Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction 5
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 9
Aaron P Simpson, Claire François and James Henderson
Hunton Andrews Kurth LLP

The Privacy Shield 12
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 17
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 25
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 33
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 45
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 53
Doug Tait and Catherine Hamilton
Thompson Dorfman Sweatman LLP

Chile 60
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 67
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Colombia 76
María Claudia Martínez and Daniela Huertas Vergara
DLA Piper

France 83
Benjamin May and Farah Bencheliha
Aramis Law Firm

Germany 95
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Greece 102
Vasiliki Christou
Vasiliki Christou, Attorney at Law

Hong Kong 109
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 118
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 126
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Indonesia 133
Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Noor Prayoga Mokoginta
AKSET Law

Italy 142
Paolo Balboni, Luca Bolognini, Antonio Landi and Davide Baldini
ICT Legal Consulting

Japan 150
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Malaysia 159
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 166
Terence Cassar, Ian Gauci and Bernice Saliba
GTG Advocates

Mexico 174
Abraham Diaz and Gustavo A Alcocer
OLIVARES

Netherlands 182
Inge de Laat and Margie Breugem
Rutgers Posch Visée Endedijk NV

New Zealand 190
Derek Roth-Biester and Megan Pearce
Anderson Lloyd Lawyers

Portugal 197
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 206
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Laura Dinu
MPR Partners | Maravela, Popescu & Asociații

Russia 214
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian L Zimbler
Morgan Lewis

Serbia 222
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 229
Lim Chong Kin and Charis Seow
Drew & Napier LLC

South Korea 243
Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim
LAB Partners

Sweden 253
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 261
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 271
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Turkey 278
Esin Çamlıbel, Beste Yıldızili Ergül and Naz Esen
Turunç

United Kingdom 286
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 296
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

South Korea

Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim
LAB Partners

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of PII in Korea consists of the Personal Information Protection Act (the PIPA) and various sector-specific laws. The PIPA is the overarching statute regarding the protection of PII and was enacted with reference to the Organisation for Economic Co-operation and Development guidelines and similar foreign precedents. Prior to the amendments that became effective as of 5 August 2020, the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) applied to information and communications technology (ICT) and online privacy. However, the amendments, effective as of 5 August 2020, amended the Network Act and the PIPA so that the privacy-related provisions in the Network Act are incorporated into the PIPA. Additionally, Korea has the following sector-specific laws that regulate the protection of PII:

- the Credit Information Use and Protection Act (the Credit Information Act) governs the protection of credit information in the finance sector;
- the Framework Act on Consumers applies to consumer data;
- the Act on the Consumer Protection in Electronic Commerce governs privacy in the context of electronic commerce;
- the Act on the Protection, Use, Etc, of Location Information (the Location Information Act) governs location information;
- the Medical Service Act applies to data related to healthcare;
- the Act on the Promotion of Workers' Participation and Cooperation applies to data in the context of labour and employment; and
- the Framework Act on Education applies to data in the context of education.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

In Korea, multiple governmental authorities deal with data protection. The Personal Information Protection Commission, which is under the direct supervision of the president, is a governmental commission established pursuant to the PIPA with the authority to review and determine PII protection policy-related matters. The Ministry of the Interior and Safety has the authority to oversee compliance with the PIPA and enforce it. The Korea Communications Commission (KCC) and the Financial Services Commission have authority pursuant to the Network Act and the Credit Information Act, respectively, to perform PII protection-related work.

Under the amendment to the PIPA, effective as of 5 August 2020, the Personal Information Protection Commission has broader authority and is expected to become the control tower for PII protection. In addition to having the authority to review and determine PII protection-related matters, the Personal Information Protection Commission has the authority to enforce and oversee compliance with the PIPA. The power of the Personal Information Protection Commission has also been expanded to include the discretion to investigate and impose sanctions and fines. Further, the joint responsibilities of the Ministry of the Interior and Safety, the KCC and the Financial Services Commission to oversee PII protection have been consolidated and transferred to the Personal Information Protection Commission (such as the power to demand information, investigate, impose monetary fines, issue corrective orders, charge and recommend sanctions).

Regardless of the amended PIPA coming into effect, as the controlling authority for the Credit Information Act in relation to financial institutions and credit information companies, the Financial Services Commission has the power to investigate any violation of the Credit Information Act and impose monetary or administrative fines. As the controlling authority for the Location Information Act, the KCC has the power to demand information, investigate and impose monetary or administrative fines in relation to the protection of location information. The Fair Trade Commission has the power to order corrective measures regarding unfair terms and conditions relating to PII.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There has been an increasing need to establish a body to enable the consistent making of PII protection policies and discussions regarding PII protection among central administrative agencies. As such, the Enforcement Decree of the PIPA (the Enforcement Decree), which has also been amended with effect on 5 August 2020, stipulates that each special metropolitan city, metropolitan city, special self-governing city, province and special self-governing province must establish a council of institutions related to PII protection (a city or province council), the composition of the city or province council, and matters subject to discussion by the city or province council.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The PIPA, the Credit Information Act and other sector-specific laws provide for administrative sanctions or criminal penalties that apply upon breaches occurring.

