Korea amends Personal Information Protection Act

Kwang Bae Park, **Hwan Kyoung Ko** and **Sunghee Chae** of Lee & Ko in South Korea
explain the changes to the three main privacy laws in Korea and what they mean for business.

On 9 January 2020, amendments to Korea's three major data privacy laws (Three Data Laws), i.e., Personal Information Protection Act (PIPA), Act on the Promotion of Information and Communications Network Utilization and Information Protection (Network Act), and Credit Information Use and Protection Act (Credit Information Act), were passed at a plenary session of the National Assembly of Korea. These three amendments bills were promulgated on 4 February and will enter into force on 5 August 2020.

We live in an era of the data-driven economy where the use of new technologies such as artificial intelligence (AI), cloud services, and Internet of Things (IOT) has become a necessity in order to process increasingly larger amounts of data and develop new businesses in the IT sector. In line with the legislative trends in other major parts of the world, there has long been a push in Korea towards amending the Three Data Laws to ensure the secure use of personal information while still paving the way for the more efficient processing of big data. The revisions to the Three Data Laws are the culmination of such efforts.

> These three amendments bills were promulgated on 4 February and will enter into force on 5 August 2020.

The amendments to the PIPA that have been adopted include, among others:

1. Clarification of the definition of "personal information;"
2. The introduction of pseudonymized information and the permitted use of pseudonymized information for research and statistical purposes without the data subject's consent;
3. The introduction of compatibility;
4. The transfer of the Network Act's personal information-related provisions to the PIPA; and
5. The elevation of the Personal Information Protection Commission's (PIPC's) status to a central administrative agency responsible for the enforcement of the PIPA.

Given the importance of the newly amended PIPA and its potential implications on data-reliant industries regulated by the PIPA, we have summarized below the key changes to the law.

Key Provisions of the Amended PIPA

Clarification of the definition of "personal information" (Article 2(1)): As is the case under the current PIPA, the definition of "personal information" under the amended PIPA continues to include "information that can be easily combined with any other information to identify a specific individual." The amended PIPA provides clearer direction on what this means, by stipulating the criteria for determining whether certain information can be "easily combined with any other information to identify a specific individual." The specific criteria set forth in the amended PIPA is that one must give "reasonable consideration to factors such as time, cost, and technology required for identifying an individual, including the likelihood of obtaining additional information to be combined with the subject information." The above criteria are intended to prevent the definition of personal information from being interpreted too broadly under the PIPA.

Introduction of "pseudonymized information" (Article 2(1)(c), 2(1-2), 2(1-8) and Chapter 3): The amended PIPA introduces the concept of "pseudonymized information," which means "information which, through the process of pseudonymization, may no longer be used to identify a specific individual without using or combining additional information to restore the information to its original state." Here, "pseudonymization" means the process of fully or partially deleting or replacing personal information or employing other similar methods such that the personal information can no longer be attributed to a specific individual without additional information.

The initial draft amendment of the PIPA provided that the specific methods of pseudonymization would be set forth in the relevant Presidential Decree. However, the final version of the amendment which passed the National Assembly stipulates the principles governing the pseudonymization methods in the PIPA itself, rather than delegating the authority to the President to determine such methods in the Presidential Decree. Therefore, data handlers are advised to continue monitoring the position of the pertinent regulators, including any guidelines to be issued by them, and see how the principles stipulated in the amended PIPA are applied in practice going forward.

Under the amended PIPA, data handlers may process pseudonymized information without the consent of the data subject for purposes including statistical compiling, scientific research, and record preservation for the public interest. Moreover, the PIPA's provisions regarding the destruction of personal information and the data subject's right to request access, or the correction/deletion of personal information, do not apply to pseudonymized information. As stated in the reasons for the proposed amendment to the PIPA, "scientific research" purposes include

"commercial purposes such as the development of data-based, innovative technology, products, and services." The wider scope of purposes for which personal information may, after being pseudonymized, be used and provided to third parties under the amended PIPA is in line with the demands of the current data economy.

Meanwhile, the amended PIPA regulates the combining of pseudonymized information managed by different data handlers by stipulating that only professional institutions designated by the PIPC or by the head of a pertinent central administrative agency may combine such pseudonymized information. Also, the combined information may only be exported outside of the professional institution after obtaining the approval of the head of the said institution.

