Data Protection

Laws of Korea

|CONTENTS|

01 Basic Structure - constitution

The right to privacy is a fundamental right

▶▶ 'The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private living. Concretely, the privacy protection is defined as protecting and maintaining the confidential secrecy of an individual; ensuring the inviolability of one's own private life; keeping from other's intervention of such sensitive areas as one's conscience or sexual life; holding in esteem one's own personality and emotional life; and preserving one's mental inner world'. *Constitutional Court, 2003. 10. 30. 2002Hun-Ma518*

The right to control one's own personal information is a fundamental right

▶▶ '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 info-communication technology.' *Constitutional Court, 2005. 5. 26. 2004Hun-Ma190 (Consolidated)*

01 Basic Structure - laws

> ## The Data Protection Laws of Korea consists of general law and specific laws.

▶▷ A general law – Personal Information Protection Act (PIPA)

▶▷ Specific sector laws
– Utilization and Protection of Credit Information Act, Network Act, etc.

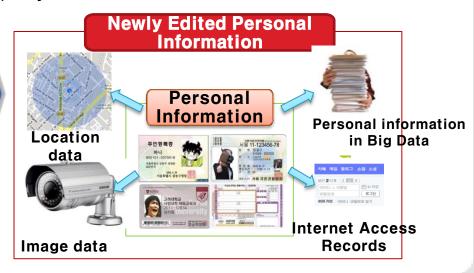> ## The Data Protection Laws of Korea regulate 'data handler'

▶▷ a public agency, company, organization, or individual that by itself
 or through a third party, handles 'personal data' to make use of
or carry out any operation of a 'personal data file'
in the course of or in relation to its business activities.

01 Basic Structure - laws

Personal Information: information that pertains to a living person
– location and image data, internet access records are also included as a personal information

- **Data which can identify the individual in question** (RNN, passport number, drivers' license number, etc.)

- **Data which can identify the individual by easily combining with other information** (name+phone number, name+e-mail+work piece, etc)

Existing Personal Information

RNN, drivers license number, name, etc.

Newly Edited Personal Information

Personal Information

Location data

Image data

Personal information in Big Data

Internet Access Records

01 Basic Structure - laws

| Specific Sector Laws | ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.

ACT ON THE PROTECTION, USE, ETC. OF LOCATION INFORMATION | USE AND PROTECTION OF CREDIT INFORMATION ACT

ACT ON REAL NAMES FINANCIAL TRANSACTONS AND CONFIDENTIALITY
……… | MEDICAL SERVICE ACT

FRAMEWORK ACT ON HEALTH EXAMINATION

ACT ON WELFARE OF PERSONS WITH DISABILITIES

………… | FRAMEWORK ACT ON EDUCATION

ELEMENTRARY AND SECONDARY EDUCATION ACT

EARLY CHILDHOOD EDUCATION ACT
…… | Many special laws on
………
Passport, Taxation, Police, Customs, Etc.
……… |
| | Personal Information in ONLINE COMMERCE | Credit & Financial Information | Health Information | Student Information | |

| General Law | Personal Information Protection Act |

02 Comparison with OECD Guidelines

1 Collection Limitation Principle

- ✓ obtain **prior opt-in** consent from the data subjects when collecting personal information (Article 15(2) of PIPA, Article 22(1) of IC Network Act)

- ✓ collect only the **minimum** amount of personal information necessary to achieve the contemplated purposes of data processing (Article 3(1), 16(1) of PIPA, Article 23(2) of IC Network Act)

- ✓ adequately process the personal information to the extent necessary to achieve such purposes (Article 3(4) of PIPA)

- ✓ not use personal information for any other purposes (Article 18 of PIPA, Article 24 of IC Network Act)

- ✓ not refuse to provide the service just because the data subject did not consent to the collection of his/her personal information (Article 16(3) of PIPA, Article 23(3) of IC Network Act).