A company that violates the PIPA can be subject to administrative sanctions and criminal penalties. The Personal Information Protection Commission can issue corrective orders, such as the termination of any activities that infringe on PII, the temporary suspension of PII processing, and the implementation of necessary measures to protect and prevent any infringement of PII. Additionally, if the company is determined to have violated any laws related to PII protection, a recommendation for disciplinary measures against the responsible individual (including the representative director and the officer in charge) may be issued. Further, a monetary fine of up to 500 million won can be imposed for the loss, theft, leakage, alteration and impairment of a resident registration number and under certain other circumstances. A monetary fine of up to 3 per cent of total revenue can be imposed for processing pseudonymised information for the purpose of identifying a particular individual. For violations of certain provisions of the PIPA, such as providing PII to a third party without the data subject's consent, criminal penalties may be imposed, such as imprisonment for up to five years or a monetary penalty of up to 50 million won.

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Information Protection Act (the PIPA) is the overarching law and applies to all private sectors and government sectors, individuals and companies. There is no organisation that is exempt from the PIPA. However, the PIPA provides that when a governmental agency requires personally identifiable information (PII) to conduct its duties prescribed by law for the purpose of public interest, PII may be collected, used and provided without consent.

The sector-specific laws such as the Credit Information Use and Protection Act (the Credit Information Act), the Act on the Protection, Use, Etc, of Location Information (the Location Information Act), the Medical Service Act, and the Framework Act on Education only apply to the relevant sectors.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The PIPA and the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) both restrict the unauthorised interception of communications or electronic commerce. The PIPA focuses on implementing measures that would prevent unauthorised interception while the Network Act provides for protection of PII processed by information and communications technology (ICT) networks and penalises interception by unauthorised persons.

Such activities could also be subject to the Protection of Communications Secrets Act or the Criminal Act. Under the Protection of Communications Secrets Act, mail censorship, interception of ICT communications, providing communication records, or the recording of or listening to confidential conversations of third parties are prohibited unless they fall under statutory exceptions.

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

In addition to the PIPA, there are several laws that provide for specific data protection rules by sector. The ICT sector is subject to the Network Act, the Framework Act on Electronic Documents and Transactions, the Location Information Act, and the Protection of Communications Secrets Act. Employee monitoring is governed by the Act on the Promotion of Workers' Participation and Cooperation. Information in the healthcare sector is subject to the Medical Service Act, the National Health Insurance Act, the Public Health and Medical Services Act and the Emergency Medical Service Act. Data protection in the finance sector is governed by the Credit Information Act, whereas the education sector is governed by the Framework Act on Education.

PII formats

8 What forms of PII are covered by the law?

Under the PIPA, PII means the following:

- information that can identify a living person, such as their name, resident registration number or image;
- a certain piece of information that, even if it cannot identify a person by itself, can be easily combined with other information to identify a person, reasonably considering the accessibility of the other information and the time, cost and technology required for identifying a person; and
- pseudonymised information that cannot be used to re-identify a person without the assistance of additional information.

There is no limit as to the format or formality of PII.

Under the sector-specific laws, the scope of PII that is covered differs. For example, under the Credit Information Act, personal credit information means data that is necessary to determine the creditworthiness and credit transaction capacity of an individual. Under the Location Information Act, 'personal location information' means the location of a certain individual (including information, when combined with other information, that can identify the location of an individual).

Extraterritoriality

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The existing obligations of foreign ICT service providers to appoint a representative in Korea under the Network Act that have been moved to the PIPA pursuant to the amendments effective as of 5 August 2020 are as follows:

First, an ICT service provider that does not have a domicile or place of business in Korea with total revenue for the preceding year of no less than 1 trillion won; or revenue relating to ICT services for the preceding year of no less than 10 billion won, or average daily users (whose PII is being stored and managed) of no less than 1 million for the last three months of the preceding year must designate a representative in Korea to act as its chief information protection officer (CIPO) under the PIPA. This representative must perform the duties of the CIPO under the PIPA and in the event of any data leakage, file reports to the regulatory authorities, notify the data subjects and submit material for investigation.

Second, the rules that previously applied to overseas transfer of PII also apply to the onward transfer of PII (ie, the transferring of PII that

has already been transferred overseas) to a third country. Accordingly, in cases of onward transfer, the data subject's consent is required.

Third, by adopting the principle of reciprocity, any foreign ICT service provider that is domiciled in a country that restricts overseas transfer of PII can be subject to the same level of restriction on the overseas transfer of PII from Korea.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Under the PIPA, 'processing' means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, output, correction, recovery, use, provision, disclosure and destruction of PII, and other similar activities. The PIPA does not particularly distinguish between those that control or own PII and those that provide PII processing services to owners. Under the PIPA, the term 'PII processor' is defined broadly to include any party (such as a public institution, legal person, organisation or individual) that processes personal information directly or indirectly to operate personal information files for official or business purposes.

