Data Protection & Privacy

Contributing editors
Aaron P Simpson and Lisa J Sotto

2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2019

Contributing editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

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

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Seventh edition
ISBN 978-1-78915-010-0

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

CONTENTS

Preface

Data Protection & Privacy 2019

Seventh edition

Getting the Deal Through is delighted to publish the seventh edition of *Data Protection & Privacy*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

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 **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 Argentina, Colombia, Greece, Korea, Malta and Taiwan.

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.gettingthedealthrough.com.

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.

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.

GETTING THE DEAL THROUGH

London
July 2018

Korea

Seung Soo Choi and Seungmin Jasmine Jung
Jipyong LLC

Law and the regulatory authority

1 Legislative framework

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?

Korea has a comprehensive set of laws for the protection of PII. The generally applicable law is the Personal Information Protection Act (the PIPA), which provides for the overall protection of PII. The PIPA was enacted with reference to the OECD guidelines and similar foreign precedents. Other than the PIPA, Korea has sector-specific laws as follows:

- the Credit Information Use and Protection Act (the Credit Information Act) protects credit information used in the finance sector;
- the Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc (the Network Act) governs the information communication technology sector; and
- the Medical Service Act applies to the healthcare sector.

2 Data protection authority

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

The Ministry of the Interior and Safety has the authority to oversee compliance with the PIPA and has the powers to investigate any violation of the PIPA. The Financial Services Commission has the authority to oversee the Credit Information Act and has the powers to investigate any violation of the Credit Information Act and impose monetary fines. The Korea Communications Commission has the authority to oversee compliance with the Network Act and has the powers to investigate, regulate and impose monetary fines. The Personal Information Protection Commission is a governmental commission that has the authority to review and determine PII protection policies, to enhance systems and laws and to interpret and implement laws related to PII. The Korea Internet and Security Agency has been delegated authority from the Ministry of the Interior and Safety and the Korea Communications Commission and functions as the governmental agency for the purposes of the PIPA and the Network Act.

3 Legal obligations of data protection authority

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

The PIPA explicitly states that 'unless specifically provided in other laws, the regulation of PII protection shall comply with the PIPA'. This means that it is inevitable for sector-specific authorities such as the Financial Services Commission or the Korea Communications Commission to cooperate with the Ministry of the Interior and Safety, which oversees the PIPA. Although there are no statutory legal obligations, the relevant authorities all cooperate with each other in practice.

4 Breaches of data protection

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

A company that violates the PIPA can be subject to both administrative sanctions and criminal penalties. The Ministry of the Interior and Safety 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 up to 500 million won can be imposed for the loss, theft, leakage, alteration and impairment of a resident registration number.

An individual who discloses or provides unauthorised access to PII acquired in the course of business or impairs, destroys, modifies, falsifies or impairs another person's PII without proper authorisation or beyond the scope of his or her authorisation can be subject to imprisonment for up to five years or a monetary penalty up to 50 million won.

Further, a party that fails to adopt necessary measures to procure security pursuant to the PIPA and, as a result, incurs loss, theft, leakage, alteration or impairment of PII can be subject to imprisonment for up to two years or a monetary penalty up to 10 million won.

Scope

5 Exempt sectors and institutions

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

The PIPA is a general law and applies to all private sectors and government sectors, individuals and companies.

In contrast, the Credit Information Act has limited applicability to financial institutions. The Network Act applies only to information communication service providers.

6 Communications, marketing and surveillance laws

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 Network Act both restrict the unauthorised interception of communications or electronic commerce. Such activities could also be subject to the Protection of Communications Secrets Act or the Criminal Act.

7 Other laws

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

There are several laws that provide for specific data protection rules by sector. 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, National Health Insurance Act, Emergency Medical Service Act and Public Health and Medical Services Act. Information in the finance sector is governed by the Credit Information Act. Lastly, the information communication sector is subject to the Framework Act on Electronic Documents and Transactions, the Act on the Protection, Use, etc, of Location Information (the Location Information Act), the Network Act and the Protection of Communications Secrets Act.

8 PII formats

What forms of PII are covered by the law?

PII under the PIPA means information regarding a living person such as the name, resident registration number or image that can identify such living person. Even if a certain piece of information cannot, by itself, identify a person, if the information can be easily combined with other information to identify a person, such information is also deemed to be PII.

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

9 Extraterritoriality

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

The PII protection laws of Korea do not explicitly deal with extraterritorial application. The position of the Korean government, however, is that foreigners or foreign corporations that process PII of Koreans should be subject to the PII protection laws of Korea.

10 Covered uses of PII

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 distinguish between those that control or own PII and those that provide PII processing services to owners. Rather, a single concept or term of 'PII processor' is used for a 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.