Furthermore, the amended PIPA requires that anyone who processes pseudonymized information must implement the statutorily-prescribed security measures. Processing pseudonymized information for the purpose of identifying a specific individual is also prohibited under the amended PIPA. Anyone who violates this prohibition may be subject to a penalty surcharge of 3% or less of their total revenue, and imprisonment of up to five years or a fine of up to 50 million South Korean Won (KRW).

Use of personal information within the scope reasonably related to the original purpose of the collection (Article 15(3), Article 17(4)): The amended PIPA allows data handlers to use or provide personal information within the scope reasonably related to the original purpose of the collection without the consent of the data subject in accordance with the Presidential Decree to be promulgated, after considering, for example, whether such use or provision may result in any disadvantage to the data subject and/or whether the data handler has implemented the necessary safeguards to ensure the security of the personal information, e.g., encryption. By doing so, the amended PIPA has relaxed the existing consent-oriented regulations which have been subject to continued criticism for being excessively formalistic and stringent, and adopted the purpose limitation principle of the GDPR, which allows the use of personal information for purposes that are not incompatible with the purpose of initial collection. The specific details regarding the method of using and providing personal information for the purposes as described above will be set forth in the Presidential Decree, so it is important to continue monitoring any amendments to be made to the Presidential Decree.

Exclusion of anonymized information from the application of the PIPA (Article 58(2)): The amended PIPA explicitly provides that any information which cannot be used to identify a specific individual even if the information is combined with any other information, after reasonably considering factors such as time, cost, technology ("Anonymized Information"), is not subject to the provisions of the PIPA.

Under the current PIPA, Anonymized Information is already considered as non-personal information which is not subject to the PIPA. However, to avoid any dispute over potential grey areas, the amended PIPA explicitly states that Anonymized Information is excluded from the application of the PIPA.

Transfer of the Network Act's personal information-related provisions to the PIPA (Chapter 6): The amended PIPA includes a new chapter on the "Special Provisions for the Processing of Personal Information by Information and Communications Service Providers and Recipients of Personal Information Provided by Information and Communications Service Providers (collectively, the ICSPs)" (Special Provisions), which basically consists of the Network Act's provisions relating to personal information protection that are not in harmony with those set forth in the PIPA. Examples of such provisions include those on the collection and use of personal information, notification and report of personal information leakages, destruction of personal information of inactive users, notification of personal information usage details/records, damage compensation guarantees, designation of a domestic representative, protection of personal information transferred abroad, and penalty surcharges.

Consent no longer required for an ICSP's outsourcing of data processing to a third party: Under Article 25 of the current Network Act, an ICSP who wishes to outsource the processing of personal information to a third party (Outsourcing) is obliged, in principle, to obtain the data subject's (i.e., user's) consent. However, this provision was not transferred to the amended PIPA as part of the Special Provisions, and thus the PIPA's provisions on Outsourcing will now apply to an ICSP who wishes to engage in Outsourcing.

Under the current PIPA, the data subject's consent is not required for Outsourcing. However, because the Network Act included such a consent requirement, ICSPs were required to obtain separate consent to not just the collection/use of personal information and provision of personal information to a third party, but also Outsourcing. Due to this additional consent requirement, Article 25 of the Network Act was often mentioned as one of the main reasons that IT service providers were prevented from more actively utilizing cloud services, which is generally how most IT service providers process data of their customers.

The Initial PIPA Bill included Article 25 of the Network Act as one of the Special Provisions to be transferred to the PIPA. Yet, the idea of transferring Article 25 to the PIPA was discarded during the bill review process after several legal and industry experts pointed out the problems with doing so, and data handlers/ICSPs also criticized the possible implications.

Streamlining of Korea's data protection regulatory authorities (Article 7, 7-14): The PIPC will be elevated to a central administrative agency reporting to the Prime Minister, and will also become the supervisory authority for data breaches (including the misuse/abuse of personal information and leakages). Personal information protection matters that are currently handled by multiple agencies (i.e., Ministry of Public Administration and Security, Korea Communications Commission) will all be handled by the PIPC instead. In order to ensure the independence of the PIPC, Article 18 of the Government Organization Act — which stipulates the Prime Minister's authority to direct and supervise

the heads of central administrative agencies under orders from the President, and revoke or suspend any administrative orders issued by the head of a central administrative agency if they are deemed unlawful or unjust — will not apply to certain tasks performed by the PIPC.

Network Act: Deletion of personal data provisions

As explained above, in order to achieve harmonization among the Three Data Laws, the personal information-related provisions of the Network Act have been transferred to the PIPA, and thus the said provisions (i.e., Chapter 4 (Protection of Personal Information)) have been deleted from the Network Act.