Rather, a similar distinction under the PIPA to that between data controller and data processor would be the concepts of 'delegator' and 'delegatee' of processing. When a PII processor delegates PII processing to a third party (ie, delegatee), the delegator needs to conduct training of the delegatee to prevent loss, theft, leakage, falsification, alteration or destruction of PII and supervise the delegatee's processing activities to ensure secure processing of PII in accordance with the Enforcement Decree of the PIPA. In the event any liability arises in the context of PII processing by the delegatee due to a violation of the PIPA, the delegatee would be treated as an employee of the delegator vis-à-vis the data subject. The delegatee is prohibited from using PII beyond the scope of the delegation and from providing the PII to third parties. Since the delegatee falls under the scope of PII processor, the delegatee is subject to the obligations of a PII processor, such as the obligation to procure PII security measures.

The PIPA also imposes a higher level of PII protection to certain types of PII processors. Governmental agencies have heightened obligations for PII protection compared to the private sector. Such obligations include the duties to:

- disclose the registration of PII files;
- conduct privacy impact assessments;
- establish and disclose privacy policies that include policies regarding PII files that are subject to registration;
- grant the data subject the right to access PII; and
- participate in dispute resolution procedures.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

As a matter of principle, personally identifiable information (PII) processing is permitted only with the consent of the data subject. However, PII processing without consent is possible in the following exceptional or inevitable cases under the applicable law.

Under the Personal Information Protection Act (the PIPA), PII processing without the data subject's consent is permitted in the following cases:

- statutory exceptions;
- inevitable for compliance with law;
- inevitable for governmental agencies to conduct their statutory duties;
- inevitable for execution of and performing under contracts with the data subject;
- necessary to protect the life, physical safety or property interest of the data subject or a third party and the data subject is not available to provide consent; or
- necessary to achieve the legitimate interest of the data processor and such interest overrides the interest of the data subject.

In addition to the above, under the amendments to the PIPA, effective as of 5 August 2020, the PII processor may use PII without the consent of a data subject pursuant to the Enforcement Decree as long as the use is within the scope reasonably related to the initial purpose of PII collection, taking into account whether such use would cause disadvantages to the data subject and whether the necessary measures to ensure security, such as encryption, have been taken. The PII processor may also process pseudonymised information without the consent of data subject for purposes such as statistics, scientific research and preservation of records for public interest.

Under the Credit Information Act, PII processing without the data subject's consent is permitted in the following cases:

- PII processing without data subject's consent that is permitted under the PIPA;
- disclosure or public filing of information pursuant to certain statutes;
- disclosure or public filing of information through publications, media or channels, such as the websites of public institutions set forth under the Official Information Disclosure Act; and
- disclosure of information by the data subject directly or through a third party on social networking services, or circumstances equivalent thereto, as set forth in the Enforcement Decree of the Credit Information Use and Protection Act (the Credit Information Act) only to the extent that it is objectively determined that the data subject consented.

Further, under the amendments to the Credit Information Act effective as of 5 August 2020, an exception allows the use of pseudonymised information by credit information companies without the data subject's consent for specific purposes such as generating statistics for commercial purposes including market research, research including industrial research, and the preservation of records for public interest.

Under the Act on the Protection, Use, Etc, of Location Information (the Location Information Act), PII processing without the data subject's consent is permitted in the following cases:

- upon the request of an emergency rescue agency or the police for the purpose of emergency rescue;
- upon the request of an emergency rescue agency for the purpose of sending warnings;
- inevitable for execution of and performance under contracts with the data subject;
- necessary to process payment for the location information services or location-based services that have been provided to the data subject; or
- statutory exceptions under other laws.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Under the PIPA, more stringent rules (such as the requirement to obtain a separate consent) apply to:

- sensitive information (which encompasses types of information that can substantially impair the data subject's privacy, such as ideology, beliefs, trade union or political party membership, political opinion, health and sexual life); and
- PII (such as resident registration number, passport number, driver's licence number or foreigner registration number).

In particular, the processing of resident registration numbers is prohibited in principle and may only be allowed if specifically permitted under law or explicitly required to protect the life, physical safety or property interest of the data subject or a third party, or similar inevitable circumstances prescribed by the Personal Information Protection Commission.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The Personal Information Protection Act (the PIPA) requires data processors to notify data subjects as set forth below.

First, when the data processor obtains consent from the data subject for personally identifiable information (PII) collection, the data processor must notify the data subject of the following information:

- the purpose of the collection and use of PII;
- the type of PII being collected;
- the retention period of PII; and
- the data subject's right to refuse consent and any disadvantages which will result from refusing consent.

If there are any changes to the above, such changes also need to be notified to the data subject.

Second, if the PII being processed by the PII processor is collected from a party other than the data subject, the PII processor must notify the data subject of the following information immediately upon the data subject's request:

- the source where the PII was collected;
- the purpose of the PII processing; and
- the right of the data subject to request that the PII processor suspend the processing of the data subject's PII.

Third, if the PII processing is being delegated to a third party, the following information needs to be published on the relevant website or otherwise disclosed in a manner easily accessible to the data subject.

