Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

South Korea's innovations in data privacy principles: Asian comparisons

Graham Greenleaf [a,*], Whon-il Park [b]

[a] Faculty of Law, University of New South Wales, Australia
[b] School of Law, Kyung Hee University, South Korea

Keywords:
South Korea data privacy law
Privacy principles
Personal Information Protection Act 2011
Data breach
International data flows
Digital identity

ABSTRACT

Over the last two decades, at least a dozen Asian jurisdictions have adopted significant data privacy (or 'data protection') laws. South Korea started to implement such laws in relation to its public sector in the 1990s, then its private sector from 2001, culminating in the comprehensive Personal Information Privacy Act of 2011. Internationally, there have been two stages in the development of data privacy principles (the common core of such laws), the first typified by the OECD's data protection Guidelines of 1981, and the second typified by the European Union data protection Directive of 1995, with a third stage currently under development.

This article analyses the privacy principles in this Korean law, focussing on those aspects that are innovative or offer a high level of protection in international terms, and demonstrates the extent of innovation and strength of the Korean law by comparison with data privacy principles in laws of other Asian jurisdictions. The principles in the Korean law are clearly the strongest in Asia, although this is not yet fully complemented on the enforcement side. A brief comparison is also made with proposed European Union and Council of Europe reforms. In some respects the Korean principles go beyond those currently found in European laws, and indicate that innovation in data privacy legislation no longer originates solely in Europe.

1. Global and Asian contexts of South Korea's privacy law

Over the last two decades, at least a dozen Asian jurisdictions have adopted substantial data privacy (or 'data protection') laws. South Korea started to implement such laws in relation to its public sector in the 1990s, then its private sector from 2001, culminating in the comprehensive Personal Information Privacy Act of 2011. Internationally, there have been two stages in the development of data privacy principles (the common core of such laws), the first

* *Corresponding author*. Professor of Law & Information Systems, Faculty of Law, University of New South Wales, Sydney, NSW 2052, Australia.
E-mail address: graham@austlii.edu.au (G. Greenleaf).
http://dx.doi.org/10.1016/j.clsr.2014.07.011

typified by the OECD's data protection Guidelines of 1980, and the second typified by the European Union data protection Directive of 1995, with a third stage currently under development by the European Union and the Council of Europe.

This article analyses the privacy principles in this Korean law, focussing on those aspects that are innovative or offer a high level of protection in international terms. It demonstrates the extent of innovation and strength of the Korean law by comparison with data privacy principles in laws of other Asian jurisdictions, and with some European comparisons. In some respects the Korean principles go beyond those currently found in European laws, and indicate that innovation in data privacy legislation no longer originates solely in Europe. The article also aims to provide a detailed introduction to the content of Korea's legislation, other than its enforcement and administration.[1]

1.1. *The global development of data privacy laws and international standards*

By mid-2014, 103 countries across the globe have enacted laws that meet the criteria for a national data privacy law.[2] In each decade since the 1970s the number of such laws has grown at an accelerating rate, and the 22 new laws in the first four years of this decade are the highest rate of growth yet seen. Slightly more than half of those laws (53) still come from European jurisdictions (members of the Council of Europe), but there are now 50 data privacy laws outside Europe (plus sub-national laws) and very shortly non-European national laws will be in the majority.

A 'first generation' or 'minimum' set of data protection principles (called 'data privacy principles' in this article) was established by the OECD privacy Guidelines[3] and the Council of Europe data protection Convention 108,[4] both dating from 1981.[5] The EU Data Protection Directive[6] in 1995 and the Additional Protocol to Convention 108[7] in 2001 added further 'European elements'[8] including both additional data privacy principles and enforcement requirements (primarily, the requirement of a data protection authority, and a right of access to the courts) to create a 'second generation' or 'European' set of data privacy principles.

1.2. *Asia's adoption of data privacy laws*

Taking 'Asia' to encompass 26 jurisdictions from Japan to Afghanistan, and from China to Timor Leste, ten Asian jurisdictions have enacted data privacy laws comprehensively covering their privacy sectors, on the above criteria. In chronological order of enactment of private sector coverage they are: Taiwan (1995, revised 2010)[9]; Hong Kong (1996, revised 2012),[10] and South Korea (2001, revised 2011),[11] Macau (2005)[12];

[1] For those aspects, see Greenleaf *Asian Data Privacy Laws*, Ch 5.

[2] These criteria are defined in Graham Greenleaf, "Scheherazade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (2014 forthcoming) J of L & Info Sc, at <http://ssrn.com/abstract=2280877>. The 103 laws are the 101 to which that article refers, plus new laws in the Dominican Republic (2013) and Brazil (2014).

[3] Organisation for Economic Cooperation and Development (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* adopted by OECD Council on 23 Sept 1980 (OECD Doc. C(80)58/FINAL).

[4] Council of Europe *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No. 108; adopted 28th Jan. 1981.

[5] Graham Greenleaf, "Scheherazade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (2014 forthcoming) J of L & Info Sc.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Data Protection Directive) (1995) available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

[7] Council of Europe *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8.XI.2001, available at http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

[8] Graham Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108" (2012) 2(2) Intl Data Privacy L 68.

[9] Personal Data Protection Act 2010 (Taiwan); Greenleaf *Asian Data Privacy Laws*, Ch 6; .Graham Greenleaf "Taiwan Revises its Data Protection Act" *Privacy Laws & Business International Report*, Nos. 108 & 109, 2010–11 <http://ssrn.com/abstract=1975631> (accessed 17 July 2013); Graham Greenleaf and Hui-ling Chen "Data Privacy Enforcement in Taiwan, Macau, and China" *Privacy Laws & Business International Report*, Issue 117, 11–13, June 2012, <http://ssrn.com/abstract=2118332> (accessed 17 July 2013).

[10] Personal Data (Privacy) Ordinance CAP 486 (Hong Kong) <http://www.hklii.hk/eng/hk/legis/ord/486/> (accessed 17 July 2013); Greenleaf *Asian Data Privacy Laws*, Ch 4.; Robin McLeish and Graham Greenleaf "Reform of Hong Kong's Privacy Ordinance After 15 Years" *Privacy Laws & Business International Report*, Vol. 1, Issue 113, pp. 15–17, October 2011, <http://ssrn.com/abstract=1972669> (accessed 17 July 2013); Graham Greenleaf and Robin McLeish "Hong Kong's Privacy Enforcement: Issues Exposed, Powers Lacking" *Privacy Laws & Business International Report*, Issue 116: 25–28, April 2012, <http://ssrn.com/abstract=2057294> (accessed 17 July 2013); Graham Greenleaf "Country Studies: B.3 – Hong Kong" *Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, D. Korff, ed., European Commission, May 2010, <http://ssrn.com/abstract=2025550> (accessed 17 July 2013).

[11] Personal Information Protection Act 2011 (South Korea); unofficial English translation by Whon-il Park <http://koreanlii.or.kr/w/images/9/98/KoreanDPAct2011.pdf>; Greenleaf *Asian Data Privacy Laws*, Ch 5.; Graham Greenleaf and Whon-il Park "Korea's New Act: Asia's Toughest Data Privacy Law" *Privacy Laws & Business International Report*, Issue 117, 1–6, June 2012, <http://ssrn.com/abstract=2120983> (accessed 17 July 2013).

[12] Personal Data Protection Act 2005 (Act 8/2005) (Macau SAR) <http://www.gpdp.gov.mo/cht/forms/lei-8-2005_en.pdf> (accessed 17 July 2013); Greenleaf *Asian Data Privacy Laws*, Ch 9.; Graham Greenleaf "Macao's EU-Influenced Personal Data Protection Act" Privacy Laws & Business International Newsletter, Vol. 96, pp. 21–22, Dec 2008 <http://ssrn.com/abstract=2027852> (accessed 17 July 2013); Graham Greenleaf and Hui-ling Chen "Data Privacy Enforcement in Taiwan, Macau, and China" Privacy Laws & Business International Report, Issue 117, 11–13, June 2012, <http://ssrn.com/abstract=2118332> (accessed 17 July 2013).

