Recent Legal Issues and Amendments of the Privacy Laws in Korea

Jongsoo(Jay) Yoon
Partner, Lee&Ko
jay.yoon@leeko.kim
iwillbe99@gmail.com
twitter @iwillbe99
www.facebook.com/iwillbe99
www.jayyoon.com

Asia Privacy Bridge Forum

(1) OVERVIEW

	Public Sector	Private Sector
general law	PIPA(Personal Information Protection Act)	
special law	• the Statistics Act • the Official Information Disclosure Act • the Resident Registration Act • the Electronic Government Act • the Framework Act on Education	• **Network Act**(the Act on Promotion of Information and Communications Network Utilization and Information Protection) • **Credit Information Act**(the Use and Protection of Credit Information Act) • the Act on the Protection, Use, Etc, of Location Information • the Financial Holding Companies Act • the Act on Real Name Financial Transactions and Confidentiality • the Medical Service Act • the Bioethics And Safety Act

(1) OVERVIEW

APPLICATION SCOPE OF PIPA

Personal Information	Filing System	Processor
• living natural person • identified or identifiable information • directly or indirectly	• set of personal information • structured set • accessible according to specific criteria	• as part of duties • managing the filing system • processing personal information

• regulation on the Personal Information Processor
• all or nothing approach

(1) OVERVIEW

Network Act

- personal information of users who use information and communications service
- regulation on information and communications service providers

Credit Information Act

- personal credit information necessary to determine the credit rating, credit transaction capacity, etc. of an natural person
- regulation on credit information company, credit information collection agency and credit information provider/user(including non-financial institutions)

- amended on May 28, 2014 in accord with PIPA
  - prior consents required to collect and provide personal credit information
- pre-announcement of amendment
  - applied only to financial institutions and financial information

(2) RESTRICTION ON MANAGEMENT OF RESIDENT REGISTRATION NUMBERS

PIPA

- no personal information manager shall manage resident registration numbers except the following cases: amended on Nov. 19, 2014

  1. Where any statute specifically requests or permits to manage resident registration numbers;
  2. Where it is deemed obviously necessary for the urgent benefit of life, body or property of a subject of information or a third party;
  3. Cases prescribed by Ordinance of the Ministry of Government Administration and Home Affairs, which correspond to subparagraph 1 or 2 and in which cases it is inevitable to manage resident registration numbers.

- **exception of information self-determination scheme**

(3) ADOPTION OF A STRONGER SCHEME FOR RECOVERY OF DAMAGES

Background

- shift of burden of proof in a claim for damages

- But until now, many lawsuits seeking damages for personal information breach ended up awarding victims only KRW 100,000-200,000 per individual as compensation for the emotional distress, even if the data processor was at fault. Furthermore, a data subject is required to prove his or her emotional distress and suffering caused by the leak of personal information to qualify for compensable damages.

- Following the massive leakage of personal information from credit card companies in January 2014, there has been constant demand to overhaul the relevant law

(3) ADOPTION OF A STRONGER SCHEME FOR RECOVERY OF DAMAGES

Statutory Damages

- **Introduction of Statutory Damages**

  - Article 32-2 of Network Act amended on May 28, 2014
  - Article 43-2 of Credit Information Act amended on March 11, 2015
  - Article 39-2 of PIPA amended on July 24, 2015

  - if a person whose personal information is lost, stolen or leaked by willful misconduct or negligence of a personal information processor, such person is entitled to claim statutory damages of up to KRW 3 million instead of prvoving actual damages

- Reportedly, the Supreme Court will overhaul its standards for calculation of compensation for damages caused by personal information breach and implement them

(3) ADOPTION OF A STRONGER SCHEME FOR RECOVERY OF DAMAGES

Punitive Damages

- **Introduction of Punitive Damages**

  - Article 32 (2) and 32 (3) of Network Act amended on March 22, 2016
  - Article 43 (2) and 43 (3) of Credit Information Act amended on March 11, 2015
  - Article 39 (3) and 39 (4) of PIPA amended on July 24, 2015

  - if personal information is damaged by <u>willful misconduct or gross negligence</u>, the court may determine punitive damages of up to <u>three times the actual damages.</u>

(4) REGULATIONS GOVERNING CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

PIPA

- for cross-border provisions of personal information, the controller should get the prior consent and shall not enter into a contract contravening PIPA

Network Act

- From September 30, 2016, the user's consent must be obtained for the following types of cross-border transfer of personal information (Article 63)
    (a) provision of personal data to a third party
    (b) outsourcing of processing of personal information
    (c) storage of personal data

