

University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012

Paper 28

Korea's New Act: Asia's Toughest Data
Privacy Law

Graham Greenleaf*

Whon-il Park[†]

*University of New South Wales

[†]Kyung Hee University

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps12/28>

Copyright ©2012 by the authors.

Korea's New Act: Asia's Toughest Data Privacy Law

Graham Greenleaf and Whon-il Park

Abstract

South Korea's new *Personal Information Protection Act* came into force on 30 September 2011. A six month grace period in which the Act was not strictly enforced ended on 31 March 2012. Business commentators describe the Act as the 'strictest in the world', as the Asian law to which most attention should be paid, and as a law likely to be enforced. This brief article explains why.

The new Act replaces the existing *Public Agency Data Protection Act* in whole and in relation to the private sector it replaces in part the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.* That Act will continue to provide additional privacy and other obligations on information and communications service providers (ICSPs). Korea's previous legislation had considerable limitations. In the private sector, its scope was limited to businesses utilising telecommunications services, although it was actively enforced by a novel mediation structure that is being continued under the new legislation. The public sector legislation, administered by Ministry of Public Administration and Safety (MOPAS), covered all public agencies, and included most basic OECD principles, but with few limits on excessive data collection by governments. However, there seems to have been minimal enforcement.

The new Act is therefore a comprehensive Act for the first time, because it covers both public and private sectors, and the whole of the private sector. More than 3.5 million public entities and private businesses are now regulated by common criteria and principles, and common enforcement mechanisms. It added many new features to existing strong foundations.

The article identifies seventeen ways in which this Act's Principles exceed the

OECD/APEC standards, including: an independent fifteen member Data Protection Commission (a departure from the Ministry-based enforcement of civil law neighbours Japan and Taiwan); Privacy Compliance Officers required for most businesses and agencies; collective mediation for disputes with widespread small damage; mandatory data breach notification to both affected individuals and to authorities where significant; mandatory Privacy Impact Assessment (PIA) for potentially dangerous public sector systems; and explicit (opt-in) consent required for marketing using a company's own databases.

The new Act establishes a complex administrative and enforcement structure which involves five parties: (i) The Data Protection Commission (DPC); (ii) The Korea Internet & Security Agency (KISA) and its Personal Data Protection Center (PDPC); (iii) The Personal Information Dispute Mediation Committees (Pico); (iv) The Ministry of Public Administration and Security (MOPAS); and (v) The Korea Communications Commission (KCC). Korea has developed a system unique in the Asia-Pacific of two independent bodies, one for complaint resolution (Pico), serviced by a government agency (KISA/PPDC) and the other (the DPC) for 'policy matters' (with its own internal secretariat).

Korea's new Act: Asia's toughest data privacy law

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales, Australia.

Whon-il Park, Professor of Law, Kyung Hee University, South Korea

Privacy Laws & Business International Report, Issue 117, 1-6, June 2012

28 May 2012

Contents

A comprehensive new Act now being enforced	1
Beyond the OECD and APEC Principles in 17 ways	2
Complex policy and enforcement structures.....	4
The Data Protection Commission (DPC).....	4
The PDPC within KISA	5
The Ministry of Public Administration and Security (MOPAS).....	5
The Personal Information Dispute Mediation Committees (Pico)	5
The Korea Communications Commission (KCC)	
New enforcement actions and remedies	6
Conclusions: The strongest law in Asia – and beyond?	6

A comprehensive new Act now being enforced

South Korea's new *Personal Information Protection Act*¹ was promulgated on 29 March 2011, and came into force six months later on 30 September. However, the government allowed a further six month grace period in which the Act was not strictly enforced, but that ended on 31 March 2012. The new Act replaces the existing *Public Agency Data Protection Act* in whole and in relation to the private sector it replaces in part the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc* (ICN Act). That Act will continue to provide additional privacy and other obligations on information and communications service providers (ICSPs). The new Act is therefore a comprehensive Act for the first time, both because it covers both public and private sectors, and the whole of the private sector. More than 3.5 million public entities and private businesses are now regulated by common criteria and principles, and common enforcement mechanisms. The new Act has added many new features to existing strong foundations (at least in relation to the private sector). Significant content depends on regulations for which there is no English translation as yet.²

Korea's previous legislation had considerable limitations. In the private sector, its scope was limited to businesses utilising telecommunications services, although it was actively enforced by a novel

¹ An English version of the *Personal Information Protection Act* translated by Whon-il Park is available at <<http://koreanlii.or.kr/w/images/9/98/DPAct1110en.pdf>>

² Quotations from regulations in this article are translations by Whon-il Park.

mediation structure (including publication of case details) that is being continued under the new legislation. The public sector legislation, administered by Ministry of Public Administration and Safety (MOPAS), covered all public agencies, and included most basic OECD principles, but with few limits on excessive data collection by governments. However, there seems to have been minimal enforcement, and no publication of case details. Korea also has a number of Acts with specific requirements (e.g., on medical records, on credit reporting, and on ICSPs) which will still take precedence over the new Act (A 6).