Credit Information Act and Act on the Protection and Use of Location Information

The amendment to the Credit Information Act was also passed by the National Assembly's plenary session on 9 January 2020, the same date that the amendments to the PIPA and Network Act were passed. Among the changes that were adopted, certain provisions of the Credit Information Act that overlapped with the PIPA were revamped so that the relevant provisions of the PIPA would apply instead, and some provisions were revised to clarify the Credit Information Act's relationship with the PIPA. As such, in order to determine whether the amended PIPA (and not the Credit Information Act) will apply to the processing of an individual's personal credit information, concerned businesses and companies should review the PIPA's new changes in detail. The amended Credit Information Act stipulates that the PIPC has the authority to supervise personal credit information that is processed by a business operator and not a financial institution, while the Financial Services Commission has supervisory authority over personal credit information processed by financial institutions.

The draft amendment for the Act on the Protection and Use of Location Information (Location Information Act) — which was also proposed to the National Assembly on November 15, 2018 along with the draft amendments of the PIPA and Network Act — includes a provision that would transfer the KCC's authority to enforce/oversee matters relating to the protection of personal location information (which qualifies as personal information) to the PIPC, and have the KCC and PIPC be jointly responsible for enforcing the Location Information Act. The National Assembly's review of the Location Information Act's amendment bill has been postponed due to the need to further discuss and clarify the respective scope of tasks to be performed by each of the two authorities. As such, it would be helpful to keep an eye on whether the bill is eventually passed.

The new PIPA is meaningful in that it provides clearer guidance to data handlers on what constitutes the lawful processing of personal information, and also sets forth the standards for the secure processing of personal information. Yet, since the amended PIPA also imposes additional obligations on data handlers and provides for heavier sanctions (e.g., introduction of a penalty surcharge) in the case of a violation, the recent changes should not be taken lightly.

The amended PIPA is expected to go into effect six months from its promulgation date, and the amendment of the PIPA's implementing regulations and related public notices are also expected to take place in the upcoming months. Therefore, we recommend that anyone who is likely to be affected by the new PIPA review the changes carefully and continue to monitor any related legislative developments.

AUTHORS

Kwang Bae Park, Hwan Kyoung Ko and Sunghee Chae are Partners at law firm Lee & Ko in South Korea.
Emails: kwangbae.park@leeko.com
hwankyoung.ko@leeko.com
sunghee.chae@leeko.com

ADEQUACY ISSUES FOLLOWING KOREA'S REFORMS

Korea's January 2020 reforms to its three main data privacy laws are outlined in the above article. This note makes brief observations on the possible significance of those reforms for the assessment under the GDPR. Art. 45 of the adequacy of Korea's data protections by the European Commission (EC).

The transfer of the Network Act's personal information related provisions to the Personal Information Protection Act (PIPA) (Park, 1(5)), coupled with the transfer of enforcement powers from the Ministry of Public Administration and Security (MOPAS), and the Korean Communications Commission (KCC), to the Personal Information Protection Commission (PIPC), and the provisions exempting the PIPC from Prime Ministerial and Presidential directions (Park, 1(7)), may mean that the PIPC will now satisfy the EC's requirements for an independent supervisory authority, including independence in control of enforcement actions. The transfer of KCC's previous regulation of ICSPs (Information and Communications Service Providers) to PIPC also means that PIPC regulates a sufficiently comprehensive part of Korea's private sector to make an adequacy finding worthwhile for both sides.

Other aspects of the Korean reforms may raise issues which the EC will need to address because those provisions are different from their GDPR equivalents. The Korean use of 'easily combined' makes the definition of 'personal information' narrower than in the GDPR (Park, 1(1)). Whether the Korean allowed non-consensual uses of 'pseudonymized information' for commercial purposes, the inclusion without conditions of 'sensitive' information, its provision to third parties, and its combining, can be done under a 'presumption of compatibility' for archival, research and statistical uses similar to that in the GDPR art. 5(2) (Park, 1(2)) are all issues as well. Even the Korean use of 'etc' in describing the scope of this compatibility is questionable. It is not useful to speculate to what extent the differences between the Korean provisions and the GDPR will be regarded as significant for the question of adequacy. Neither the EC's adequacy decision concerning Japan, nor the EDPB's opinions, give useful guidance.