Fourth, information and communications technology (ICT) service providers that have an average number of daily users (whose PII is being stored and managed) of no less than one million for the last three months of the preceding year or a revenue for ICT-related services that is no less than 10 billion won in the preceding year, must notify their users at least once a year in writing of the details of their PII usage, including any provision and delegation of processing to third parties.

Exemption from notification

14 | When is notice not required?

Under the PIPA, notice is not required under exceptional circumstances, such as a threat to life, risk of bodily harm or substantial impairment of rights regarding another person's property or other interest.

Under the Credit Information Use and Protection Act (the Credit Information Act), in principle, any person who intends to provide, or who receives, personal credit information to or from a third party is required to notify the data subject. However, the Credit Information Act waives this notice requirement for pseudonymised information, and notice is not required when a credit information provider or user provides pseudonymised information to personal credit evaluation companies, sole proprietorship credit evaluation companies, corporate credit verification companies or credit information collection agencies for credit rating and evaluation purposes.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Under the PIPA, the consent for collection of PII and the consent for sharing PII with a third party should be clearly distinguished so that the data subject is aware of the scope of each consent. Also, when collecting PII, the data processor needs to clearly distinguish between mandatory PII and optional PII, thereby providing a degree of control to the data subject.

However, under the amendments to the PIPA effective as of 5 August 2020, a PII processor may use PII without the consent of a data subject pursuant to the Enforcement Decree of the PIPA (the Enforcement Decree) as long as the use is within the scope reasonably related to the initial purpose of PII collection, taking into account whether such use would cause disadvantages to the data subject and whether the necessary measures to ensure security, such as encryption, have been taken.

Under the Enforcement Decree, the following criteria must be considered in order to determine whether PII can be used without consent:

- whether the purpose of the additional use of the PII without consent has considerable relevance to the initial purpose of the collection;
- whether, given the circumstances and processing practices in which the PII was collected, additional use or provision of the PII was foreseeable;
- whether the additional use of the PII without consent unfairly infringes the interests of the data subject; and
- whether measures necessary to secure safety, such as pseudonymisation or encryption, were adopted.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Under the PIPA, a PII processor must ensure the accuracy, completeness and currency of the PII to the extent required for the purpose of the PII processing by implementing the following procedures:

- pre-verification of the PII being inputted;
- upon a request by the data subject to access and correct their PII; and
- correction or deletion of inaccurate information.

Further, the PII processor should exercise due care when processing PII to prevent any intentional or negligent alteration or destruction of PII.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Under the PIPA, PII must be destroyed when it becomes no longer necessary to retain the PII due to the expiry of the PII holding period or the expiry or completion of the purpose of the PII processing.

Also, in the case of ICT service providers whose users have been inactive for a year (or other period as permitted under applicable

statutes or as requested by the data subject), the PIPA requires the destruction of PII (or other necessary measures) and notice given to the data subjects by email (or other means) at least 30 days prior to the expiry of such a one-year period (or the aforementioned different period) of the items set forth in the Enforcement Decree, such as the fact that the PII will be destroyed, the expiry date and the type of PII which will be destroyed.

The specific holding period for PII is determined by the sector-specific laws. For example, the Act on the Consumer Protection in Electronic Commerce, Etc, states that:

- records of expression and advertising should be stored for six months;
- records of contracts and retractions of applications should be stored for five years;
- records of payments and provision of goods should be stored for five years; and
- records of consumer complaints and dispute resolutions should be stored for three years.

Additionally, under the Credit Information Act, credit information should be deleted by the date which is the earlier of five years from the termination of the financial transaction and three months from the date on which the purpose for collecting and providing PII has been achieved. Certain records require retention for three years under the Credit Information Act.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

In principle, a PII processor can only use PII for the purpose for which the PII was collected. Under the amendments to the PIPA effective as of 5 August 2020, however, the PII processor may use PII without the consent of a data subject pursuant to the Enforcement Decree, as long as it is within the scope reasonably related to the initial purpose of PII collection, taking into account whether such use would cause disadvantages to the data subject and whether the necessary measures to ensure security, such as encryption, have been taken. The PII processor may also process pseudonymised information without the consent of data subject for purposes such as statistics, scientific research and preservation of records for the public interest.

It is illegal for a PII processor to use the PII beyond the purpose of collection unless the consent of the data subject has been obtained or there are exceptions in other statutes. Accordingly, it can be viewed that the finality principle has been adopted.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In principle, a PII processor can only use PII for the purpose for which the PII was collected, unless the purpose falls under the explicit exceptions that allow PII processing without consent or the purpose relates to pseudonymised PII in limited circumstances. Accordingly, unless the new purpose falls under the aforementioned exceptions, additional consent from the data subject would be required to use PII for a new purpose.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Under the Personal Information Protection Act (the PIPA), a personally identifiable information (PII) processor is required to implement physical, technical and organisational measures to procure security, including the implementation of internal controls, access controls, access authority restrictions, application of encryption technology or equivalent measures, storage of access records and measures to prevent forging or alteration, installation and renewal of security software, and the procurement of PII storage facilities or a lock system. Details of such measures are set forth in the Standards for Procuring Safety Measures regarding Personal Information issued by the Ministry of the Interior and Safety.