Although the PIPA does not impose different duties on controllers or processors, a higher level of PII protection duties are imposed on governmental agencies compared to the private sector. Such obligations include the duties to:

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

Legitimate processing of PII

11 Legitimate processing – grounds

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, PII processing is permitted only with the consent of the data subject. However, PII processing without consent is possible for certain exceptional or inevitable cases, such as cases in which:

- statutory exceptions are provided;
- it is inevitable for compliance with the law;
- it is inevitable for governmental agencies to conduct their statutory duties; or
- it is inevitable for executing and performing contracts with the data subject.

12 Legitimate processing – types of PII

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

Under the PIPA, more stringent rules apply to:

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

Data handling responsibilities of owners of PII

13 Notification

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?

Under the PIPA, if the PII being processed by the PII processor is collected from someone other than the data subject, the PII processor must notify the data subject of the following information immediately upon the request of the data subject:

- the source of the PII collection;
- the purpose of the PII processing; and
- the right of the data subject to request the PII processor to suspend processing of the data subject's PII.

14 Exemption from notification

When is notice not required?

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

15 Control of use

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

In the event the PII processor intends to use PII for marketing purposes, separate consent for such use must be obtained from the data subject.

16 Data accuracy

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.

17 Amount and duration of data holding

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

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

The 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 information on:

- expression and advertising should be stored for six months;
- contracts and retraction of applications should be stored for five years;
- payment and provision of goods should be stored for five years; and
- consumer complaints and dispute resolution should be stored for three years.

18 Finality principle

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

A PII processor can only use PII for the purpose for which the PII was collected. It is illegal for a PII processor to use the PII beyond the purpose of collection. Accordingly, it can be viewed that the finality principle has been adopted.

19 Use for new purposes

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. Although there are exceptions that allow PII processing without consent (such as statutory exceptions, inevitable for compliance with law, inevitable for governmental entities to conduct their statutory duties and inevitable for executing and performing contracts with the data subject), it is difficult to view the use of PII under such exceptions as a new purpose.

Security

20 Security obligations

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

A PII processor is required to implement physical, technical and organisational measures to procure security pursuant to the Enforcement Decree of the PIPA, including the establishment of internal controls and the maintenance of access records in order to prevent loss, theft, leakage, falsification, alteration or impairment of PII.

21 Notification of data breach

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 data subject of the following:

- the type of PII leaked;
- the timing and account 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.

Further, in the event the PII leakage exceeds the scale prescribed under the Enforcement Decree of the PIPA, the PII processor must notify, without delay, the result of the remedial measures and data subject notification to the Minister of the Ministry of Interior and Safety or other professional agency set forth in the Enforcement Decree of the PIPA.

Internal controls

22 Data protection officer

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

A PII processor has the obligation to designate a PII protection officer (often called the data protection officer or DPO) who oversees, and is in charge of, activities related to PII processing. The duties of the DPO include the following:

- 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; and
- other activities prescribed in the Enforcement Decree of the PIPA for the proper processing of PII.

23 Record keeping

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

The obligation to maintain internal records is 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 workscope requested by the customer and the date thereof; and
- the processing details of the requested workscope and the date and details of the credit information provided.

24 New processing regulations

Are there any obligations in relation to new processing operations?

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.

Additionally, electronic communication business operators and information providers or intermediaries using the electronic communication services provided by electronic communication business operators are required to obtain certification of their overall systems, including the physical, technical and organisational measures in order to ensure the security and reliability of the information communication network.

Registration and notification

25 Registration

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 PII processors to register or file a report with the supervisory authorities. However, for certain specific industries, registration with, or permits from, the relevant supervisory authority is required.

Under the PIPA, governmental agencies that operate PII files must register certain matters regarding the PII files with the Minister of the Ministry of Interior and Safety.

Under the Location Information Act, a permit from the Korea Communications Commission is required to provide location-based services, and the following information is required to be submitted to obtain the permit: the company name, the address of the main office, a description and type of the location-based service and major business facilities including the location information system. On the other hand, any location-based service that does not deal with personal location information can file a report with the Korea Communications Commission pursuant to the Enforcement Decree of the Location Information Act.

Under the Credit Information Act, a permit from the Financial Services Commission is required to conduct a business that deals with credit information, such as a credit rating business, credit investigation business or debt collection business.

26 Formalities

What are the formalities for registration?

With respect to a location-based service, the procedures for obtaining the requisite permit or filing a report is set forth in the Enforcement

Decree to the Location Information Act. No fees are required to be paid to the Korea Communications Commission with respect to the permit or filing.

For credit information businesses, the procedures for obtaining the requisite permit are set forth in the Enforcement Decree to the Credit Information Act. There are no fees to be paid to the Financial Services Commission for obtaining such a permit.

27 Penalties

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

Any location-based service that has not obtained the requisite permit or filed the relevant report will be subject to criminal penalties. Likewise, conducting any credit information business without the requisite permit will be subject to criminal penalties.

28 Refusal of registration

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

With respect to a location-based service that deals with personal location information, the following criteria will be comprehensively reviewed in determining the issuance of the permit:

- the feasibility of the location-based service plan;
- technical and organisational measures for the protection of personal location information;
- adequacy of the size of facilities regarding the location-based service;
- financial and technical capacity; and
- other matters necessary for conducting a location-based service.

