

Korea's proposed overhaul of its data protection laws

Kwang Bae Park et al.



Korea's proposed overhaul of its data protection laws

New Bills are designed with the GDPR in mind. By **Kwang Bae Park, Hwan Kyoung Ko, Sung Hee Chae and Minchae Kang** of Lee & Ko Attorneys, Seoul.

In recent years, the need for balance between the utilization versus protection of personal information has been a hot topic among industry professionals and experts in Korea. On 15 November 2018, a number of bills amending four of Korea's major data protection and privacy laws were introduced in the National Assembly, and each of the Bills aims to achieve such a balance while encouraging the active use of big data and other data-based applications by businesses. The four laws for which the Bills were introduced are: 1. the Personal Information Protection Act (PIPA), 2. Act on Promotion of Information and Communications Network Utilization and Information Protection (Network Act), 3. Act on the Protection and Use of Location Information (Location Information Act), and 4. Credit Information Use and Protection Act (CIUPA – Credit Information Act).

PURPOSE OF THE BILLS

The Bills reflect the results of the Regulatory and Institutional Reform Hackathon that was held by the Presidential Committee on the Fourth Industrial Revolution in early 2018. Specifically, the Bills clarify the definition of "personal information" by introducing the concepts of pseudonymized data and anonymized data, and also set forth the detailed scope for which pseudonymized data may be used. Under the Bills, the Ministry of Interior and Safety (MOIS) and the Korea Communications Commission (KCC) are, in principle, no longer in charge of handling matters related to the protection of personal information, as that responsibility is transferred to the Personal Information Protection Committee (PIPC). Also, by integrating the Network Act's personal information-related provisions as special provisions in the PIPA, the Bills aim to achieve consistency in the application of

Korea's various data protection and privacy laws. In addition, the Bills allow for the combination of data sets, which is likely to make it easier for data handlers to utilize personal credit information in their possession. Meanwhile, under the influence of the European Union's General Data Protection Regulation (GDPR), the Bill for the Credit Information Act introduces new types of rights to be exercised by data subjects, such as the right to request the transmission of one's personal credit information (which is similar to the right of data portability) and the right to control automated individual decision-making.

Until now, Korea's data protection regime has been heavily focused on protecting data, which has meant that the effective use of data was limited, due to the tight restrictions placed on their use. As such, Korea's data protection regulations were known as some of the most stringent in the world. However, this is likely to change to some extent, now that the Bills have been introduced into the National Assembly. They are designed with the GDPR and other countries' current data protection regulations in mind. The Bills also strive to strike a balance between the protection of data and its active use.

While the Bills have yet to be passed by a plenary session of the National Assembly, there is a high likelihood that they will be passed eventually (even if some changes are made to their current drafts), since it has been reported that the Bills reflect the mutual discussions between the ruling party and the Korean Government over the past several months. However, a number of civil societies have apparently requested that additional changes be made to the current drafts of the Bills in order to strengthen their data protection aspects. Regardless, once the Bills are adopted, they are expected to bring

about the most wide-sweeping changes across Korea's data industry since the PIPA was first implemented.

KEY PROVISIONS OF THE PIPA BILL

1. Secure data processing to not identify individuals: Personal information is divided into three categories: personal information, pseudonymized data and anonymized data. Pseudonymized data, which is personal information that has been processed/ pseudonymized such that it cannot be used to identify a specific individual without the use or combination with other information, may be used to compile statistics, carry out scientific research, or preserve public records without the data subject's consent. Yet, even in such cases, combining the data sets of two or more data handlers must be done through a professional institution (i.e., a third party institution qualified under the PIPA) and requires the approval of the professional institution before the combined data set may be exported to a third party.

Data handlers are required to implement certain statutorily-prescribed security measures when processing pseudonymized data or combining two or more different data sets. Data handlers cannot engage in any act that will allow a specific individual to be identified from the pseudonymized data or combined data sets, and failure to do so may result in criminal sanctions or a penalty surcharge.

2. Reform of related data protection laws and supervisory authorities: Personal information-related provisions have been deleted from the Network Act, and instead special provisions regarding (i) safeguards to be implemented for the cross-border transfer of personal information, (ii) restrictions on the onward transfer of personal information, (iii) the designation of a local representative, and (iv) purchase of insurance for

damage compensation have been added to the PIPA. The Bills for the Network Act, Location Information Act, and Credit Information Acts are subject to the (adoption of the) PIPA Bill.

The PIPC is promoted to a central administrative agency that has the independent authority to handle matters relating to the processing of personal information under the PIPA, and all functions of the MOIS under the PIPA and the KCC under the Network Act related to personal information matters are transferred to the PIPC. The powers that are granted to the PIPC include the authority to investigate alleged violations of applicable data protection and privacy laws, and impose a penalty surcharge and/or administrative fine on violators. Also, the KCC and PIPC will jointly enforce the Location Information Act.