Under the Network Act, manufacturers of mobile device hardware, operating systems or software are required to procure PII protection measures for access control that restrict information and communications technology (ICT) service providers from accessing information and functions in mobile devices (such as consent and withdrawal mechanisms).

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the PIPA, once the PII processor finds out that PII has been leaked, the PII processor must notify, without delay, the effected data subject(s) of the following:

- the type of PII that has been leaked;
- the timing and background of the leakage;
- the actions that the data subject can take to minimise the damages resulting from the PII leakage;
- the remedial measures being taken by the PII processor and the procedures for compensation for damages; and
- the contact information of the division where the data subject can file for damages.

In the event the PII processer takes an emergency action to prevent any additional leakage (such as suspending connection, inspecting and supplementing defects and deleting the leaked PII), the PII processor can notify the data subject after such action has been taken. If the data leakage involves no less than 1,000 data subjects, the PII processor must notify the data subjects in writing and also post such information on its website for seven days or more (or if there is no website, in its place of business or another easily accessible place).

Further, in the event a PII leakage involves no less than 1,000 data subjects, the PII processor must notify, without delay, the result of the remedial measures and data subject notification to the Personal Information Protection Commission or the Korea Internet and Security Agency (KISA).

The PIPA also imposes obligations on ICT service providers (or any third party who has been provided with PII from an ICT service provider) to notify, without delay, the data subject and the Personal Information Protection Commission or the KISA upon loss, theft or leakage of PII. If there is a justifiable ground, such as that the data subject's contact information is not known, the ICT service provider or the third party may take a substitute measure in place of notifying the data subject. Further, if such an ICT service provider or a third party receives a request from

the Personal Information Protection Commission (or any other professional institution designated under the Enforcement Decree of the PIPA) regarding PII that has been exposed to the public, it must take necessary measures such as deleting or blocking such PII.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Under the Personal Information Protection Act (the PIPA), a personally identifiable information (PII) processor is obligated to designate a chief privacy officer (CPO) who is in charge of PII processing activities. The CPO's duties include:

- the establishment and implementation of PII protection plans;
- the periodical review and improvement of PII processing status and practice;
- the handling of complaints and compensation for damages arising from PII processing;
- the establishment of internal control systems to prevent leakage, misuse and abuse of PII;
- the establishment and implementation of PII protection education plans;
- the protection, control and supervision of PII files;
- the establishment, amendment and implementation of privacy policies;
- the organisation of PII files; and
- the destruction of PII where its purpose has been achieved or where the retention period has expired.

Further, the CPO must take immediate remedial action once they become aware of any breach of privacy laws.

In particular, an information and communications technology (ICT) service provider must designate a representative in Korea to act as the domestic representative as an agent of the CPO, if the ICT service provider does not have a domicile or place of business in Korea and its total revenue for the preceding year is no less than one trillion won, revenue relating to ICT services for the preceding year is no less than 10 billion won, or whose number of daily average users is one million or above for the last three months of the preceding year. An ICT service provider who has designated a domestic representative must disclose the name, address, telephone number and email address of the domestic representative by including the information in the PII processing policy.

Separate from the requirement to appoint a CPO under the PIPA, under the Network Act, a chief information security officer (CISO) must be appointed in relation to the security of ICT systems and security of PII. However, this requirement does not apply to an ICT service provider whose number of daily average users is less than one million for the last three months of the preceding year and whose revenue relating to ICT services for the preceding year is less than 10 billion won, and if the ICT service provider is also a person who intends to operate a small-scale value-added telecommunications business, the capital of which falls under the criteria prescribed by the Enforcement Decree of the PIPA (the Enforcement Decree), who is deemed to have filed a report on the value-added telecommunications business pursuant to the Telecommunications Business Act, a micro-enterprise (eg, whose number of full-time workers is less than 10) under the Act on the Protection of and Support for Micro-Enterprises or a small enterprise under the Framework Act on Small and Medium Enterprises.

The duties of the CISO include:

- the establishment, management and operation of an information protection system;
- the analysis, assessment and improvement of defects in PII protection;
- the prevention and remedy of infringement accidents;
- the establishment of preemptive data protection measures, and the design and implementation of security measures;
- the pre-assessment of information security;
- the review of encryption of material information and the adequacy of security servers; and
- any other activities prescribed under the relevant laws to procure information protection.

Under the Credit Information Act, credit information companies must designate at least one credit information administration and protection officer (CIAPO). Centralised credit information collection agencies, credit rating businesses and certain other providers or users of credit information (whose total assets at the end of the preceding year are not less than 2 trillion won and whose number of full-time workers is not less than 300) must appoint an executive as its CIAPO.

Record keeping

23 Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Under the Standards for Procuring Security Measures regarding Personal Information issued by the Ministry of the Interior and Safety, records of access to a PII processing system by a person handling PII under the supervision of a PII processor must be maintained for not less than one year. In the case of PII systems processing PII of more than 50,000 data subjects or PII relating to personal identification or sensitive information, PII must be maintained for not less than two years.