Japan (2003, effective 2005)[13]; Malaysia (enacted 2010, but in force November 2013)[14]; Vietnam (2006, 2011, revised 2013),[15] India (Rules 2011 under the Information Technology Act 2000),[16] the Philippines (2012, in force but inoperative until a data protection authority is appointed)[17] and Singapore (2012).[18] To complete the Asian picture, Thailand (1997) and Nepal (2007) have laws that only cover their public sectors. Two further very important jurisdictions – China and Indonesia – have adopted extensive data privacy legislation which falls slightly short of being a full data privacy law in some principles, and also have limitations of scope in applying only to the e-commerce and consumer sectors, and not comprehensively to the private sector. It is of little significance whether we say there are ten or fourteen data privacy laws in Asia (or somewhere in between), the fundamental is that the most economically significant parts of Asia have them or are developing them.

Some of the most informative comparisons that can be made with Korea's law are with Hong Kong, whose law is the longest-established comprehensive law and has seen a history of active enforcement by a data protection authority, with Macau, which has the most 'European' law, and with Singapore, whose law is the most recent enacted in Asia. Where comparisons are given, detailed references at section level will not be given to each piece of legislation that is considered. The footnotes provide a starting point for more detailed research.

2. Korea's Personal Information Protection Act (PIPA)

South Korea has made one of the world's most successful transitions from dictatorship to democracy. Since the gradual overturning of right wing military rule, accelerating from 1980, Korea has in the last thirty years established a very energetic multi-party democracy. It is now a country in which the rule of law is well established. South Korea's achievements in the protection of privacy are therefore relatively recent, but more notable for that, because (as in Eastern Europe at the same time) they represent a significant element of the post-authoritarian construction of a liberal democratic state.

2.1. *Gradual development of data privacy laws*

South Korea's privacy protection legislation has been established sector by sector since the early 1990s. Korea, an OECD member since 1996, initially only legislated in relation to the public sector, like some other OECD members such as Australia, Canada, and Japan. The *Public Agency Data Protection Act* of 1995 included most basic OECD principles, but with few limits on excessive data collection by government, and with coverage restricted to computerised data. There was no guarantee of independence of the oversight body established by the responsible Ministry, no publication of case details, and little apparent enforcement.

Private sector legislation was implemented incrementally from 2001. Chapter 4 of the 2001 Act,[19] 'Protection of Personal Information' was generally known as the '*Data Protection Act*' and is referred to herein as 'the previous Act'. Its scope was limited initially to businesses utilising telecommunications services, but extended to apply to most businesses in relation to personal information on users of their services and their customers in 2007. There was no dedicated data protection authority (DPA), but it was actively enforced by the Korea Internet & Security Agency (KISA), and a novel mediation body (PIDMC), which published case details. Its principles and enforcement were strengthened considerably in 2007, particularly in relation to consent. Its stronger features are continued in PIPA.

[13] Act on the Protection of Personal Information 2003 (Act No. 57 of May 30, 2003) (Japan), <http://www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02>; Greenleaf *Asian Data Privacy Laws*, Ch 8.; Graham Greenleaf "Country Studies – B5 Japan (Information Privacy Protection in Japan)" *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, D. Korff, ed., European Commission, May 2010, <http://ssrn.com/abstract=2025557>.

[14] Personal Data Protection Act 2010 (No 710 of 2010) (Malaysia); Greenleaf *Asian Data Privacy Laws*, Ch 11.; Graham Greenleaf 'Malaysia: ASEAN's First Data Privacy Act in Force' (2013) 126 *Privacy Laws & Business International Report*, 11–14, <http://ssrn.com/abstract=2404893> (accessed 12 May 2014).

[15] Law on information technology (No. 67/2006/QH11) (Vietnam), <http://www.asianlii.org/vn/legis/laws/oit264/oit264.html> (accessed 17 July 2013); Law on Protection of Consumer's Rights (Law 59/2010/QH12 17/11/2010) (accessed 17 July 2013) (Vietnam), <http://www.asianlii.org/vn/legis/laws/pocrl592010121711201039 3/>; Greenleaf *Asian Data Privacy Laws*, Ch 13.; Graham Greenleaf 'Vietnam's 2013 E-Commerce Decree Consolidates Data Privacy Protections' (2013) 125 Privacy Laws & Business International Report, 22–24, <http://ssrn.com/abstract=2369779> (accessed 12 May 2014).

[16] Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011 (GSR 313(E) Dated 11 April 2011) (India) <http://www.mit.gov.in/content/notifications> (accessed 17 July 2013); Greenleaf *Asian Data Privacy Laws*, Ch 15.; Graham Greenleaf "Promises and Illusions of Data Protection in Indian Law" *International Data Privacy Law*, 2011: 47–69, Vol. 1, No 1.

[17] Data Privacy Act of 2012 (Republic Act NO. 10173) <http://www.gov.ph/2012/08/15/republic-act-no-10173/> (accessed 15 August 2013) (Philippines); Greenleaf *Asian Data Privacy Laws*, Ch 12.; Graham Greenleaf "ASEAN's 'New' Data Privacy Laws: Malaysia, the Philippines and Singapore" *Privacy Laws & Business International Report*, Issue 116: 22–24, April 2012 <http://ssrn.com/abstract=2049234> (accessed 17 July 2013).

[18] Personal Data Protection Act 2012 (Act 26 of 2012) (Singapore); Greenleaf *Asian Data Privacy Laws*, Ch 10.; Graham Greenleaf "Singapore's Personal Data Protection Act 2012: Scope and Principles (With so many Exemptions, It Is only a 'Known Unknown')" (2012) 120 Privacy Laws & Business International Report 1 and Graham Greenleaf "Singapore's New Data Protection Authority: Strong Enforcement Powers and Business Risks" (2012) 121 Privacy Laws & Business International Report 14.

[19] *Act on Promotion of Information and Communications Network Utilization and Data Protection, etc (ICN Act)*.

2.2. *Personal Information Protection Act (PIPA) 2011 – a comprehensive Act*

South Korea's new *Personal Information Protection Act* (PIPA) has been enforced since March 2012.[20] It replaces the existing public sector Act in whole and in relation to the private sector it replaces the previous Act except for some additional privacy obligations on information and communications service providers (ICSPs). Korea also has a number of Acts with specific privacy requirements which will still take precedence over PIPA (A 6), in relation to both the public sector[21] and private sector.[22] PIPA is therefore a comprehensive Act for the first time in Korea, covering 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. Statutory references herein are to PIPA unless otherwise stated.

2.3. *PIPA's complex data protection authorities*

PIPA establishes a complex administrative and enforcement structure which involves six parties.

(i) The Personal Information Protection Commission (PIPC), an independent data protection authority (DPA) for the first time in Korea, but with more limited enforcement powers than would be expected of a DPA in Europe;
(ii) The Ministry of Security and Public Administration (MOSPA), which still has the most significant general enforcement powers, despite the creation of PIPC[23];
(iii) The Korea Internet Security Agency (KISA) and its Personal Data Protection Center (PIPC), who continue to a large extent their informal dispute mediation roles under the previous Act;
(iv) The Personal Information Dispute Mediation Committees (DMC or Pico), who continue their formal dispute mediation roles under the previous Act;
(v) The Korea Communications Commission (KCC), which has significant continuing responsibilities for regulation of information and communications service providers (ICSPs), in relation to data protection as well as other areas; and
(vi) Other Ministries and agencies with responsibilities for specific sectors.

Korea has therefore established a unique and multi-faceted enforcement structure, but it is not the subject of this article, and will only be discussed where necessary to explain the operation of privacy principles.

2.4. *Structure of the privacy principles in PIPA*

The Act first makes a general statement of Data Protection Principles,[24] and Rights of the Data Subject[25] and then provides detailed obligations in relation to all Principles.[26] Many Articles have further operative details provided by Enforcement Decree.[27] In addition, there are MOSPA 'Standard Guidelines',[28] and additional guidelines from other central administrative departments or agencies.

The following analysis considers the general and specific principles together, and deals with them in the order of the normal life-cycle of personal information, from collection through to destruction. The privacy principles in PIPA will now be discussed in detail, after consideration of the scope of the Act, with a focus on innovative aspects of the principles and comparisons with other Asian jurisdictions. Where possible, the position in Asian jurisdictions is compared with the requirements of the EU data protection Directive.[29]

3. Scope, comprehensiveness, and enforceability

Of the thirteen Asian jurisdictions that have significant data privacy laws, only six have comprehensive laws covering both the public and private sectors, of which Korea is one. The others are Hong Kong, Japan, Macau, the Philippines, and Taiwan. Three others have laws which cover most of their private sector (India, Malaysia and Singapore), although in all cases with very significant exclusions and no public sector coverage. A further three (China, Vietnam and Indonesia) have laws which only cover their e-commerce and consumer sectors, but not the private sector generally. Nepal and Thailand's laws currently cover only their public sectors.