KEY PROVISIONS OF THE CREDIT INFORMATION ACT

1. Use and protection of data in the financial sector: By introducing the concept of pseudonymized data and professional data institutions, a legal basis for analyzing, using, and combining data in the financial sector will be established.

All credit information companies, credit information collection agencies and credit information providers/users (collectively, Credit Information Companies) are required to implement a security plan to ensure the safe processing of pseudonymized data. If the pseudonymized data is used to re-identify a specific individual for commercial or illegal purposes, the Credit Information Companies will be subject to criminal sanctions and/or a penalty surcharge.

2. Reforms to promote competition

in the financial information industry: The current version of the CIUPA defines “credit inquiry service” rather broadly. The CIUPA Bill breaks down the credit inquiry service into subcategories based on the nature of the service, such as the “personal credit evaluation service,” “sole proprietorship credit evaluation service,” and “corporation credit inquiry service,” while adding new types of services (i.e., “professional individual credit evaluation service” and “self-credit information management service (MyData)”) that use non-financial data to evaluate an individual’s credit rating.

Credit bureaus are no longer prohibited from performing any other commercial business at the same time as a credit information business, and are allowed to concurrently carry out a commercial business that is not at risk of harming a credit information subject or the sound practices of credit transactions.

Changes are made to the regulations on the ownership structure of financial information companies and business activities that Credit Information Companies are allowed to engage in. More roles are also assigned to credit information collection agencies.

3. Protection of credit information subjects: A rating system is introduced for consent forms, such that different ratings will be assigned to consent forms depending on the risk(s) and benefit(s) associated with giving consent. Influenced by the GDPR’s concepts of a data subject’s right to data portability and automated individual decision-making, new types of rights such as the right to request the transmission of one’s personal credit information and right to control

automated individual decision-making have been introduced.

A regular review system is introduced in order for the Financial Services Commission to monitor the use and management of personal credit information by financial institutions.

CONCLUSION

The Bills are known to be the product of more than several months of extended discussions between various interested parties across the private sector, civil society, academia, legal sector, and industrial circles. In light of the Bills, the adequacy assessment under the GDPR that the Korean Government has been pursuing in consultation with the EU Commission is likely to continue on the basis of the PIPA instead of the Network Act. Companies that process large volumes of personal information in the course of their business are advised to closely monitor the final drafts of the Bills, and make the necessary preparations to their practices in light of the changes that are expected to occur once the Bills are adopted into law.

AUTHORS

Kwang Bae Park, Hwan Kyoung Ko, Sung Hee Chae and Minchae Kang are lawyers at Lee & Ko Attorneys, Seoul. Email: kwangbae.park@leeko.com

Windows 10 breaches Dutch DP law

The Netherlands’ Data Protection Authority has ruled that Microsoft breaches Dutch data protection law by processing personal data of people that use the Windows 10 operating system on their computers. Dutch Data Protection Authority ran an investigation of Windows 10 Home and Pro, and found that Microsoft does not clearly inform users about

the type of data it uses, and for which purpose.

Also, people cannot provide valid consent for the processing of their personal data, the DPA says. “The company does not clearly inform users that it continuously collects personal data about the usage of apps and web surfing behaviour through its web browser Edge, when the default

settings are used. Microsoft has indicated that it wants to end all violations. If this is not the case, the Dutch DPA can decide to impose a sanction on Microsoft,” the DPA says.

• See <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10>



ESTABLISHED
1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Spain adopts GDPR implementing law

The new law entered into force on 7 December.

Rafael García del Poyo of Osborne Clarke reports from Spain.

Spain's Senate approved, on 21 November, the law that complements the GDPR, and the text of the law was published in the Official Gazette on 6 December¹. The adoption of the law was delayed because, among other reasons, Spain's legislature took the opportunity to add provisions that guarantee

citizens' "digital rights".

In general terms, the law closely follows the GDPR. But as the national law must avoid derogations or overlaps with the GDPR, subsequent interpretation will be made by Spain's DPA, as it is in their practical

Continued on p.3

How Ireland's DP Commission will exercise its powers

This will be a long process as many multinational cases need to go through the EDPB cooperation and consistency mechanism.