In addition to its comprehensiveness, other key innovations in the new Act include: an independent fifteen member Data Protection Commission (a departure from the Ministry-based enforcement of civil law neighbours Japan and Taiwan); Privacy Compliance Officers required for most businesses and agencies; collective mediation for disputes with widespread small damage; mandatory data breach notification to both affected individuals and to authorities where significant; mandatory Privacy Impact Assessment (PIA) for potentially dangerous public sector systems; and explicit (opt-in) consent required for marketing using a company's own databases. Details are given below.

For these and other reasons, business commentators are describing this Act as the 'strictest in the world', as the Asian law to which most attention should be paid, and as a law that is likely to be enforced.³

Beyond the OECD and APEC Principles in 17 ways

Korea's new Act includes all of the basic requirements of the OECD's privacy Guidelines and its derivative, the APEC Privacy Framework, because all of those matters were satisfied by the previous legislation. The previous private sector legislation already went beyond the OECD/APEC model, but was of limited scope. The new legislation extends the scope of all those 'OECD-plus' aspects to the public sector and to the rest of the private sector, as well as adding more new protections. Rather than focus only on these new aspects, it is more useful to consider all of the ways in which the Korean Act now exceeds the OECD/APEC minimum standards for data privacy laws. The Act first makes a general statement of Data Protection Principles (A 3), and Rights of the Data Subject (A 4) and then provides detailed obligations in relation to all Principles (As 15-39). The brief summary following identifies seventeen ways in which this Act's Principles exceed the OECD/APEC standards. At a greater level of detail, more could be found.

1. The *onus of proof* of almost all requirements under the Act is on the processor, not on the individual who is claiming a breach (As 22(2), 39).
2. Only the *minimum collection* of personal data necessary for the purpose of collection is allowed (A 16(1)). Processors are also required by the general DP Principles to 'make efforts to process personal information in *anonymity*, if possible' (A 3(7)). The Act's requirements are therefore at least the European standard (minimality), and in some cases anonymity.
3. A distinctive Korean principle is that there must be *no denial of services* because of a person's refusal to provide legally unnecessary information (A 16(2)). Organisations therefore cannot decline to provide services if a person refuses to provide more than the minimum data allowed to be collected. Such refusal would be a separate breach of the Act.
4. *Sensitive data* cannot be processed without consent (A 23).

³ Quotations from a business conference in Washington, cited in BNA staff 'Strict New Privacy Law's Grace Period For Enforcement Ends March 31, 2012' 12 WDPR 25, *BNA World Data Protection Report*, 2012

5. *Alternatives to identification* other than the Residence Registration Number (RRN) must be provided (A 24). Further new Korean legislation now has even tighter requirements on ICSPs, who will be prohibited from collecting RRNs except in very narrow circumstances.⁴
6. There are strict limits on operation of *visual surveillance devices* (such as CCTV) in public places (A 25).
7. A Privacy Policy must notify individuals how to *opt-out of automated collection* of personal data (A 30).
8. Notification to the data subject is required when personal data is *collected from third parties* (A 20).
9. *Consent for disclosure* to third parties is required, and they must be *identified* (A 17). There are limited exceptions (A 18), but these do not including 'compatible uses' or similar expressions. The consent requirements of the Korean Act are one of its strictest requirements, and an aspect that will be considered onerous by businesses.
10. *Notice of sub-processing* to the data subject is required (A26), and the sub-processor must be *identified*. Alternatively, a publicly available Privacy Policy (PP) can give notice of sub-processing. Sub-processors are deemed employees (A 26(6)) of the processor, who therefore has vicarious liability for their actions.
11. *Deletion* of personal data is required after the purpose of processing is complete, or any other retention period completed (A 21). As an example of the latter, where personal data have been unused for a period of time (yet to be specified), ICSPs will have to delete them.⁵
12. *Suspension of processing* can be required by the data subject (A 37).
13. A *Privacy Policy* must be issued, covering required matters (A 30). In the event of any discrepancy between the policy and an agreement with a data subject, whatever is beneficial to the data subject will prevail (A 30(3)).
14. A *Privacy Officer* must be appointed, with detailed duties (A 31). Standard guidelines suggest this officer must be appointed regardless of the size or nature of the entity, and the public or private sector except fraternal associations. This is an application of the EU's proposed version of an 'accountability principle'.
15. *Data breach notification* to data subjects is mandatory (A 34). There must also be notification to MOPAS and other authorities if the breach is 'large scale'. ICSPs will also have additional obligations to notify the Korean Communications Commission (KCC) of any 'data leak or breach'.⁶
16. *Detailed security measures* are prescribed by Executive Orders, both locally and for data exports (As 29, 14(2)).