[20] It was promulgated on 29 March 2011, came into force on 30 September 2011, but the government allowed a 'grace period' to 31 March 2012 before strict enforcement.
[21] In relation to the public sector, privacy protection provisions are found in the *Act on the Communication Secrets*, the *Telecommunications Business Act*, and the *Medical Services Act*.
[22] Other private sector legislation containing data protection provisions includes the *Use and Protection of Credit Information Act*, the *Act on Real Name Financial Transactions and Confidentiality*, the *Framework Act on Electronic Documents and Electronic Commerce* and the *Electronic Signature Act*, the *Act on the Protection and Use of Location Information*, the *Act on the Creation and Facilitation of Use of Smart Grids*.
[23] Prior to the Park Geun-hye government, it was the Ministry of Public Administration and Security (MOPAS).
[24] PIPA (Korea), art. 3.
[25] PIPA (Korea), art. 4.
[26] PIPA (Korea), arts. 15–39.
[27] PIPA Enforcement Decree (KoreanLII, transl. Whon-il Park) <http://koreanlii.or.kr/w/images/d/d7/DPAct_EnforceDecree.pdf> accessed 23 February 2014. The Decree was issued 29 September 2011, is in force from 30 March 2012, and is the only one issued to December 2013.
[28] MOSPA, 'Standard Guidelines' issued September 2011.
[29] References are given to Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd Ed, OUP, 2007), in which references to the specific provisions in the Directive, selected European laws, and court decisions, may be found. References are also given to European Union Agency for Fundamental Rights (FRA) *Handbook on European Data Protection Law* (FRA, 2013).

Compared with the five other Asian laws with comprehensive sectoral coverage, both the definitions used in the Korean law, and the scarcity and narrowness of exemptions from it, only Macau can compare with the comprehensiveness of its coverage.

3.1. *Definitions*

Key terms are defined in Article 2. The Act applies to 'personal information', which is given a conventional definition,[30] essentially meaning any information capable of identifying a living person, including when 'combined with other information'. A natural person so identifiable is a 'data subject'. No Asian laws yet go further than that.[31] Singapore and the Philippines each provide some protection to information about deceased persons, but Korea (like other Asian jurisdictions) does not. Hong Kong imposes a restriction that the information must be collected with the intention to identify the individual (*Eastweek Case*), but this has not been applied elsewhere.

A 'personal information file' is a set of personal information systematically organised to enable easy access. As with all data protection laws influenced by the European data protection Directive, the term 'processing' refers generally to all types of actions that can be taken in relation to personal information.[32] A 'personal information processor' is any person or organisation that processes (directly or indirectly) personal information 'to operate personal information files for official or business purposes'. Laws in Asia include data held in organised manual filing systems, as in Europe,[33] and are not restricted to data processed by automated means (except in India). Information held only in a person's mind is therefore exempt in Korea and elsewhere, with the exception of the Philippines, which specifies that its law applies to personal information 'whether recorded in a material form or not'.

3.2. *Exemptions*

A significant test of the strength of a data privacy law is how comprehensive is its application. Korea's law has few complete exemptions creating 'privacy-free zones': it is unusual in having only partial exemptions. There are no international data privacy agreements in Asia which impose any enforceable obligations concerning scope of data privacy laws. The OECD Guidelines and the APEC Privacy Framework say little about exemptions.[34]

Various categories of personal information are exempt from the principles concerning processing and the enforcement measures in Chapters 3–7, namely, personal information collected under the Statistics Act, for national security analysis, to be processed temporarily in cases where it is 'urgently necessary for public safety and welfare, public health etc', that used for reporting by the press, missionary activities of religious organisations, and nomination of candidates by political parties.[35] Where these exemptions apply, the processor must process the information as little as possible to achieve its purposes, and must make arrangements for security and for handling grievances.[36] However, the normal enforcement provisions will not apply to these obligations. The requirements of consent to collection, privacy policy and privacy officer are also waived for clubs and associations such as alumni associations or hobby clubs.[37] Korea, like Macau and Hong Kong, and like the European Union,[38] does not have any exemption for 'publicly available information, unlike some other Asian laws'. The conventional exemption, found in the EU Directive,[39] for personal data held or used only for personal, household or family affairs, is found in all Asian jurisdictions including Korea. There are no special provisions covering Internet publications by individuals. Widely-accessible publication by individuals via the Internet will probably fall outside the 'personal affairs' exemption in any event, but Korea has not joined Macau in making this explicit by excluding processing for 'systematic communication and dissemination' from the exemption. Korea has one of the strongest media exceptions in Asian data privacy laws, with the Philippines, Hong Kong, Macau and Japan, all jurisdictions which in any event provide constitutional guarantees for freedom of expression which a privacy law cannot override.

Korea's exemptions are not extensive compared with any other jurisdictions in Asia. The Hong Kong and Macau legislation has similarly wide scope. Korea has very narrow exemptions compared with Singapore, Malaysia or India. For example, all types of non-commercial activities are completely exempt from Malaysia's law, and India's law also only applies to 'corporations'. Korea's legislation can be described as largely comprehensive.

[30] '"Personal information" shall mean the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information).' (art. 2).

[31] One Chinese regulation may go further and mean that 'call data' information is by itself regarded as personal data, irrespective of whether it is collected in conjunction with data with the capacity to identify.

[32] '"Processing" shall mean the collection, generation, recording, storage, retention, value-added processing, editing, retrieval, correction, recovery, use, provision, disclosure and destruction of personal information and other similar activities.' (art. 2).

[33] Kuner, *European Data Protection Law*, p. 99.

[34] The OECD Guidelines allow exclusion of data which does not 'pose any risk to privacy or individual liberties', and says exceptions should be as few as possible and made known to the public (arts. 3 and 4). The only specific exclusion from the APEC Privacy Framework is uses for personal, family and household affairs, plus a suggestion that publicly available information may be excluded (art. 11). The only limit it suggests on local exceptions are that they should be (a) proportional to their objectives, and '(b) (i) made known to the public; or, (b) (ii) in accordance with law'. This last use of 'or' appears to be a drafting error and should say 'and' (art. 13).

[35] PIPA (Korea), art. 58(1).

[36] PIPA (Korea), art. 58(4).

[37] PIPA (Korea), art. 58(3).

[38] Kuner, *European Data Protection Law*, p. 93.

[39] EU Directive, art. 3(2).

3.3. *Proving breaches – openness, accountability and onus of proof*

Korea's Act is unusual in how it makes it easier for individuals to prove breaches. This can be seen in three requirements, concerning privacy policies, the onus of proof, and privacy officers.

A *Privacy Policy* must be issued, covering required matters including the purpose of processing, retention period, and any policy concerning disclosure to third parties or consignment for processing.[40] In the event of any discrepancy between the policy and an agreement with a data subject, 'what is beneficial to the data subject prevail'.[41] Processors therefore cannot obtain consents from individuals that are contrary to what their privacy policy promises.[42] No other Asian jurisdiction gives a privacy policy the legal effect of over-riding the data controller's legal relationship with the data subject, whether arising by contract or mere consent.

The *onus of proof* of many requirements under the Act is on the processor, not on the individual who is claiming a breach.[43] Although an individual would still have to prove a breach of Act on the balance or probabilities, once this is done the processor must 'prove non-existence of its wrongful intent or negligence' to avoid payment of damages,[44] and where the damage results from 'loss, theft, leak, alteration or damage of personal information' damages can only be reduced on proof by the processor of 'compliance with this Act and non-negligence of due care and supervision'.[45] No other jurisdiction in Asia imposes such an onus.

A *Privacy Officer* must be appointed, with detailed duties to implement a data protection plan, survey and improving its actual operation, set up internal control systems, investigate complaints and provide 'remedial compensation'.[46] MOSPA Standard Guidelines suggest this officer must be appointed regardless of the size or nature of the entity, and whether a public or private sector body (except fraternal associations). This is similar to the EU's proposed version of an 'accountability principle', and makes it easier for individuals to show that a processor has failed in its duties to properly safeguard personal information. Korea is the only Asian jurisdiction to yet require appointment of data protection officers with such duties and qualifications. India has a very weak requirement that of an identifiable officer responsible for receiving and responding to complaints.