- in the cases of (b) and (c), ICSPs may be exempted from user consent requirements if all of the following elements are satisfied
    (i) necessary to perform a contract and increase the convenience of the user
    (ii) the ICSP has disclosed all required matters via its privacy policy or individually notified users via a statutorily-prescribed method such as email

(4) REGULATIONS GOVERNING CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

Credit Information Act

- pre-announcement of amendment
  - for cross-border provisions of credit information, prior consents of the data subject or conclusion of a contract in accord with the guideline set by FSC required

※ *changes to the* <u>*Regulations on Delegation of Information Processing and IT Facilities of Financial Companies*</u>

- *abolishing the approval requirement for delegation of IT facilities*
- *ex post facto report for delegation of information processing except for financial transaction information of individual customers*
- *permitting delegation to third parties such as IT firms and sub-delegation subject to the same standards applicable to delegation.*

(5) REGULATION ON SMARTPHONE ACCESS

Network Act

- New Provisions Regarding Smartphone Access By App Developers etc. (Article 22-2)

  - From March 23, 2017, ICSPs (e.g., smartphone app developers) wishing to access stored data or functions within a user's smartphone will be required to obtain the user's prior informed consent to the granting of certain access authority ("Smartphone Access Authority")

  - In conjunction with ICSPs, the developer/supplier of a mobile handset's basic operating system, the manufacturer of a mobile handset, and the developer/supplier of a mobile handset's software are also required to implement necessary measures to protect the personal information of the user – including having in place a function which allows the user to provide or withdraw his/her consent to the granting of Smartphone Access Authority to the ICSP.

(6) BIG DATA ISSUES

What Big Data Mean

- "a term that describes large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information" (demystifying big data – practical guide to transforming the business of government" techamerica foundation)

- amount of data being collected and change in how they are used

- benefits to individuals and society
- potential threats to individual privacy
  - over-collection, use unrelated to the original purpose, fusion leading to new data and new meanings

- big data, big innovation, big brother

(6) BIG DATA ISSUES

OECD Privacy principles in 1980

1. Collection Limitation Principle

2. Data Quality Principle

3. Purpose Specification Principle

4. Use Limitation Principle

5. Security Safeguards Principle

6. Openness Principle

7. Individual Participation Principle

8. Accountability Principle

(6) BIG DATA ISSUES

OECD Privacy principles in 1980

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

(6) BIG DATA ISSUES

- On December 2014, KCC announced the final version, 'Guidelines for Protection of Big Data Personal Information', detailing specific standards for the protection and safe use of personal information in connection with the processing and utilization of big data.

  - publicly available information, where the data subject or the rightful person has provided the information without any restriction
  - details of the history of access or use of the service

- **de-identification based approach**

(6) BIG DATA ISSUES

Guideline for Protection of Big Data Personal Information

- de-identification (sections 3, 4, 5, etc.)

  - making impossible to identify a particular user, even if such information is combined with other information
  - at the stage of data collection through deletion, pseudonymization, aggregation, categorization and data masking

- allowed to collect and exploit personal information without user's consent (article 4), provide such information to a third party (article 10), and use them internally for the purpose of provision of their services, unless the user expressly refuses (article 9).

(6) BIG DATA ISSUES

Guideline for Protection of Big Data Personal Information

- immediate destruction of re-identified personal information and measures to make such personal information unidentifiable (Sections 3 and 6)

- prohibition on collection, exploitation or analysis of sensitive information and communications secrets (Sections 7 and 8)

- promotion of transparency (Sections 4, 5 and 6)

- technical, managerial measures to protect collected information for storage and maintenance {Section 3(2)}

(6) BIG DATA ISSUES

PIPA

- **Notice Requirements For Certain Data Handlers Seeking To Process Personal Information Received From Third Parties {Article 20 (2), (3)}**

  - In the event a data handler who satisfies certain criteria set forth in the Presidential Decree with respect to the type and volume of personal information, number of employees, and volume of sales revenue ("Substantial Data Handler")intends <u>to process personal information it receives from anyone other than the data subject,</u> even though the personal information was transferred lawf ully (e.g., with the data subject's consent pursuant to Article 17(1)(i) of the PIPA), <u>the Substantial Data Handler must also notify the data subjects of (i) the sources from which their personal information was collected, (ii) the purposes of processing of the subject personal information, and (iii) other required matters prior to the data processing.</u>