⁴ Park, K B 'New South Korean Amendments Include New Data Breach Notification Requirements, Expanded Data Protections', *BNA World Data Protection Report*, 2012, referring to 2012 changes to the ICN Act, promulgated on 17 February 2012, and to come into effect on 18 August 2012.

⁵ Park, KB, as above, by the same amendments to the ICN Act.

⁶ Park, KB, as above, by the same amendments to the ICN Act.

17. *Data exports* are subject to prior consent of data subjects, and processors shall be prevented from making contracts of data exports in violation of the the Personal Information Protection Act (A 17(3)).

Complex policy and enforcement structures

The new Act establishes a complex administrative and enforcement structure which involves five parties, and also have an expanded role in applying to both the public and (whole) private sectors:

- (i) The Data Protection Commission (DPC);
- (ii) The Korea Internet & Security Agency (KISA) and its Personal Data Protection Center (PDPC);
- (iii) The Personal Information Dispute Mediation Committees (Pico);
- (iv) The Ministry of Public Administration and Security (MOPAS); and
- (v) The Korea Communications Commission (KCC).

As explained below, Korea has developed a system unique in the Asia-Pacific of two independent bodies, one for complaint resolution (Pico), serviced by a government agency (KISA/PPDC) and the other (the DPC) for 'policy matters' (with its own internal secretariat).

There are no provisions in the new Act for co-regulatory schemes or the issuing of binding sectoral codes, but MOPAS does have a role of promoting and supporting self-regulatory activities (A 13). There was no significant self-regulation in Korea under the previous Act.

The Data Protection Commission (DPC)

The new Act provides for establishment of a Data Protection Commission (DPC)⁷ under the Presidential Office 'to deliberate and resolve the matters regarding data protection', and that it 'shall independently conduct the functions belonging to its authority'. It has a wide range of powers concerning determining policy matters, the giving of opinions, issuing reports, the 'coordination of positions taken by public institutions', and the interpretation of laws and regulations, but not the resolution of individual complaints.

The DPC consists of not more than 15 Commissioners, including a Chairperson (appointed by the President from among the Commissioners who are not public officials) and one Standing Commissioner, a politically appointed official. While the President appoints the rest of the Commissioners, this is within constraints⁸. A secretariat is to be 'established within the Commission' to support its administration. Appointments are for a fixed term of three years. Because of a deadlock in the National Assembly, which is entitled to elect five Commissioners of the 15-member DPC, the nomination of the First Chairperson and deliberation on the Basic Plan for the initial three years and the Implementation Plan for 2012 were postponed accordingly. The Commission was completed in the early January 2012 (with Park, Tae-Jong as Chair), and first met on 9 January 2012.

⁷ The DPC's website <<http://www.pipc.go.kr>> is in Korean only as yet.

⁸ These include that five 'shall be appointed or commissioned from among the candidates elected by the National Assembly', and another five 'from among the candidates designated by the Chief Justice of the Supreme Court'. Other appointees are to be persons recommended by 'privacy-related civic organizations or consumer groups' or 'by the trade associations composed of personal information processors' and others 'who have ample academic knowledge and experiences related with personal information'

The PDPC within KISA

The Personal Data Protection Center (PDPC) receives and investigates complaints, and mediates minor complaints. It assists complainants to prepare complaints to go to Pico. In more serious cases, it notifies MOPAS, police and prosecutors' office of violations or incidents.

The Korea Internet & Security Agency (KISA) will continue to exercise some data privacy functions, such as issuing guidelines for the private sector. KISA actually carries out many of the statutory duties of MOPAS and KCC which both departments have delegated to KISA.

The Ministry of Public Administration and Security (MOPAS)

MOPAS is responsible for preparing a Data Protection Basic Plan every three years, but submits it to the DPC and then carries it out 'subject to the deliberation and resolution' of the DPC (A 9). The Basic Plan is required to include such matters as basic goals, intended improvements and development of counter-measures, facilitating self-regulation, education and training. Departments and agencies are then required to carry this out, once again 'subject to the deliberation and resolution' of the DPC. MOPAS also issues Standard Guidelines concerning data privacy, which departments and agencies can then modify for particular sectors (A 12). It can also investigate the 'actual state of regulatory compliance' in all sectors (A 11).

MOPAS applied for accreditation to the Data Protection Commissioner's conference 2011 (before the DPC was established), but this was refused because it was not independent of government⁹.