[40] PIPA (Korea), art. 30.
[41] PIPA (Korea), art. 30(3).
[42] In addition there is a requirement in the public sector that all personal information filing systems, with some specified exceptions, must be registered with MOSPA, with the registry being open to 'any person', whether or not they are a data subject of one of the files registered. (PIPA (Korea), art. 32). This is an implementation of the OECD Guidelines 'Openness Principle'.
[43] PIPA (Korea), arts. 16, 22(2), 39.
[44] PIPA (Korea), art. 39(1).
[45] PIPA (Korea), art. 39(2).
[46] PIPA (Korea), art. 31.

4. Collection limitations

The Korean legislation has provisions to minimise collection of personal data, and collection is also limited by the provisions requiring notice, on sensitive information, and ID numbers. PIPA also contains a separate regime for automated visual surveillance devices,[47] which are an unusual inclusion in a data privacy law.

The requirements of purpose specification, consent, and notice are first stated generally (articles 3 and 4), and then more specifically in Chapter 3. Data controllers ('personal information processors') must make their purposes of processing explicit and specific,[48] and data subjects have the right to be informed of that and to consent to it.[49] Processing requires consent,[50] or it must come within a small number of common exceptions (legal requirements, contract, interests of the data subject), or an exception where the data controller's interests are clearly superior to those of the data subject.[51] The data subject must be informed of the purpose of collection and other matters when consent is obtained.[52] How consent is obtained, both at the point of collection, and later for changes of purpose or disclosures, is strictly regulated (see the next section).

4.1. *Minimal collection – a very strong version*

PIPA has a number of principles putting it in the 'most restrictive' category in relation to collection of personal information. At least four provisions contribute to this: minimum collection; anonymity; 'no denial of services'; and unfair collection.

Only the minimum collection of personal data necessary for the purpose of collection is allowed, and the processor has the burden of proof to show that it is the minimum.[53] Korea is

[47] They impose strict limits on operation of 'visual data processing devices', such as CCTV, both in public ('open') places (art. 25, incorporating Provisions CCTV provisions previously in the Public Agency Data Protection Act), and for some sensitive uses within enclosed spaces. These are 'devices installed continuously at a certain place' to take (and store or transmit) pictures of persons or things (art. 2 definition). So a human photographer is not included, nor a device which does not take a representation of a person/thing but only some abstract information such as height or speed. Where these provisions apply the data collected is not considered to be 'personal information' (art. 58(2)), and the normal PIPA provisions do not apply but analogous protections apply, including no use of the information for purposes other than the initial one; no directing cameras to new locations; no collection of audio data in addition (art. 25(6)). and strict security measures (PIPA arts. 25(6) and (7) and PIPA Enforcement Decree, arts. 22–27).
[48] PIPA (Korea), art. 3.
[49] PIPA (Korea), art. 4.
[50] PIPA (Korea), art. 15(1).
[51] Similar to EU Directive, art. 7(f); see European Union Agency for Fundamental Rights (FRA) *Handbook on European Data Protection Law* (FRA, 2013), pgs. 84–90.
[52] PIPA (Korea), art. 15(2).
[53] PIPA (Korea), art. 16(1).

part of the majority of jurisdictions in Asia (also China, Hong Kong, India, Macau, Taiwan and Singapore) which implement the stricter European approach of 'minimal' collection, that personal data should only be collected where it is necessary for a (legitimate) specified purpose,[54] Japan, Malaysia, the Philippines and Vietnam (only by implication) adopt the less strict 'not excessive' approach. Korea's PIDMC reported an example of a company selling financial products of more than a specified value required more personal information than the 'authentication certificate' it normally accepted, which was held not to be excessive collection because this justified a more strict policy.

Processors are also required to 'make efforts to process personal information in anonymity, if possible',[55] as a requirement additional to the principle of minimal collection. The only other data protection Acts to include a specific requirement that anonymity should be offered where possible, are those of Germany and Australia.

A distinctive Korean principle is that there must be no denial of services because of a person's refusal to provide legally unnecessary information.[56] Organisations therefore cannot decline to provide services because a person refuses to provide more than the minimum data allowed to be collected. Such action would be a separate breach of the Act. This principle is reiterated in relation to data subjects who refuse to consent to matters where consent is optional under the Act,[57] discussed later in relation to consent. These protections to data subjects are more explicit than in legislation found in other countries. They are reinforced by 2013 amendments providing that the data subject must be explicitly informed of their right to refuse to provide information more than the minimum necessary.[58] Singapore is similar in the provision prohibiting organisations, as a condition of providing a product or service, from requiring an individual to consent to the collection, use, or disclosure of their personal data beyond what is reasonable to provide the product or service. At best, such restrictions are only implied in other laws, including in most European countries.

PIPA imposes individual obligations on anyone processing personal information, prohibiting obtaining it, or consent relating to it, 'in a fraudulent, improper or unfair manner',[59] which includes what is often called 'unfair collection'. In Asia, only India and Malaysia omit the fair collection requirement.

Taken together, the Korean requirements equate to the European standard (minimality), not the weaker OECD/APEC standards that there be some limits on collection. The other provisions support the minimality requirement, and in the case of the 'anonymity' provision, go beyond it.

[54] Kuner, *European Data Protection Law*, pgs. 73-74.
[55] PIPA (Korea), art. 3(7).
[56] PIPA (Korea), art. 16(2).
[57] PIPA (Korea), art. 24(4).
[58] PIPA (Korea), art. 16(2), amended March 23, 2013 and effective 7 August 2014.
[59] PIPA (Korea), art. 59(1).

4.2. *Google's combined TOS – an example of purpose and consent breaches*

The first decision made by Korea's new data protection authority the Personal Information Protection Commission (PIPC)[60] was that Google's January 2012 changes to the Terms of Service (TOS) of over 60 of its services, unifying them in a single TOS, may be in breach of various provisions of PIPA. Google's TOS changes, which became effective on 1 March 2012, were considered by PIPC to be likely to breach PIPA in three ways: (i) they do not specify the purpose of collection clearly enough, and cannot comply with the requirement that personal information may only be collected and used to the minimum extent necessary for the purpose for which it is collected; (ii) they do not comply with the requirement that where personal information is to be used for purposes other than the purpose for which it was collected, it is necessary to obtain additional consents for such uses; and (iii) they do not specify that that personal information will be erased immediately upon the expiration of its retention period or on request from a data subject.[61] The PIPC decision has not subsequently been confirmed (though the PIPC stated it was waiting for Google's response), nor revoked, and no further decision on this was made by PIPC in 2013–14. Although the PIPC is reported as stating that 'possible further steps could include administrative and criminal sanctions but the most likely outcome in the long term if Google continues its stance will be a fine up to one percent of its annual revenue,' it is not clear what role PIPC would play in any such enforcement action,[62] or even what continuing role in adjudication of disputes concerning individual companies.

4.3. *Sensitive data and IDs*

Sensitive data cannot be processed without consent, and in Korea this includes 'ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life',[63] and 'DNA information obtained from genetic examination' and certain criminal history data under the extinction of punishment legislation.[64] Laws and regulations may make exceptions.[65] The consent required is a specific (non-bundled) consent obtained where the individual is informed of the content required by articles 15(2) or 17(2). About half of Asia's data privacy laws are like Korea in having European-influenced principles of additional protection for a broad range of categories of sensitive personal data (also

[60] Personal Information Protection Commission (South Korea) Decision, 'Comments on Improvements of Privacy Policy of Google Inc.', 11 June 2012, at <http://www.pipc.go.kr/pds/news/120612.html>.
[61] For a more detailed analysis, see Graham Greenleaf and Whon-il Park, 'Korean DPA Faults Google's TOS Changes: Global Privacy Implications?', (2012) 119 *Privacy Laws & Business International Report*, pgs. 22–25 <http://ssrn.com/abstract=2186874>.
[62] It may be more likely that any such fines would result from the Korea Communications Commission's role in relation to regulation of information and communications service providers (ICSPs).
[63] PIPA (Korea), art. 23.
[64] PIPA Enforcement Decree, art. 18.
[65] PIPA (Korea), art. 23(2).