The obligation to maintain internal records is also set out in sector-specific PII protection laws. For example, under the Credit Information Act, credit information companies are required to maintain the following information for three years:

- the name and address of the customer, and the name and address of the entity whom the PII was provided to or exchanged with;
- the details of the scope of work requested by the customer and the date thereof;
- the processing details of the requested scope of work, and the date and details of the credit information provided;
- the purpose, basis, date and items of the PII collected and used;
- the purpose, basis, date and items of the PII provided or received;
- the purpose, basis, date and items of the PII destroyed; and
- other matters prescribed by the Enforcement Decree.

While the above retention period applies to the aforementioned information, the Credit Information Act requires that all credit information be deleted by the date that is the earlier of five years from the termination of the financial transaction and three months from the date on which the purpose for collecting and providing PII has been achieved.

New processing regulations

24 Are there any obligations in relation to new processing operations?

Under the PIPA, heads of governmental agencies have the obligation to conduct a privacy impact assessment that analyses the causes and suggests improvements if there is a risk of infringement of PII arising from the management of PII files, pursuant to the standards prescribed under the Enforcement Decree of the PIPA.

The Network Act requires electronic communication business operators and information providers or intermediaries using

electronic communication services to obtain certification of their overall systems (including physical, technical and organisational measures) to ensure the security and reliability of the information communication network. Details of such certification is set forth in the Standards for Information Protection and the Certification of Personal Information Management Systems issued by the Ministry of Science and ICT.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no general obligations that require personally identifiable information (PII) processors to register with the supervisory authorities. However, under the Personal Information Protection Act (PIPA), governmental agencies that operate PII files must register with the Personal Information Protection Commission certain matters regarding the PII files, including privacy impact assessments. Under the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act), in order to conduct an identity verification business, an application to and designation by the Korea Communications Commission (KCC) is required.

Formalities

26 | What are the formalities for registration?

Under the PIPA, governmental agencies operating PII files are required to register the following information regarding PII files with the Personal Information Protection Commission:

- the title of the PII file;
- the purpose and basis for operating the PII files;
- the PII items recorded in the PII files;
- the method of processing the PII;
- the retention period of PII;
- the recipient of PII, if the PII is provided routinely or repetitively;
- the governmental agency operating the PII files;
- the number of data subjects whose PII is retained as PII files;
- the PII processing department within the governmental agency;
- the department receiving and processing requests for PII access; and
- the scope of PII in PII files to which access can be restricted or denied, or the basis of such a restriction or denial.

Any changes to the registered matters shall be registered by the head of the relevant governmental agency. Meanwhile, certain PII files, such as PII files recording matters related to national security, diplomatic secrets or other matters regarding important national interests, are exempt from such registration requirements.

The application for identity verification business under the Network Act is made to the KCC, pursuant to the Enforcement Decree of the Network Act. Periodical renewal is not required but an amendment filing should be made when there is a change in the information submitted to the KCC.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

The PIPA does not impose any fines or criminal penalties on public institutions that fail to register PII files as required under the PIPA. On the other hand, anyone conducting an identity verification business without a designation by the applicable regulatory authority will be subject to a monetary penalty of 10 million won.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

Pursuant to the amendments to the PIPA, effective as of 5 August 2020, the Personal Information Commission has the right to review the registration status and contents of PII files and recommend improvements to the heads of the relevant governmental agencies but does not have the right to refuse registration.

Under the Network Act, the KCC uses the following criteria to determine whether an entity can conduct an identity verification business in a secure and credible manner:

- physical, technical and organisational measure to procure security for an identity verification business;
- technical and financial capacity to conduct an identity verification business; and
- the adequacy of the size of facilities related to the identity verification business.

When an identification verification service agency falls under any of the following, the KCC may order a full or partial suspension of the identification service business for a period of up to six months and, in the case of (1) and (2), revoke the designation as an identity verification service agency:

1 the designation as an identity verification service agency was induced by fraud or other unjust methods;
2 when an identity verification service agency subject to a suspension order fails to comply with such a suspension order;
3 the entity does not commence an identity verification service business within six months or discontinues an identity verification service business for a period exceeding six months; and
4 the entity no longer satisfies the standards for designation as an identity verification service agency.

Public access

29 | Is the register publicly available? How can it be accessed?

The registration status of PII files registered by the head of a governmental agency that operates PII files is publicly available and may be accessed through the portal for PII protection that is established by the Ministry of the Interior and Safety and operated by Korea Internet and Security Agency upon delegation of authority from the Ministry of the Interior and Safety. The KCC website provides information on the businesses designated as identity verification agencies.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

As, in general, registration or filings are not required for PII processors in Korea, specific legal effects do not exist.

Other transparency duties

31 | Are there any other public transparency duties?