By **Helen Dixon**, Ireland's Data Protection Commissioner.¹

The GDPR has undoubtedly given rise to considerable additional work specific to EU Data Protection Authorities due to new obligations. Ireland's Data Protection Commission (DPC) has

had to introduce a new classification system internally to deal with cases that pertain to cross-border processing entities in order to ensure the cases are appropriately recorded on

Continued on p.5

Issue 156 **December 2018**

NEWS

- 1 - Spain adopts GDPR implementing law
- 1 - How Ireland's DP Commission will exercise its powers
- 2 - Comment
GDPR still not in force everywhere
- 8 - Q&A with Helen Dixon
- 16 - Norway's DPA and Consumer Council support each other
- 20 - Uruguay moves towards the EU GDPR standard
- 26 - DPAs: Ethics comes before, during and after law

ANALYSIS

- 9 - Japan and Korea: Different paths to EU adequacy
- 18 - Cathay's data breach catastrophe goes beyond Hong Kong
- 19 - The GDPR's extra-territorial effect is felt in Hong Kong
- 22 - Asia-Pacific free-trade deals clash with GDPR and Convention 108

MANAGEMENT

- 25 - The role of legal protection insurance

LEGISLATION

- 12 - Korea's proposed overhaul of its data protection laws
- 14 - Finland's new Data Protection Act enters into force on 1 January

NEWS IN BRIEF

- 4 - EDPB issues guidelines on territoriality of the GDPR
- 13 - Windows 10 breaches Dutch law
- 15 - Facebook fined €10m
- 20 - Ethics research issued in HK
- 21 - EU Standard Contractual Clauses case imminent in Ireland
- 27 - EDPB under pressure to produce more GDPR guidance

www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Materials from PL&B events
- Special Reports
- Videos and audio recordings

See the back page or **www.privacylaws.com/subscription_info**

To check your type of subscription, contact
kan@privacylaws.com or telephone +44 (0)20 8868 9200.

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL
report

ISSUE NO 156

DECEMBER 2018

PUBLISHER**Stewart H Dresner**

stewart.dresner@privacylaws.com

EDITOR**Laura Linkomies**

laura.linkomies@privacylaws.com

DEPUTY EDITOR**Tom Cooper**

tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR**Professor Graham Greenleaf**

graham@austlii.edu.au

REPORT SUBSCRIPTIONS**K'an Thomas**

kan@privacylaws.com

CONTRIBUTORS**Ana Brian Nougères**

Estudio Jurídico BrianN and Associates, Uruguay

Rafael Garcia del Poyo

Osborne Clarke, Spain

**Jukka Lång, Tuomas Haavikko and
Kaisa Päivinen**

Dittmar & Indrenius Attorneys Ltd, Finland

Kwang Bae Park, Hwan Kyoung Ko,**Sung Hee Chae and Minchae Kang**

Lee & Ko Attorneys, South Korea

Helen Dixon

Data Protection Commission, Ireland

Allan Chiang

Hong Kong

Merrill Dresner

PL&B Correspondent

Published byPrivacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Fax: +44 (0)20 8868 5215****Email: info@privacylaws.com****Website: www.privacylaws.com****Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753

Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2018 Privacy Laws & Business

comment

GDPR still not in force everywhere

The GDPR adaptation laws were delayed both in Finland (p.14) and Spain (p.1) due to national legislative traditions, and ambitions to add extra provisions on digital rights. In Spain, the new law is now in force and Finland's law will follow on 1 January 2019. But there are still some EU Member States that have not yet managed to bring the GDPR's provisions into national law, for example Greece, Portugal and the Czech Republic.

The European Data Protection Board (EDPB) will now increase its work rate by meeting every month for three days and is trying to achieve consistency in GDPR implementation. The Board is now dealing with cross-border cases. Much pressure has landed on Ireland, and the Data Protection Commissioner, Helen Dixon, says that many complaints and cases on systemic issues about tech companies do not need to be led by her office alone, as they apply equally across the EU (p.1). She promises fines, but not yet – the correct procedures takes time.

The EDPB has issued opinions on national lists for Data Protection Impact Assessments. In December it evaluated the European Commission's adequacy opinion on Japan. Japan's adequacy decision is close but not there yet. Korea has decided to amend its laws to facilitate its entry to the club of adequate countries (p.9). Another regional development is the new Asia-Pacific free trade agreements that include strict limits on how legislation can restrict personal data exports or require data localisation (p.22).

In October, Stewart Dresner and I attended the Data Protection Commissioners' International Conference in Brussels. DPAs spent a few days discussing the importance of data ethics (p.26). A valuable message was heard and reported also by national media, at least in the UK, but my impression was that the real work took place behind closed doors and at 31 side events on one afternoon and more on another. We organised a very well attended event on the potential for collective action under the GDPR and will be returning to this theme both on these pages and at our future events.

Laura Linkomies, Editor

PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality

Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service

Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

Subscription Fees

Single User Access

International Reports £560 + VAT*

UK Reports £450 + VAT*

UK & International Reports £900 + VAT*

* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition

Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions

Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.

www.privacylaws.com/UK