Macau, Malaysia, the Philippines and Taiwan, and Japan in separate provisions). Korea largely follows the EU approach, but also includes 'DNA information obtained from genetic examination'. Some jurisdictions (e.g. Malaysia) include only a sub-set of the European categories, but the Philippines includes other categories. Singapore, Hong Kong, India, Vietnam and China do not have special protections for sensitive data. Businesses dealing with personal information across a range of Asian jurisdictions are likely to find these differences cause problems.

4.3.1. *Special restrictions on unique identifiers*

The most controversial personal information in Korea is the resident registration (RR) number which was previously compulsory in almost all dealings with government and many organisations in the private sector.[66] 'Unique identifiers', namely RR number, passport number, driver's license number and alien registration numbers,[67] may not be processed unless (i) the same consent is obtained as for sensitive data processing or (ii) there is explicit legislative approval.[68] The public sector is exempted. Specific regulation by general data privacy laws of the use of ID numbers is otherwise only found in Hong Kong and the Philippines.

4.3.2. *Resident registration (RR) numbers*

Alternative means of identification other than the RR number must now be provided by processors where individuals are subscribing to web-based services, by specified means.[69] Additional 2012 legislation imposed even tighter requirements on ICSPs, who are prohibited from collecting RR numbers except in very narrow circumstances.[70] Further 2013 legislation, effective August 2014, prohibits any organisation from processing RR numbers, except where laws or regulations explicitly require or allow this, or it is explicitly necessary for the protection of life, body or property of the data subject or a third party.[71] MOSPA is also to take into account the role of RR numbers in any data breaches, in deciding whether to apply very high 'surcharges' on companies responsible.[72] It is therefore, increasingly difficult for private sector organisations to make use of the RR number except where legislation requires this. Further restrictions have already followed the 2014 data breach catastrophe (see part 10 of this article). PIPA has been amended (effective 1 January 2016) so that any personal information processor must encrypt RR numbers, with the scope and timing of the encryption able to be further regulated by Presidential Decree.[73]

However, there is still considerable concern among Korean commentators that there are too many laws allowing or requiring use of RR numbers, and thereby exempt from PIPA article 24, and so RRNs are still very widely used and collected. In January 2014 it was officially estimated that 866 provisions required it to be used.[74] Continuing heavy reliance for identity verification is seen to be an unnecessarily high risk of privacy invasion and identity theft. The problems are particularly intense because Korea's RR number is not a random number, but is composed of 13 digits which reflect a person's sex, year of birth and location of birth, and it is therefore relatively easy to identify a person from an RR number, and vice versa. Because of this structure, it is also impossible for people to change their numbers even after they are compromised.[75] Particular problem areas are seen as ICN Act allowing KCC to authorise by regulation any ICSP to collect RR numbers (and that KCC has authorised all telcos to collect RRNs),[76] and that the Real Name Financial Transactions Act requires use of RR numbers, requiring all banks and credit card companies to collect them.[77] The evolving history of the use of RR numbers in Korea is on the one hand of the most significant attempts in any country to 'roll back' a surveillance mechanism, but on the other hand is a project that is arguably far from complete.

5. Disclosure and use limitations

Articles 17 and 18 of PIPA, setting out the basic principles for disclosure and use of personal information, are somewhat overlapping and confusing, but are in fact consistent. Other principles elaborate the meaning of consent, and impose special rules for data exports, processing, and sale of businesses.

[66] For example, in 2007, abuse of the RR number, even after some initial limitations on its use, still accounted for over 20% of all complaints received by KISA (over 7000 complaints per year), with abuse of all other identification information only about one third of that. (KISA/DMC, *2007 Annual Report*: 22).

[67] PIPA Enforcement Decree, art. 19.

[68] PIPA (Korea), art. 24(1).

[69] PIPA (Korea), art. 24(2) and PIPA Enforcement Decree, art. 19.

[70] ICN Act, arts. 23-2(1). The amended ICN Act, effective 18 August 2012, allows only (i) the authentication agencies, designated by the government for the purpose of provision of alternative ID numbers, (ii) qualified ICSPs permitted by the relevant laws, or (iii) the KCC-notified ICSPs which rely on the collection and use of RR numbers on business. This amendment was caused by a series of massive scale data breach incidents in which RR numbers became a prey to hackers and phishing scammers. For details see Whon-il Park, 'Data breach incidents' (KoreanLII, in English, undated) <http://koreanlii.or.kr/w/index.php/Data_breach_incidents> accessed 14 December 2013.

[71] PIPA (Korea), art. 24-3 (Limitation to processing resident registration number), effective 7 August 2014 (numbering amended from 24-2 to 24-3 by Act 12504, 24 March 2014).

[72] PIPA (Korea), art. 34, as amended 2013, effective 7 August 2014.

[73] PIPA (Korea), art. 24-2, as amended Act 12504, 24 March 2014, effective 1 January 2016.

[74] Kyung-Sin Park 'Paradox of trust: Korean Resident Registration Numbers' (OpenNet blog, 28 May 2014) <http://opennetkorea.org/en/wp/920>.

[75] Kyung-Sin Park 'Paradox of trust'.

[76] Kyung-Sin Park, 'It is Illegal for Telcos to Provide Identification Services' (in Korean) (*Kyunghyuang Sinmun*, 14 March 2013), <http://m.blog.daum.net/ruru63/15972810>.

[77] Kyung-Sin Park, 'Must Ban Collection of RRNs by Financial Institutions in Wake of 100 Million-people Data Breach' (in Korean) (*Kyung-hyuang Sinmun*, 12 February 2014) <http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201402112046175&code=990303>.

5.1. *Consent-based limits*

Consent for disclosure by a processor to third parties is required, except where such disclosure is 'within the scope' of the purpose of collection.[78] Individuals must be informed of the identity of the party to whom the personal information is to be disclosed, the proposed uses, retention, the fact that consent may be denied, and the consequences of refusal of consent.[79] This is the basis of informed consent. In effect, consent is also required for any change of use by the controller[80], and the individual must be informed of the same matters before there is informed consent.[81]

In Asia quite a range of wordings are used to indicate allowed secondary uses, but Korea's provisions only allowing uses and disclosures 'within the scope' of the purpose of collection, may mean that there is no allowing of merely 'compatible' uses, but that other exceptions must be relied upon, including consent. This may be the most restrictive requirement in Asia.

In relation to both disclosure to third parties and change of use by the controller, there are limited exceptions to the need for consent: where special provisions exist in other laws; where the data subject (or legal representative) is not in a position to give consent, or their address is unknown, and it is necessary to protect the interests of the data subject or a third party (but not the interests of the processor); or whether the use disclosure is for 'statistics or academic research' and individuals are 'kept unidentifiable'.[82] Furthermore, the use or disclosure must not be likely to infringe unfairly on the interests of the data subject or a third party. There are further limited exceptions applicable only to public authorities.[83] Where they are relied upon this must be gazetted or notified on the agency's website.[84] The consent requirements of the Korean Act are one of its strictest requirements, and an aspect that will be considered onerous by some businesses.

PIPA also imposes individual obligations on anyone processing personal information prohibiting leaking personal information obtained in the course of business or providing it to another without authority.[85]

5.2. *Examples of disclosure and use complaints*

The majority of the reported PIDMC mediation cases from 2002 to 2007[86] concerned breaches of the previous (similar) disclosure principles. In the reported case resulting in the highest damages to date, a woman specifically requested her mobile phone company not to disclose details of her telephone calls to anyone else. Then she found that a branch of the telephone company had nevertheless disclosed them to her ex-husband, who had produced a copy of her ID card when applying for the details. The mobile phone company was held responsible for professional negligence, and she was awarded 10 million won (equivalent to US$10,000) in compensation for the economic and mental damages. Other reported cases have resulted in damages, more typically of a few hundred dollars. These have involved matters such as (damages amounts are stated in approximate US$): a plastic surgeon displayed a movie of a patient's operation on his clinic's website (US$4000), and the award would have been increased if she had objected it during the filming; a translation service company posted a woman's resume on its website without her consent, as if she was an interpreter employed by them (US$200); an insurance company provided a person's personal information to another company so that they could solicit business from him (US$200); a telecommunications company failed to stop telemarketing after a person unsubscribed (US$300); disclosure to a family member was a breach (US$100).