The Personal Information Dispute Mediation Committees (Pico)

Pico comprises up to 20 members (now increased from 15 under the previous Act), appointed by MOPAS from among qualified lawyers, academics, senior government officials, and representatives of consumer organizations and IT businesses, and with a non-government chair (A 40). Members have a term of two years, can be re-appointed once, and cannot be removed from office except for loss of qualification, serious offence or incapacity. KISA is likely to continue to provide Secretariat services through PDPC to Pico.).

Pico sub-committees propose informal settlement of complaints. If this fails, then after fact-finding efforts through hearings, discoveries and experts' examinations, Pico suggests a mediation proposal for an agreement by the parties within 60 days from the filing of petition. If it is accepted, the mediation record is executed and becomes legally enforceable like an out-of-court settlement. Otherwise, the data subject may take the matter to court and Pico may support the data subject to conduct the court proceedings with evidence it has obtained and its own findings. The PDPC/Pico combination has been very effective¹⁰ and has resulted in numerous accepted mediations, usually involving modest payments of compensation. Examples of Pico summaries of its mediation decisions are available online in English¹¹. Of 22 reported cases in 2003-04, Pico awarded compensation (from \$100-\$10,000) in 17 cases. Pico mediations usually involve individual disputes with businesses, whereas disputes between individuals go directly to Court.

⁹ Greenleaf G 'Independence and structure of data protection authorities: International standards and Asia-Pacific experience' *Computer Law & Security Review*, Vol 28, Nos 1 and 2, 201, at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971627>

¹⁰ Park, W 'Korea', in Rule, J and Greenleaf, G *Global Data Privacy Laws: The First Generation*, Edward Elgar, 2008

¹¹ 61 Pico decision summaries 2002-07 are at <<http://www.worldlii.org/kr/cases/KRPIDMC/>>. English translations are by Pico.

The Korea Communications Commission (KCC)

KCC, which took over a part of the former Ministry of Information and Communication, is responsible for policy-making on broadcasting and communications, and enforcement of the ICN Act. KCC still regulates ICSPs with respect to data protection as well as communication affairs subject to the ICN Act.

New enforcement actions and remedies

The new Act strengthens the range of remedies and actions that are available in data privacy disputes. Because of the stricter Principles in the Act, it also makes the remedies applicable to a wider range of cases. The followings are some examples:

1. Data subjects may *sue for damages for breach* of any provision of the new Act (A 39). The onus of proof is on the processor of lack of 'wrongful intent or negligence', as well as compliance with the Act and 'non-negligence of due care and supervision'. There are already many actions before the Courts under the old Act, including class actions¹². A court held in 2011 that a massive data leak did not automatically result in damages for mental distress, damage must be proven by the plaintiff.
2. *Collective dispute mediation* by Pico is now possible (A 49). Where multiple data subjects are affected, any parties can request Pico to undertake collective dispute mediation. A Presidential Decree sets out procedural details. Mediation continues even if some of the complainants go to Court.
3. *Class action-like proceedings* are now provided for by the new Act, under the name 'Data protection collective suit' (Part 7). If a processor rejects collective mediation, various types of NGOs (defined in the Act) are entitled to file a collective suit. Suit is filed in the District Court of the defendant's place of business, or of the main office of a foreign business's representative (A 52).
4. There are *new offences* where a person improperly deals with, discloses or receives personal data.

The strongest law in Asia – and beyond?

The new South Korean law is, at least on paper, stronger in its requirements than any other Asian data privacy law¹³. South Korea also has a good track-record of enforcement of its previous law, in relation to the private sector. Depending on how vigorously the new law is enforced in all sectors, future comparisons of effectiveness with laws in European countries, or other countries outside Europe, could see Korea rank favourably in the 'strongest privacy law' category. Businesses need to take very seriously its compliance requirements. Consumer and privacy advocates should note its innovations with interest and probably with admiration.

South Korea is an OECD and APEC member, and a member of the Asia-Pacific Privacy Authorities (APPA), and it wishes to be accredited to the International Data Protection and Privacy Commissioners Conference (IDPCC). It is an influential middle-ranking country, but its influence in data protection is less than it could be, partly because the strength and novelty of its data privacy

¹² Some information on massive scale data breach incidents including the Auction case is available in English at KoreanLII site <http://koreanlii.or.kr/w/index.php/Data_breach_incidents>.

¹³ For a summary of the other Asian privacy laws as at September 2011, see Greenleaf, G 'Major Changes in Asia-Pacific Privacy Laws: 2011 Survey', *Privacy Laws & Business International Report*, Issue 113: 1, 5-14, October 2011; also available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001820>.

laws are too little known. This article has aimed to provide a short introduction to its innovative law.