Under the PIPA, a PII processor has the obligation to disclose its PII processing policy, which includes the purpose of PII processing, the retention period, third-party sharing, delegation of processing, the data subject's rights, the chief privacy officer, and the operation of any devices that automatically collect PII (such as internet connection information files) and the refusal thereof. The PII processor must also grant the data subject access to his or her PII and disclose the method and procedure for access to the data subject.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the Personal Information Protection Act (the PIPA), the data subject's consent is required for the personally identifiable information (PII) processor to disclose PII to a third party. In contrast, the data subject's consent is not required to delegate PII processing to a third party as long as such delegation is posted on the PII processor's website. The rationale behind this dichotomy is that the provision of PII to third parties is for the benefit of the third-party recipient, whereas the delegation of PII processing is for the benefit of the PII processor.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

Under the PIPA, when PII is being disclosed to another recipient due to a merger or business transfer, the PII processor is required to notify the data subject in writing or by disclosure on the company website if providing a written notice is not possible.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

Under the PIPA, to provide PII to a third party outside of Korea, the following information needs to be notified to the data subject and consent must be obtained for such transfer:

- the recipient of PII;
- the recipient's purpose for using PII;
- the type of PII being provided;
- the period of retention and use of PII by the recipient; and
- the data subject's right to refuse consent to transfer and any disadvantages that will result from refusing consent.

A PII processor cannot enter into a contract for the overseas transfer of PII in violation of these restrictions under the PIPA. Note, however, that consent is not required when PII is being provided to a third party outside of Korea for the purpose of delegating PII processing.

Further, under the amendments to the PIPA effective as of 5 August 2020, information and communications technology (ICT) service providers are required to obtain the consent of the user in order to provide, delegate processing, or store PII outside of Korea. However, ICT service providers may be exempt from the consent requirements in relation to the delegation of processing or storing of PII outside of Korea, provided that they notify the users of the following information by email, writing or continuously posting on the PII processor's website:

- the PII items being transferred;
- the country to which the PII is being transferred;
- the transfer date and method;
- the name of the recipient of the PII (in the case of a corporation, the name of the corporation and the contact number of the data protection officer); and
- the recipient's purpose in using the PII, and the period of retention and use of the PII.

Under the Enforcement Decree of the PIPA (the Enforcement Decree), when PII is transferred overseas, measures to secure the safety and the protection of the PII, matters concerning the handling of grievances against the infringement of PII and dispute resolution, and other measures necessary for the protection of users' PII must be taken. The same rule will be applied, in principle, to PII that has been lawfully transferred overseas and is re-transferred to another country.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Approval or authorisation from a supervisory authority is not required for cross-border transfer of PII.

Notwithstanding, the government can require an ICT service provider to adopt the following measures with respect to the processing of information related to national security and policies or information regarding advanced technology or devices developed in Korea:

- the establishment of systematic and technical measures to prevent illegitimate use of the information communication network;
- systematic and technical measures to prevent unlawful destruction or manipulation of information; and
- measures to prevent leakage of material information acquired during the information communication service provider's processing of information.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The amendments to the PIPA effective as of 5 August 2020, require the data subject's consent in the case of onward transfer of PII (that has already been legally transferred outside of Korea) to a third country. In the event of onward transfer of PII to a foreign country, ICT service providers must implement measures related to procuring security measures required for a PII processor, dispute resolution and handling of grievances regarding PII, and other measures necessary for the protection of users' PII. Such rules also apply to overseas transfers of PII for the delegation of PII processing.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Personal Information Protection Act (the PIPA), a data subject can request a personally identifiable information (PII) processor to provide access to the PII being processed, and the PII processor must allow the data subject to access his or her PII within the time frame set forth in the Enforcement Decree of the PIPA. If there is any justifiable reason for a delay in granting access, the PII processor can extend the time frame by notifying the data subject of such an extension and the relevant cause. Once the cause no longer exists, the PII processor must grant access to the data subject without delay.

The PII processor can refuse or limit the data subject's access in the event there are:

- statutory prohibitions or restrictions on access;
- potential threat to life or risk of bodily harm; or
- potential impairment of property or other rights of another person.

In such cases, the PII processor must notify the data subject of the reason for the refusal or limitation of access.

Under the amendments to the PIPA, which became effective as of 5 August 2020, an ICT service provider must ensure that the method

for requesting access to PII by a data subject must be easier than the method for providing consent for PII collection.

Other rights

38 | Do individuals have other substantive rights?

Under the PIPA, a data subject can require a PII processor to correct or delete his or her PII once the data subject has accessed and reviewed his or her PII, pursuant to the method and procedures set out by the PII processor. Further, the data subject can require the PII processor to suspend the processing of his or her PII. Upon receiving a request for correction or deletion of PII, the PII processor must correct or delete such information or notify the head of the agency that provided the PII and take necessary measures.

Under the amended PIPA effective as of 5 August 2020, the data subject has the right to withdraw his or her consent for PII processing by an ICT service provider at any time, and the method for requesting corrections must be easier than the method of providing consent to PII collection.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the PIPA, a data subject can seek monetary damages or compensation if the damages incurred by the data subject were due to the violation of the PIPA by the PII processor. In such cases, the PII processor will be liable unless it can prove that there was no intentional misconduct or negligence on the part of the PII processor. If the data subject incurred damages caused by the loss, theft, leakage, falsification, alteration or impairment of PII arising from the intentional misconduct or negligence of the PII processor, a court may order payment of damages up to three times the amount of the damages incurred.