Since 2007 there have been similar reported cases concerning the previous Act.[87] A company printing wedding invitations used surplus invitations from a person's wedding to show prospective customers, disclosing photos of previous couples (US$200). 'Before and after' photos of a complaint's plastic surgery, placed on a clinic's website, were blurred but still recognisable and were a very serious breach (US$3000). Disclosure of a complaint's phone call history to his wife, by a telco, which did not sufficiently check the documents presented by his wife, was in breach and found to be a contributing factor in a successful divorce action against him (US$5000).

5.3. *Consent – a strong interpretation*

The Korean Act is unusual in both the range of circumstances where consent of the data subject is required (most disclosures and change of use, and data exports) and in what is required for consent to be legitimate. Its requirements are stronger than anywhere else in Asia, and probably anywhere else. Notifications that must be given before consent is obtained (e.g., under A 15(2) or 18(3)) must explicitly separate three types of matters requiring consent, so as to assist data subjects to recognise what requires consent and what does not:

(i) each matter requiring consent must be stated separately, and each consent obtained separately, so that it is possible to consent to one but refuse consent to another (i.e., no 'bundling' of different consents)[88];
(ii) where information is collected which requires consent, it shall be segregated from information which does not require consent (i.e., there should be no misleading bundling of information), and the burden of proof that no consent is required is borne by the processor[89];

[78] PIPA (Korea), art. 17(1).
[79] PIPA (Korea), art. 17(2).
[80] PIPA (Korea), art. 18(2).
[81] PIPA (Korea), art. 18(3).
[82] PIPA (Korea), arts. 18(2)1–4.
[83] PIPA (Korea), arts. 18(2)5–9.
[84] PIPA (Korea), art. 18(5).
[85] PIPA (Korea), art. 59(2).
[86] English summaries of all of these cases are in the Korean Personal Information Dispute Mediation Committee Cases at the AsianLII website <http://www.asianlii.org/kr/cases/KRPIDMC>.
[87] These examples are all from 'PIDMC cases: Noteworthy cases' (KoreanLII, transl. Whon-il Park, 2007-11) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Noteworthy_Cases>.
[88] PIPA (Korea), art. 22(1).
[89] PIPA (Korea), art. 22(2).

(iii) if consent is being obtained so as to use information 'to promote goods or services or solicit purchase therefor' then the data subject must be told this, and their consent to this obtained (i.e., data subjects must opt-in to marketing uses of their information, a stronger requirement than in Europe or other laws in the region).[90]

A processor must not deny the provision of goods or services to a data subject who refuses to provide consent under A 22(2) or (3), or 'additional consent' under A 18(2) to allow additional uses or disclosures of personal information beyond what was consented to at the time of collection.[91] This does not cover A 22(1), only because A 16(2) already provides that there can be 'no denial' for refusal to provide more than the minimum information a processor is entitled to require.

Additional requirements for the method by which consent must be obtained under A 22(6), are provided by Enforcement Decree.[92] Though there is no explicit requirement that consent must be express, the better interpretation of the above provision, and of A 17(2) of the Enforcement Decree, is that it must be express. For example, it is difficult to see how the right 'to elect the scope of consent'[93] could be implemented as implied (opt-out) consent. This is different from some legislation in the region (e.g., Australia) allowing consent to be implied. Knowingly providing or receiving personal information without the required consent is an offence.[94]

Few enforcement examples under PIPA are known, though 2007 there have been reported cases concerning consent under the previous Act.[95] A complainant who stopped halfway through completing an online 'Marriage Club' enrolment form was entitled to object when the defendant company used the information she had provided to contact her (US$300).

5.4. *Processors and data controllers*

When a data controller consigns processing of personal information to another party, they must document or get an agreement concerning (i) prevention of use other than consigned purpose; (ii) technical and managerial safeguards; and (iii) other matters required by Enforcement Decree.[96] The data controller must inspect these matters as required by Enforcement Decree.[97]

Notice of the fact of processing to the data subject is also required,[98] and the processor must be identified. Alternatively, such notice of processing shall be posted on its website or at a publicly noticeable place for more than 30 days. This applies even if the 'processing' is marketing ('public relations') on behalf of the data controller.[99] It will also apply to any overseas processing. Korea is the only Asian jurisdiction that does require disclosure to a data subject that processing has been outsourced, whether locally or overseas.

Processors are deemed employees of the data controller,[100] who therefore has vicarious liability for their actions. However, the processor also has separate liability for any use of the personal information beyond the purpose of consignment or to disclose it,[101] and almost all other obligations of data controller[102] also apply to the processor. Korea is one of only four Asian jurisdictions (with Taiwan, Macau and the Philippines) in which processors are required to comply with all the requirements of the law.

5.5. *Sale of businesses*

The Act is very strict in relation to business transfers, and may be a disincentive to the sale of some information-based businesses if it is likely that existing customers would object to the transfer of their personal information to a new owner. Data subjects must be informed of the transfer of their personal information as the result of sale of a business in whole or part, and that they have a right to opt-out (withdraw consent) from their personal information being transferred[103], at which point it is (presumably) destroyed. This notice must be given by the previous owner prior to transfer,[104] but if it has not been given, it must be given by the new owner upon receipt of the personal information[105]. In any event, the purchaser can only use the personal information for the purpose for which it was held by the seller.[106]

5.6. *International data flows*

The data export restrictions in PIPA are not 'border based', in that they do not depend on what data privacy laws exist in the jurisdiction in which the data is received. Data exports (disclosures to 'a third party overseas') are subject to prior consent of data subjects, after discloser of all matters required by A 17(1), and processors must not make contracts to export data in violation of the Act.[107] In other words, consent first needs to be obtained. There is, however, no requirement to inform data subjects about the country of destination, and the state of its laws. This is a weakness in the Korean law, because it is difficult to see how data subjects can give informed consent if they have no idea to where their personal data is destined to be sent, or what privacy protections are provided there. Where consent is obtained (by using standard contractual clauses adopted in Korea), and overseas

[90] PIPA (Korea), art. 22(3).
[91] PIPA (Korea), art. 22(4).
[92] They are: (i) in writing, mail, facsimile with data subject's seal or signature, (ii) telephone recording, (iii) telephone notice and web-based consent confirmed by telephone, (iv) web-based consent, (v) e-mail confirmed by corresponding reply, and (vi) any other method similar to above methods.
[93] PIPA (Korea), art. 4(2).
[94] PIPA (Korea), art. 71(1).
[95] These examples are all from 'PIDMC cases: Noteworthy cases' (KoreanLII, trans. Whon-il Park, 2007-11) <http://koreanlii.or.kr/w/index.php/PIDMC_cases#Noteworthy_Cases>.
[96] PIPA (Korea), art. 26(1).
[97] PIPA (Korea), art. 26(4).
[98] PIPA (Korea), art. 26(2).
[99] PIPA (Korea), art. 26(3).
[100] PIPA (Korea), art. 26(6).
[101] PIPA (Korea), art. 26(5).
[102] PIPA (Korea), arts. 15–25, 27–31, 33–58 and 59.
[103] PIPA (Korea), art. 27(1).
[104] PIPA (Korea), art. 27(1).
[105] PIPA (Korea), art. 27(2).
[106] PIPA (Korea), art. 27(3).
[107] PIPA (Korea), art. 17(3).

disclosure made, the original data controller is not liable for any breaches of the Act by the recipient, even if no effective remedies are available in the overseas destination. There still may be liability under the Civil Code tort provisions. There is little consistency among Asian laws on data export issues, and the Korean reliance on consent is probably as strong as other Asian laws, though there is less evidence of its enforcement than there is, say, in Macau.

Overseas processors acting on behalf of the original collector will be considered to be a 'third party' for purposes of A 17(3), and so consent to overseas processing is required, not only notice (as required for a Korean processor). The Korean processor will also remain vicariously liable for any breaches by the overseas processor. In case of transfer of a database of clients or business itself to a third party overseas, a relevant notice and corresponding consent are required as if it is a Korean party.[108]

There are no explicit provisions dealing with extra-territorial application of the Korean law.[109] In Asia, explicit assertions of extra-territorial application are unusual in data privacy laws. In Taiwan, Malaysia and the Philippines there are extra-territorial provisions which aim to benefit only their own nationals, but in different ways in each case.

