SOUTH KOREA

[ADPL Ch 5 ‘South Korea – The Most Innovative Law’]

 South Korea

- *Context:* Since 1980s, one of world's most successful transitions from dictatorship to democracy – very strong democratic and civil libertarian elements. Also the most Internet-intensive country.
- Strong *constitutional protections* via Constitutional Court
- Civil Act gives *tortious action*, used in mass data breaches
- Three largely consistent *data privacy Acts*:
  - Comprehensive *Personal Information Protection Act (PIPA) (2011)* added many new features including 1st DPA (PIPC)
  - BUT 'Network Act' (under Korean Communications Comm) continues to govern ISPs & ICSPs – see 2017 *Update* p 15.
  - Similar sectoral Acts still govern finance industry (Credit Information Act).
- Continuous strengthening of all enforcement since 2011

Overall assessment: Strongest data privacy laws in Asia, but with some key weaknesses impeding an EU adequacy finding.

- PIPA's enforcement was largely provided by a Ministry (+KISA)
- PIPA's scope did not cover large important parts of private sector
- Result is an intense 'turf war' between agencies

South Korea – Additional principles

PIPA 2011 includes **all basic OECD principles**, plus **these additions**:

1. **Onus** of proof of almost all requirements is on the processor
2. Privacy Policy necessary, and overrides any individual agreements where this favours the consumer (A 30) (strong **transparency**)
3. **Minimal** collection of personal data necessary for purpose (A 16(1)
   - Desirability of 'anonymity, if possible' of processing (A 3(7))
4. No denial of services because of refusal to provide unnecessary information (A 16(2)) + 2013 amendment requiring notice of this (**unbundling** consents)
5. Sensitive data cannot be processed without consent (A 23)
6. Alternatives to identification by the Residence Registration Number must be provided (A 24) [RRN use is separately being prohibited]
7. Strict limits on operation of visual surveillance devices (A 25)
8. **Notification** required if personal data collected from 3rd Ps (A 20)
9. Consent required to disclose to 3rd Ps, who must be identified (A 17)
   - limited exceptions (A 18) *not* including 'compatible uses'

South Korea – Additional principles (2)

10. Data exports require consent (A 17(3)) - but notice is weak
11. **Notice of sub-processing** is required (A26), and must be identified
    - OR public Privacy Policy (PP) can give notice of sub-processing
    - sub-processors are deemed employees (A 26(6)) (vicarious liability)
12. **Deletion** (not de-ID) of personal data required after use (A 21)
13. **Suspension** of processing can be required by data subject (A 37)
14. **Privacy Officer** must be appointed, with detailed duties (A 31)
    - MOSPA Guidelines do not specify any size limit of business
15. **Data breach notification** always mandatory to data subjects (A34)
    - Also to Ministry and other authorities if 'large scale'
    - 'Surcharges' of up to $0.5M if RRNs are negligently lost
16. Offences to improperly deal with, disclose or receive personal data
17. Detailed security measures are prescribed by Presidential Decree, both locally and for data exports

These 17 points mean Korea does cover ***most*** elements of the GDPR

South Korea – Range of enforcement measures (1)

- See 2019 Update, pp 10-11; see also 2017 Update, pp 15-17
- Korea has the most comprehensive 'enforcement toolkit' in Asia

1. *Administrative fines/'surcharges'*
   - 'Administrative surcharges' (fines) of up to 3% of business turnover can be issued by KCC or financial regulator; Bill for PIPC to do so is before legislature
   - *Interpark Case* resulted in US$4.5M surcharge by KCC on a shopping mall for negligent data leak (see 2019 Update p. 11) – largest Asian fine, larger than EU until 2019)
2. *Compensation (including statutory damages)*
   - Data subjects may *sue for damages for breach* (A 39)
   - Onus of proof of no intent/ negligence is on data user
   - Many actions, including class actions, but major problems in providing damage: 2011 case held massive data leak did not automatically result in damages for mental distress;
   - Reforms**: Statutory damages** (no proof of individual actual damage required) of US$3K/head for data breaches involving intentional/negligent breach resulting in data loss, theft or leakage (some cases have 1M+ claimants);
   - **Punitive damages** = treble actual damage suffered, where gross negligence occurs