29 Public access

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

Information on any location-based service or credit information business that has received a permit is publicly available. Information can be accessed through the Korea Communications Commission and the Financial Services Commission.

30 Effect of registration

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

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

31 Other transparency duties

Are there any other public transparency duties?

Under the PIPA, a PII processor has the obligation to disclose the terms and conditions of its PII processing, such as its PII processing policy. Further, a PII processor must ensure protection of the data subject's rights, such as the data subject's right to access PII.

Transfer and disclosure of PII

32 Transfer of PII

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

Under the PIPA, in order for the PII processor to disclose PII to a third party (including sharing of PII), consent from the data subject is required. Conversely, in order to delegate PII processing to a third party, the consent of the data subject is not required. 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.

On the other hand, under the Network Act, an information communication service provider is required to notify, and obtain the consent of, the data subject for both the provision of PII to third parties and the delegation of PII processing. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied.

Update and trends

The increase in the collection, use and storage of PII through newly emerging technologies of the Fourth Industrial Revolution has given rise to wide discussions on striking a balance between privacy and technological advancement. Recent developments include the amendment of the Location Information Act, which has relaxed the requirements for Location of Things (LOT) businesses. The amendment to the Location Information Act allows LOT businesses to file a report with the Korea Communications Commission instead of obtaining a permit.

In the finance sector, the relaxation of PII regulations is being discussed by regulators to promote further use of cloud computing in the sector.The protection of PII in crypto-currency exchanges is also a hot topic, as certain crypto-currency exchanges have been vulnerable to cybersecurity attacks. Given the ubiquitous nature of these technologies, the discussions inevitably involve international data protection measures. With the adoption of the General Data Protection Regulation in the EU, many Korean companies with a global presence are updating their privacy policies to comply with the GDPR.

33 Restrictions on disclosure

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

Under the PIPA, when PII is being transferred to another party due to a merger or business transfer, the PII processor is required to notify the data subject in advance of such transfer, together with the relevant information pursuant to the procedures set out in the Enforcement Decree of the PIPA. The Network Act has similar restrictions.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under the PIPA, in order to provide PII to a third party outside 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 storage and use of PII by the recipient; and
- the right of the data subject to refuse consent to transfer and, in the event there are any disadvantages arising from such refusal, the details of such disadvantage.

A PII processor cannot enter into a contract for overseas transfer of PII in violation of these restrictions under the PIPA. Note, however, that no consent is required when PII is being provided to a third party outside of Korea for the purpose of delegating PII processing.

Under the Network Act, an information communication service provider must obtain consent both for the provision of information to a third party and for the delegation of PII processing to a third party. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied.

35 Notification of cross-border transfer

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

36 Further transfer

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

Not applicable.

Rights of individuals

37 Access

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 PIPA, a data subject can request a PII processor for access to the PII being processed. Upon such request from the data subject, 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 cause for delay in granting the data subject access, the PII processor can extend the time-frame by notifying the data subject of such 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.

38 Other rights

Do individuals have other substantive rights?

Under the PIPA, an individual 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. Further, the data subject can require the PII processor to suspend processing of his or her PII.

39 Compensation

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, the court can order payment of damages up to three times the amount of the damages incurred.

40 Enforcement

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

Both. The rights of data subjects under the PIPA can be exercised through litigation in court or by filing a request for corrective orders with regards to a PII processor's infringement of the data subject's legitimate rights.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

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

No further provisions.

Supervision

42 Judicial review

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

43 Internet use

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

There are no specific statutory provisions that deal with cookies or equivalent technology. Nonetheless, cookies can be viewed as PII in certain circumstances.

JIPYONG JIPYONG LLC

Seung Soo Choi **sschoi@jipyong.com**
Seungmin Jasmine Jung **smjung@jipyong.com**

10F, KT&G Seodaemun Tower
60 Chungjeong-ro
Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1759/+82 2 6200 1712
Fax: +82 2 6200 0812
www.jipyong.com

Under the Network Act, an information communication service provider is required to include in its PII processing policy terms regarding the installation, operation and rejection of devices that automatically collect PII, such as internet connection record files. Such a PII processing policy should be disclosed to its users in an easily accessible manner according to the requirements of the Enforcement Decree to the Network Act.

44 Electronic communications marketing

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

Under the Network Act, in order to distribute marketing information for commercial purposes through electronic transmission, the express prior consent of the recipient is required. In the following cases, however, such 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 where his or her PII was collected and makes solicitations over the telephone.

45 Cloud services

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 out the standards for quality, performance and data protection (including physical, technical and organisational measures) and issue a recommendation to cloud service providers to comply with such standards.

Under the Cloud Computing Act, a cloud service provider cannot disclose a user's information to a third party nor 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.

Getting the Deal Through

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
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
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
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
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
Loans & Secured Financing
Mediation
Merger Control
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
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-Private Partnerships
Public Procurement
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
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-010-0