6. Security safeguards

6.1. *Security and data quality*

Detailed security measures ('technical, managerial and physical measures') are required, both locally and for data exports, with six types of measures prescribed,[110] including management plans, access controls, encryption, log-in records, upgrading of measure, and storage protections. The obligations are not in the OECD Guidelines form of 'take reasonable steps', but the stronger requirement of taking whatever is 'necessary to ensure' security.[111] There are likely to also be considerable obligations in relation to data transferred abroad: 'The government shall work out relevant policy measures so that the rights of data subjects may not be infringed upon owing to cross border transfer of personal information'.[112] These detailed provisions are more likely to be effective than only general statements, as found in some laws.

Under the previous Act, South Korea has been particularly pro-active in trying to get businesses to improve their data security, rather than sitting back and waiting for complaints. Security measures are reinforced by the new Enforcement Decree in which six types of required security measures spelled out.[113] These also apply to unique identifiers.[114] Further details of security measures will be established and notified by MOSPA. PIPA also imposes individual obligations on anyone processing personal information, prohibiting actions which 'damage, destroy, alter, forge or leak another's personal information'.[115]

Mediation cases reported by PIDMC from 2002 to 2007 under the previous Act include breaches of the requirements to take security measures, usually with compensation required for 'emotional damage': a social networking site allowed disclosure of a member's personal information due to errors in its search software (US$500); even the unexpected disclosure of a third party's personal data due to an error in website software was regarded as a breach deserving compensation to the person to whom the data was exposed (US$60). Since 2007, PIDMC mediated security complaints included a number of compensation payments because of inadequate security measures, including exposure on the Internet of extensive medical records of a patient, kept for research purposes, because of a medical institution taking (US$2000); and exposure of intimate communications on a social network site (US$500).

6.2. *Data breach notification*

Other than in Korea, only in the Philippines and Taiwan, are individuals likely to be affected required to be notified of data breaches, and only in China and the Philippines must the DPA or relevant Ministry be notified.

Large-scale data breaches have been a very significant issue in Korea for many years, culminating in a catastrophic breach at the start of 2014. Data breach notification to data subjects is mandatory,[116] including what was leaked, when and how, steps to take in mitigation, counter-measures being taken, and where to report damage. There must also be notification to MOSPA and to either KISA or the National Information Society Agency (NIA) if the breach is 'large scale' (affecting over 10,000 data subjects).[117] Details must be posted on websites for seven days.[118] Additional 'surcharges' of up to 500 million won (US$500,000) may be imposed by MOSPA where RR numbers have been lost, stolen, leaked, altered or damaged by a processor who has failed to take necessary security measures.[119] ICSPs will have additional obligations to notify the Korea Communications Commission (KCC) or KISA of any 'data leak or breach'.[120]

[108] Sung-Hey Park, 'South Korea's New Data Protection Act: Cross-Border Transfer Issues Examined In Relation To The Outsourcing Clause And The Relevant Regulatory Framework' (2011) 11 WDPR 6.
[109] Korean authorities have acted as if the Act had some extra-territorial effect. When investigating whether Google's Street View cars collected and stored personal data on unspecified Internet users from Wi-Fi networks in Korea, the Korean investigators summoned Google headquarters personnel to Seoul, without the basis of such action being clear.
[110] PIPA (Korea), arts. 29, 14(2) and PIPA Enforcement Decree, art. 30.
[111] PIPA (Korea), art. 29.
[112] PIPA (Korea), art. 14(2).
[113] PIPA Enforcement Decree, art. 30.
[114] PIPA Enforcement Decree, art. 21.
[115] PIPA (Korea), art. 59(3).
[116] PIPA (Korea), art. 34.
[117] PIPA (Korea), art 34(3) and PIPA Enforcement Decree, art. 39.
[118] PIPA Enforcement Decree, art. 40(3).
[119] PIPA (Korea), art 34-2, amended 6 August 2013 and effective 7 August 2014.
[120] K B Park 'New South Korean Amendments Include New Data Breach Notification Requirements, Expanded Data Protections', (2012) *BNA World Data Protection Report*, referring to 2012 changes to the ICN Act (arts. 27-3, 48-3).

An increasing number of victims go to court to claim for damages, but usually fail to get compensation owing to the difficulty to prove the causal relation between the data leakage and loss of property or mental distress.[121] Voice phishing has posed particular problems in Korea, and victims had great difficulty in recovering their funds, so a special law was enacted to facilitate this.[122]

7. Rights of the data subject

The rights of data subjects in relation to their personal information are first stated very generally: to be informed of processing; to consent to processing, including to 'elect the scope of consent' (ie unbundle consents); to confirm processing; to demand access' (including 'issuance of certificate'); to suspend processing; and 'to make correction, deletion and destruction'.[123] These rights are then expanded by specific provisions, discussed in the following.

7.1. Access and correction rights

The procedures for access include justifiable grounds to suspend or deny access to part or all of a record.[124] The content which can be accessed includes not only the content held, but the purpose of collection and use, the retention period, details of disclosures to third parties, and details of consents by the data subject.[125] Access must be provided within 10 days.[126] Access to public sector files can be via either the agency concerned or MOSPA.[127]

While access and correction rights are provided for in all Asian jurisdictions, requirements unique to Korea are that correction (and deletion) requests must also be decided within 10 days, and if denied the reasons (including information about how to appeal) must be provided in a standard Outcome Notice.[128]

7.2. Notification of data collection from third parties

On request from the data subject, notification is required of the details of data collection from third parties.[129] In practice, it is most likely to occur after the data subject has obtained access to his or her file. This notification must include that the data subject is entitled to demand suspension of the processing of that personal information. Identification of the source is also required except where (subject to the data subject's interests not being higher), there is a danger to the 'life or body' of another, or the 'property or profits of another', or a list of specified crime-related investigations. However, Korea does not require notification of corrections to be made to third parties who have had access to a person's file, unlike Hong Kong, Singapore, Macau Taiwan, and the Philippines.

7.3. Deletion rights and suspension of processing

A data subject may request deletion of any personal information except that collected under other laws and regulations.[130] Korea does have something close to the 'right to be forgotten'. In addition, automatic destruction of personal data is required after the purpose of processing is complete, or any other retention period completed.[131] Since retention periods must be specified at the time of collection, this will also provide another period that must be complied with. Suspension of processing can also be required by the data subject,[132] subject to limited exceptions.[133] Outcome Notices must be given for refusals of deletion or suspension. A right to block the use of data (but not to have it deleted) is found in Macau, Malaysia, the Philippines and Taiwan.

The deletion and suspension provisions indicate very clearly the extent of control over their personal information that individuals are given by the Korean law, not only in relation to content provided by the data subject, but also to data provided by third parties. A very informative PIDMC decision is one where the plaintiff had consented, when joining the defendant's online service, to his name, place of work, school he had graduated from and address being displayed on the defendant's website. He later decided that he wanted this information deleted, and the defendant denied this, saying the consent was irrevocable. The PIDMC upheld his request for deletion, referring not only to the equivalent to A 37 under the previous law, but also to the plaintiff's constitutional right to self-determination of his personal information (*Fingerprint Case*).[134]

[121] See the Korean Supreme Court decision discussed in Whon-il Park 'GS Caltex case' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/GS_Caltex_case> and Whon-il Park 'Compensation for data breach' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Compensation_for_data_breach>].

[122] To facilitate the recovery of damages incurred by the victims of phishing scams the Special Act on the Recovery of Financial Scam Damages via Electric Communications (Act No. 10477, effective 30 September 2011) provides for mandatory extinction of scam-related deposit claims and accelerated recovery of damages. Victims have only to report to the competent police station such phone phishing to stop the payment of scam-related bank deposits: See Whon-il Park 'Phishing' (KoreanLII, 2014) <http://koreanlii.or.kr/w/index.php/Phishing>.

[123] PIPA (Korea), art. 4.

[124] PIPA (Korea), art. 35 and PIPA Enforcement Decree, art. 42.

[125] PIPA Enforcement Decree, art. 41(1).

[126] PIPA Enforcement Decree, art. 41(3).

[127] PIPA (Korea), art. 35(2).

[128] PIPA (Korea), art. 36 and PIPA Enforcement Decree, art. 43.

[129] PIPA (Korea), art. 20.

[130] PIPA (Korea), art. 36(1).

