, the amendment proposal for profiling does not cover 'the right not to be subject to a decision based solely on … profiling, which produces legal effects concerning him or her or …' and 'the right to obtain human intervention on the part of the controller …' when the decision based on profiling is necessary for performing contracts or is based on the explicit consent of data subject.

Adequacy Negotiation with the EU

- The EU and Korea have been in negotiations over whether the latter has an adequate level of data protection under the EU's GDPR.
  - Korean companies want to make an easy access to and process EU consumer data without the other mechanism like standard clauses, as the EU is a big market for digital economy.
  - Korean government wants the Korean data protection laws to be recognized to stay at the same level of the GDPR.
  - Korea initiated the process of getting an EU adequacy decision in 2015.
- Korea initially applied for a partial adequacy decision in relation to the Network Act, which is specific to information and communications services.
  - The Korea Communications Commission (KCC), data protection authority under the Network Act, is independent and has also enforcement powers.
  - The European Commission may decide that "one or more specified sectors within a third country" ensures an adequate level of protection. (GDPR Art. 45(3))

Adequacy Negotiation with the EU

- Korea is now changing to win a general adequacy agreement with the EU in relation to the PIPA, which is a general data protection law in Korea.
  - The Personal Information Protection Commission (PIPC), data protection authority under the PIPA, has at present no enforcement powers of its own, although it is supposed to be independent.
    - The enforcement powers for data protection reside within the Ministry of the Interior and Safety, which may not be regarded independent.
    - The PIPC's lack of enforcement powers would mean that it is not really fully independent, as it should depend on the Interior Ministry for enforcement purposes.

Adequacy Negotiation with the EU

- The proposed amendment to the PIPA and the Network Act, giving the PIPC the enforcement powers from the Interior Ministry and the KCC, is pending for a while in the National Assembly.
  - The PIPC is supposed to become the independent authority for data protection after the amendment to consolidate the data protection laws is adopted.
  - The re-allocation of data protection authority to the PIPC would help meet GDPR standards for an independent authority so as to achieve an adequacy agreement for data transfers from the EU to Korea.
- As the PIPC becomes the data protection authority with independence and enforcement powers, the PIPA will be the general data protection law in Korea.
  - CIPA, nevertheless, still remains separate for the protection of individual owners of credit information.

Observation

- The GDPR has been affecting the Korean data protection laws which are struggling to cope with the fourth industrial revolution.
- The Network Act has partly borrowed from the GDPR some elements on the onward transfer of personal information abroad, and a representative.
- The pending amendments to the PIPA and CIPA would significantly relax constraints on the use of personal information by introducing pseudonymized information as a new category of personal information.
- The pending amendments to the CIPA would provide for new provisions on profiling in financial sectors, however not in a similar way to the GDPR.
- The pending amendments would make the PIPA to be the general data protection law, and the PIPC to be the independent authority with enforcement powers.
  - The adequacy agreement between the EU and Korea is expected to reach soon after the amendments are adopted by the National Assembly.