02 Comparison with OECD Guidelines

2 Data Quality Principle

Data Handler is required to:

- ✓ **ensure** that personal information is **accurate, complete** and **up-to-date** (Article 3(3) of PIPA)

3 Purpose specification principle

Data Handler must **notify** the following **before** obtaining the consent (Article 15(2) of PIPA, Article 22(1) of IC Network Act):

- ✓ **purposes of collection/use of personal information**

- ✓ **items** of personal information to be collected,

- ✓ **duration** of retention/use of personal information

- ✓ the fact that the data subject has **the right to refuse** to give consent to such collection/use, and disadvantages, if any, to the data subject to be caused by such refusal.

02 Comparison with OECD Guidelines

4 Use limitation principle

Data Handler is required to:

- ✓ not use the personal information for any other purpose (Article 18 of PIPA, Article 24 of IC Network Act)

- ✓ notify the purpose of use, the name of the 3rd party, etc. **before** obtaining such consent (Article 17(2) of PIPA, Article 24-2(1) of IC Network Act)

5 Security safeguards principle

Data Handler must process personal information in such a manner as to minimize the possible infringement upon the privacy of the data subjects (Article 3(6) of PIPA).

Security measures that **must** be taken by Data Handler includes the following:

- ✓ an internal control plan, access management, encryption of personal Information, retention of access logs/records and prevention of forging or fabrication of access logs/records, installation and operation of security programs, physical security

02 Comparison with OECD Guidelines

6 Individual participation principle

A data subject may make a **request to inspect, suspend, correct or remove his/her personal information** processed by the Data Handler (Article 35, 36, 37 of PIPA, Article 30 of IC Network Act).

7 Openness principle

Data Handler must **publicly disclose** its **privacy policy** (Article 30 of PIPA, Article 27-2 of IC Network Act) and **notify** the data subject of **the specific usage** of personal information **at least once a year** (Article 30-2 of IC Network Act).

8 Accountability principle

Data Handler must comply with PIPA, IC Network Act and relevant law. Violation of such law may entail criminal punishment, administrative penalty or fine, etc.

03 Key features – main contents of PIPA

PIPA

9 CH 81 Articles addenda

- **CH I General Provisions** – Purpose, definition, Responsibilities of state, etc.

- **CH II Establishment, Etc. of Personal Information Protection Policies**
  – Personal Information Protection Committee, Basic plans, Personal information protection guidelines, etc.

- **CH III Restrictions on Management of Personal Information**
  – Collection/use/provision of personal information, Restrictions on management of sensitive info, etc.

- **CH IV Safe Administration of Personal Information**
  – Duty to take safety measures, registration and disclosure of personal information files, etc.

- **CH V Guaranteeing Rights of Subjects of Information**
  – Inspection of personal information, correction or deletion of personal information, etc.

- **CH VI Personal Information Dispute Mediation Committee**
  – Establishment and composition, status guarantee of members, handling period, request for data, etc.

- **CH VII Class Actions on Personal Information** – Exclusive jurisdiction, etc.

- **CH VIII Supplementary Provisions** – Partial exclusion from application, prohibited acts, etc.

- **CH IX Penal Provitions** – Penalty, fines, fines for negligence, etc.

Addenda : Enforcement date, Repeal of other Acts, Relationship with other acts, etc.

03 Key features

- ✓ **Strict regulation for each stage of the life cycle of handling personal information :**

- ✓ **Prior opt-in consent**

- ✓ **Stronger protection for important personal information**

- ✓ **Privacy Officer and Privacy Policy**

- ✓ **Data Breach notification and report**

- ✓ **Administrative sanctions, Civil liability, Imprisonment, etc**

- ✓ **Personal Information Dispute Mediation Committee**

04 Enforcement and Practice

Brief statistics regarding Administrative sanctions by MOI (on Aug. 18, 2015)

Year	No. of Administrative Dispositions taken
2012	726
2013	469
2014	507
2015	61

Brief statistics regarding Criminal prosecution

	2010	2011	2012	2013	2014	Total
PIPA	–	6	128	269	628	1,031
Credit Information Act	31	60	25	90	57	263
Location Information Act	25	34	49	72	45	225
Network Act*	48	39	12	31	167	297

Source: Supreme Prosecutors' Office, Public Prosecution Yearbook 2010–14.
Note: * Data leakage-related violations only.

Thank you