[131] PIPA (Korea), art. 21 and PIPA Enforcement Decree, art. 16. For electronic files, this requires 'permanent erasure not to restore data.'

[132] PIPA(Korea), art. 37 and PIPA Enforcement Decree, art. 44.

[133] There are four exceptions: (i) to comply with other laws; (ii) where suspension is likely to cause damage to the life or body or benefits of others; (iii) where necessary for a public institution to carry out its legally required work; and (iv) where necessary to carry out a contract which the data subject has not explicitly terminated.

[134] PIDMC, 'Online service provider's failure of deletion of user's personal data on the Internet' (KoreanLII, trans. Whon-il Park) <http://koreanlii.or.kr/w/index.php/PIDMC_cases_in_2010> accessed 22 February 2014.

Other complaints mediated by PIDMC involving deletion rights or suspension of processing (with compensation noted) have included the following: failure to delete data, and to continue to use it for telemarketing after requests to cease (US$200); continued receipt of marketing messages after ceasing to use a service (US$200); and continued sending of spam despite claimant's express rejection of such messages (US$200 and education of staff required).

8. Conclusions – Asia's leader in data privacy innovation

South Korea's democracy, still less than a quarter-century old and with a continuing implementation of a 'post-authoritarian' legislative agenda, when coupled with the ubiquity of computing, the Internet and mobile telecommunications in Korean life, is underpinned by a constitution and a Constitutional Court responsive to privacy issues.

The Personal Information Protection Act of 2011 is consistent with this environment and is the most innovative data privacy law in Asia, although its enforcement has not yet fully proven itself. There are innovations in the enforcement aspects of PIPA, though they are not the subject of this article. They include Korea's long-standing innovation in mediation through PIDMC, now enhanced by collective meditation for disputes with widespread small damage; clear provisions for 'name and shame' publication; mandatory Privacy Impact Assessment (PIA) for potentially dangerous public sector systems; and extremely high financial penalties for misuse of RR numbers. PIPA includes almost every type of enforcement mechanism, with a wide range of degrees of application, so there is no impediment in theory to the law being well enforced. However, after two years of operation, there is little evidence of active enforcement beyond the well-established PIDMC mediations. The transparency of the Korean system, through various types of publication, is one of its stronger points,[135] but as yet there is not a lot of significant enforcement to be transparent about.

8.1. *The 10 most significant innovations in PIPA's principles*

PIPA's innovations apply with few exceptions to all private and public sector organisations in Korea, which increases their significance. However, PIPA does not extend the meaning of 'personal information' beyond its conventional meaning. Its innovations are found in the details of its privacy principles.

The most significant innovations in PIPA's privacy principles that have been detailed in this article, and are found in few if any other data privacy laws in Asia or anywhere else are as follows:

(i) mandatory Privacy Officers for most businesses and agencies;
(ii) a compulsory published privacy policy, the provisions of which over-ride any consents or contractual relationships between the data controller and the data subject;
(iii) the onus of proof of compliance with the legislation is placed on the data controller;
(iv) strong data minimisation through anonymous transactions requirements;
(v) the prohibition on 'denial of service';
(vi) the various requirements to 'unbundle' consents;
(vii) the opt-in required for marketing using a company's own databases;
(viii) mandatory data breach notification to both affected individuals and to authorities;
(ix) deletion of data on request; and
(x) prohibitions and penalties 'rolling back' uses of the RR number.

Some of these are innovations from a global perspective, not only in Asia.

8.2. *Comparisons with 'European' principles and inchoate European reforms*

Comparison of Korea's privacy principles with those that are distinctively 'European', in that they are required by the EU data protection Directive but not by the 1980 OECD privacy Guidelines (the 'minimum' standards,[136] shows that Korea implements four of those principles, as well as providing stronger levels of implementation of many of the 'minimum' principles). They are: Minimal collection; Deletion; Direct marketing limitations; and Sensitive data protections. It does not implement three others: Data export restrictions based on destination; Automated processing controls; or Prior checking. When combined with its strong enforcement provisions, a Korean application for an 'adequacy' assessment from the European Union, or to accede to the 'globalised' Council of Europe data protection Convention, would be a credible application, although positive decisions on such matters should never be taken for granted.

The European Union has, since 2011, been considering proposals from the Commission to reform the data protection Directive, possibly by replacing it with a Regulation. It is possible the process will be completed during 2014. At various time numerous possible enhancements to the principles in a Regulation have been identified, including in one thorough analysis, though not the most recent, the following[137]: more explicit consent (opt-in) requirements, and obligations to prove same; more explicit requirements of data minimisation at collection; a 'right to be forgotten', possibly including obligations on intermediaries to inform third parties; a right to data portability, including to obtain a copy of personal data in a portable format; regulation of automated 'profiling';

[135] Greenleaf *Asian Data Privacy Laws*, Chapter 5.

[136] Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108'.

[137] *This summary is derived substantially from an early analysis in February 2012, by Christopher Kuner* 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', (2012) *Bloomberg BNA Privacy and Security Law Report*, February 6 2012, pgs. 1–15, <http://ssrn.com/abstract=2162781> accessed 14 January 2014.

demonstrable implementation of privacy principles (stronger 'accountability'); implementation 'by design'; implementation 'by default'; liability of local European representatives of a processor; mandatory data breach notification; Data Protection Officers required; more specific requirements in relation to data exports; EU rules to apply to extra-territorial offering of goods, services or monitoring; and a right to online subject access. These reforms are broader than in Korea's Act, but many may end up 'on the cutting room floor' before a Regulation emerges, whereas quite a few (and some others) have already been enacted in Korea.

The changes proposed to the principles in Council of Europe data protection Convention 108 through its 'modernisation' process[138] are less extensive than are proposed in relation to the EU Regulation. They include expanded categories of sensitive data, data breach notification requirements, and rights concerning automated processing. Korea's reforms are already broader.

8.3. *Stronger provisions are continuous*

At the start of 2014 a massive data breach in South Korea involved 104 million data items being stolen from three credit card companies, including RR numbers and sufficient information for current credit cards to be used.[139] Collective court actions against the companies are threatened and top company officials have announced their intention to resign, and the seller and buyers of data have been indicted. The government has announced proposed further law reforms, including: punitive surcharges of up to 5 billion won (US$4.6 million) on companies causing or exploiting leakage of personal data, plus a 1% surcharge on resulting transactions; a prohibition on sharing of personal information between affiliated companies without consent; and additional authentication required of SMS funds transfers. All telemarketing was also suspended for two months to reduce fraud possibilities, causing lay-offs of thousands of telemarketers, and US insurers arguing that this was in breach of the US–Korea Free Trade Agreement. Parliamentary hearings on strengthening data protection laws will also be held in a pre-election climate.

PIPA has already been amended in March 2014 to require encryption of all RR numbers held (effective 1 January 2016). The ICN Act was also amended in May 2014 to increase the statutory damages resulting from data spills to 3 million won per person (US$3000). It also now provides that the surcharges (fines) on ICSPs negligent in protecting personal data will increase from a maximum of 100 million won (US$100,000) to a maximum of 3% of sales related to personal data.[140]

South Korea's highly interconnected and technological society is likely to continue to indicate the direction that Asian data protection laws will take. It is the 'canary in the coalmine' where problems, and solutions, happen first.

Acknowledgements

This article is based in part on Graham Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, forthcoming, 2014), Chapters 4 and 17. We wish to thank the two reviewers of this article for their helpful comments, and also other colleagues in Korea who have provided assistance and comments on previous drafts. Graham Greenleaf wishes to thank Kyung Hee University, Seoul for a number of research fellowships from 2009 to 2012 in Korea.

[138] For a full discussion see Graham Greenleaf, 'A world data privacy treaty?: 'Globalisation' and 'Modernisation' of Council of Europe Convention 108' (Witzleb, Lindsay, Paterson and Rodrick (Eds) *Emerging Challenges in Privacy Law: Comparative Perspectives* Cambridge University Press, forthcoming 2014). Alternatively, see *Graham* Greenleaf, G ''Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29(4) *Computer Law & Security Review*.

[139] For details on all of this section, see Whon-il Park 'South Korea's major financial institutions suffer data breach', (2014) 127 Privacy Laws & Business International Report, pgs. 6–7.

[140] ICN Act, (Korea), art. 64-3(1), enacted May 2013. Expected to be in force no earlier than late 2014.