South Korea – Enforcement (2)

3. *Compliance orders*
   - Ministry and agencies can issue compliance orders and fines (468 in 2013).
4. *Criminal offences*
   - Complex lists of which breaches attract which penalties
5. *Collective dispute mediation* by PIDMC (A 49)
   - PIDMC = Personal Information Dispute Mediation Committee
   - Where multiple data subjects are affected, any parties can request PIDMC to undertake collective dispute mediation
   - Presidential Decree sets out procedural details. Mediation continues even if some complainants go to Court
6. *Class actions* (Part 7 'Data protection collective suit')
   - If processor rejects collective mediation, various types of NGOs (defined in Act) are entitel to file a class action ('collective suit')
   - Suit is filed in the District Court of the defendant's place of business, or main office of foreign business's representative (A 52)
7. *Self/Co-regulation is not significant*
   - No provisions concerning enforceable codes in PIPA
   - Ministry is required to facilitate self-regulation
   - Korea has agreed to join APEC-CBPRs but has not appointed an AA

Korea – **Issues for EU adequacy**

- *2019 update pp. 11-12; 2017 Update* pp 12-18; 2018 *Update* pp 8-9
- Korea applied for adequacy 2016; being assessed 2019, after Japan
  - May have changed from limited scope under its Network Act (KCC as DPA) to comprehensive scope under PIPA (PIPC as DPA) – but this requires legislation

1. Independent powers of DPA
   - PIPC is not independent from Ministry in its exercise of powers - fatal
   - KCC is independent, and stronger powers: but KCC limited to online ISPCs
   - PIPA Bill before legislature (i) makes PIPC independent; (ii) transfers to PIPC enforcement powers of Ministry, KCC & FSA; (iii) gives PIPC same powers across all sectors. If enacted, this is a major redistribution of powers.
2. Big Data/ de-identification/anonymisation
   - Guidelines (2016) by multiple agencies: If data is PI, de-ID procedures specified, and security etc rules still apply – but then not regarded as PI; much NGO dissent
   - 2018: Korean agencies agreed to **adopt EU definition** of anonymous data, to strengthen adequacy bid; PIPA Bill implements this, but some 'processing' of pseudonymised data is still allowed – disputed.
   - **Result:** Both definition of PI & of anonymisation, are consistent with GDPR

Korea – **Issues for EU adequacy (2)**

3. Data export and onward transfer restrictions
   - Amendts in PIPA Bill (originally proposed for Network Act):
     - continues to allow data exports based on consent;
     - specific notice requirements (destination country and company, purpose, retention period, security);
     - Up to 3% turnover fines for exports without consent;
     - Purports to bind overseas recipient – enforceability uncertain;
     - Gives PIPC power to suspend any cross-border transfers if risk of severe violations of users' rights
     - Foreign businesses must appoint **local agent**; joint liability
4. Other changes to closer align with EU GDPR
   - Credit Information Bill propose data portability & controls on automated decisions – may be included in other Bills.

Korea – **Issues for EU adequacy (3)**

4. Defn of 'personal information' (PI) in PIPA & Network Act
   - PI only applies where '*easily* combined' to enable identification (some English translations)
   - KCC and other agencies relied on this to 'carve out' such data as not PI in the 2016 Big Data Guidelines
   - but *IMEI decision* (Seoul District Court, 2013) interpreted PI very broadly to include any possibility of obtaining data, even if a court order was necessary to do so. No legislative change proposed.

6. Current position on adequacy negotiations
   - PIPA and other Bills are deadlocked in National Assembly
   - EU Commission had said adequacy discussions are at an 'advanced stage'
   - BUT no sign that a narrow adequacy decision is being considered

5. Who will benefit from changes to obtain adequacy?
   - Everyone, including Koreans, will benefit from current Bills;
   - No sign yet that Korea is negotiating 'EU only' reforms (contrast Japan)
   - A Korean COM decision based on 'inclusive' reforms will help restore adequacy.