Under the amendments to the PIPA effective as of 5 August 2020, ICT service providers with sales revenue of no less than 50 million won in the previous fiscal year and the number of daily average users with PII stored and managed of no less than 1,000 during the last three months of the previous year must take necessary measures, such as retaining insurance, enrolling in associations or setting aside reserves to ensure payment of damages.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of data subjects under the PIPA can be enforced through litigation in court, by filing criminal complaints or applying to the Personal Information Dispute Mediation Committee for mediation of a dispute.

In the event of multiple data subjects being subject to similar damages or infringements of rights which are set forth in the Enforcement Decree of the PIPA, a collective dispute mediation may be filed.

If a PII processor does not accept the results of mediation, consumer groups or non-profit organisations may file a class action with the court to obtain an injunction against the infringement of rights.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The amended Personal Information Protection Act (the PIPA) stipulates that the PIPA shall not apply to anonymous information, which is information that, giving reasonable consideration to time, cost and technology, cannot be used to identify an individual even when it is combined with additional information. Such anonymous information was not deemed subject to the PIPA and has been explicitly carved out from the amended PIPA effective as of 5 August 2020. However, there are no express guidelines on the distinction between anonymous information and pseudonymised information, leaving the distinction between the two types of information unclear.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects can appeal against unlawful orders of the supervisory authorities to the courts.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

There are no specific statutory provisions that deal with cookies or equivalent technologies. Nonetheless, cookies can be viewed as personally identifiable information (PII) if they can be easily combined with additional information to identify a particular individual.

Under the PIPA, a PII processor is required to disclose, by including in its PII processing policy, terms regarding the installation, operation and rejection of devices that automatically collect PII, such as internet connection record files.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Under the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act), to distribute marketing information for commercial purposes through electronic transmission, express prior consent of the recipient is required. In the following cases, however, this consent requirement is waived:

- a party that has collected the recipient's contact information through transactions regarding certain goods sends the recipient marketing information for commercial purposes regarding the same type of goods; and
- a telemarketer under the Act on Door-to-Door Sales, Etc, verbally notifies the recipient from where his or her PII was collected and makes solicitations over the telephone.

A separate express prior consent is required for the distribution of marketing information for commercial purposes through electronic transmission (except for by email) between the hours of 9pm and 8am the following day.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The Act on the Development of Cloud Computing and Protection of Its Users (the Cloud Computing Act) was enacted in 2015 and is currently in effect. The principles of the PIPA and the Network Act, as well as sector-specific laws may also apply to cloud computing service providers.

Under the Cloud Computing Act, a cloud computing service provider must endeavour to enhance the quality, performance and data protection levels of its cloud computing service. The Minister of the Ministry of Science and ICT has the authority to set the standards for quality, performance and data protection (including physical, technical and organisational measures) and issues a recommendation to cloud service providers to comply with such standards. Also, under the Cloud Computing Act, a cloud service provider cannot disclose a user's information to a third party or use the user's information for purposes other than providing cloud computing services without the user's consent, unless a court order or subpoena has been issued by a judge. The user can require the cloud computing service provider to inform the user of the country in which the user's information is stored.

Recently, the Electronic Finance Supervisory Regulations have been amended to allow the use of the cloud for PII such as credit information and personal identification information to promote the adoption of the cloud to further innovation and development of fintech businesses.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The three major privacy laws of Korea – the Personal Information Protection Act (the PIPA), the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) and the Credit Information Use and Protection Act (the Credit Information Act) – are subject to substantial amendments, effective as of 5 August 2020. The main amendments include incorporating online privacy-related provisions regarding information and communications technology service providers (pre-existing under the Network Act) in the PIPA and permitting the use of pseudonymised information under the PIPA and the Credit Information Act. The issue of pseudonymisation of personally identifiable information (PII) has raised questions as to the standards and methods of pseudonymisation and the purpose for which pseudonymised information can be used.

Another important amendment to the PIPA relates to the status of the Personal Information Protection Commission, which has been elevated to a control tower of PII. In the past, the Personal Information Protection Commission only had the authority to review and determine PII policies as the enforcement and supervisory powers of privacy laws lied with the sector-specific agencies, such as the Ministry of Interior and Safety, the Korea Communications Commission, the Financial Services Commission, the Korea Internet and Security Agency and the Korea Fair Trade Commission. Under the amended PIPA, however, the Personal Information Protection Commission is granted with powers to enforce and supervise privacy-related matters and is expected to play a role as a central governmental agency with an independent budget and human resources.

Such changes are in line with the criteria for the European Union adequacy decision that requires a separate supervisory authority for personal information protection.

LAB PARTNERS

Young-Hee Jo
yhjo@labpartners.co.kr

Seungmin Jasmine Jung
smjung@labpartners.co.kr

Kwangbok Kim
kbkim@labpartners.co.kr

8F, VPLEX, 501 Teheran-ro
Gangnam-gu
Seoul 06168
Republic of Korea
Tel: +82 2 6956 0250
http://labpartners.co.kr

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7