Graham Greenleaf, Professor of Law & Information Technology, UNSW Australia

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

New GDPR law for Greece

Spyridon Vlachopoulos and **Vassiliki Christou** from the University of Athens explain new aspects and limitations of this law.

Greece's law implementing the GDPR, Law 4624/2019 (the Greek Law), entered into force on 29 August 2019. The new Greek Law is composed of three parts. The first part provides that the Greek Data Protection Authority (DPA), responsible for the enforcement of data protection law, including the GDPR, is the DPA already established under the previous data protection law 2472/1997, and sets out its new competences. The second part contains measures implementing the GDPR. The third part transfers into Greek legal order Directive 2016/680/EU[1]. In this article, we shall focus primarily on the second

Continued on p.3

India's data privacy Bill: Progressive principles, uncertain enforceability

The new Bill includes several notable changes from the previous version and should be followed closely not least due to the government's EU adequacy aspirations, says **Graham Greenleaf**.

India's Modi government has at long last submitted the Personal Data Protection Bill, 2019[1] to India's lower house, the *Lok Sabha*. The government Bill is based on the draft Bill (and Report[2]) prepared by the committee chaired by former Supreme Court Justice Srikrishna,

Continued on p.6

Future PL&B Events

- *Germany's data protection law: Trends, opportunities and conflicts,* 11 March 2020, Covington & Burling, London. **Speakers** include Alexander Filip, Bavarian DPA, and Covington partners from Germany & the UK. **Sessions** include: International transfers; Privacy and labour law; and Enforcement trends. www.privacylaws.com/germany
- *PL&B's 33rd Annual International Conference* St. John's College, Cambridge 29 June to 1 July 2020. www.privacylaws.com/ac (p.31)

privacylaws.com

Issue 163 **FEBRUARY 2020**

INTERNATIONAL report

ISSUE NO 163 **FEBRUARY 2020**

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
Gonzalo F. Gallego
Hogan Lovells LLP, Spain
Spyridon Vlachopoulos and Vassiliki Christou
University of Athens, Greece
Eleonora Maria Mazzoli
London School of Economics and Political Science, UK
Bertil Cottier
University of Lugano, Switzerland
Kwang Bae Park, Hwan Kyoung Ko and Sunghee Chae
Lee & Ko, South Korea
Letícia Silveira Tavares
HewardMills, UK
Helena Wootton
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
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

comment

Korea amends its privacy laws; Greece adopts GDPR law

On 9 January 2020, South Korea's national assembly adopted amendments to its major data privacy laws. This development is interesting in view of Korea's ambitions to be assessed as EU-adequate (p.21). The same scenario applies to India (p.1) although its Bill is at the start of its legislative stages.

Greece's GDPR implementation has lagged behind other EU Member States but we are pleased to publish now a full report on the specifics of this new law (p.1). Some commentators say, however, that the law was rushed through, and there are some shortcomings in the text.

The EU Commission is already looking at whether certain aspects of the GDPR should be updated (p.10) as the development of new technologies, especially AI, poses new challenges on whether it is possible to apply the regulation in this context (p.14). Our Biometric Identification Roundtable is putting recommendations and questions to the UK regulator on the UK Information Commissioner's position regarding achieving a balance between data minimisation and Artificial Intelligence's need for a vast amount of data. Can minimisation, necessity, accuracy, security and ethics be reconciled with these technological developments? (p.29). More on AI and facial recognition on p.27. As the EU debates the route to take, our correspondent analyses existing regulation. The EU white paper on AI was adopted on 19 February just as we were going to print[1].

Facebook is developing an Oversight Board – how will it work and what will be its relevance? Read a report on this topic on p.18 which raises the question of applying good governance principles to such a large and powerful enterprise.

The much-awaited Court of Justice of the European Union Advocate General's Opinion on Schrems II and Standard Contractual Clauses (SCCs) was issued last December. Despite positive messages, SCCs applicability is still limited on a practical level, our correspondent says (p.11). We await the final decision, expected in the first quarter of 2020.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1. ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

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

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

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

Stay informed of data protection legislative developments in 165+ 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 administrative 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 and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
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.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

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

privacylaws.com/reports

"*PL&B Reports* are an invaluable resource to anyone working in the data privacy, e-commerce or digital marketing fields. Unlike many news feeds or updater services, each Report provides rare depth of commentary and insight into the latest developments."

Rafi Azim-Khan, Partner, IP/IT & Head Data Privacy, Europe, Pillsbury Winthrop Shaw Pittman LLP

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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