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

Serbia

Bogdan Ivanišević and Milica Basta
BDK Advokati

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?

The Personal Data Protection Act 2008 (DP Act), governs the collection and use of PII. Serbia is not an EU member, but the DP Act has adopted some of the basic principles of the Data Protection Directive.

Sectoral laws also apply to PII processing in particular areas (see questions 6 and 7).

2 Data protection authority

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

The Serbian data protection authority responsible for overseeing the implementation of the DP Act is the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner).

In the performance of its tasks, the Commissioner has the right to access and examine:

- PII and PII files;
- all documents relating to collection of PII and to other processing activities, as well as to the exercise of the rights of the individual;
- PII owners' general enactments; and
- premises and equipment that the PII owners use.

As a supervisory authority, the Commissioner has the power to supervise PII owners by means of inspections. The inspectors act upon information acquired ex officio or received from complainants or third parties.

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 Commissioner has an explicit obligation to cooperate with data protection authorities from other countries. The DP Act does not give further details on the manner of cooperation or a mechanism to resolve different approaches.

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?

Breaches of the DP Act, established in the process of supervision, may result in an issuance of warnings or orders by the Commissioner. When the Commissioner detects a breach, he or she may:

- order the rectification of the irregularity within a specified period of time;
- temporarily ban the processing carried out in breach of the provisions of the DP Act; or
- order deletion of the PII collected without a proper legal basis.

Some of the breaches of law are set out as misdemeanours for which the DP Act prescribes fines. The Commissioner is authorised to initiate misdemeanour proceedings, while misdemeanour courts conduct the proceedings and impose sanctions.

There are also criminal penalties for unauthorised collection of personal information. The penalties are not prescribed in the DP Act, but in the Criminal Code (article 146), and ordinary courts are in charge of imposing them.

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?

In general, the DP Act covers all sectors and types of organisation, as well as areas of activity. As a partial exception, the DP Act does not apply to political parties, organisations, trade unions and other forms of associations who process PII pertaining to their members, provided that the member has waived in writing the application of specified provisions of the Act for a specified period of time not exceeding the termination of his or her membership.

In addition, most of the provisions of the DP Act do not apply to journalists and other media operatives when they process PII for the sole purpose of publishing the information in the mass media. The law fully applies, however, to the processing of PII for advertising purposes.

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 DP Act is an 'umbrella regulation' in the field of PII protection in Serbia. Therefore the general principles set out in the DP Act apply to all forms of PII processing, including interception of communications, electronic marketing, and monitoring and surveillance of individuals. There are also sectoral laws regulating PII processing in these fields. For example, the Electronic Communications Act 2010 regulates interception of communications, while the E-commerce Act 2009 regulates electronic marketing. Comprehensive regulation of the monitoring and surveillance of individuals is still missing.

7 Other laws

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

The following laws provide for specific data protection rules:

- Patients' Rights Act 2013 on the obligation of health professionals to keep the patients' PII confidential;
- Labour Act 2005 on PII processing within the employment sector. The law provides for the right of employees to access the PII held

by their employer and to have specific parts of their PII corrected or erased;
- Labour Records Act 1996 on collecting and keeping the PII in the employment sector;
- Healthcare Documentation and Healthcare Records Act 2014 on collecting and keeping the PII in the healthcare sector;
- High Education Act 2017 on PII processing within the sector of higher education;
- Education System Act 2017 on PII processing within the education sector. The processing includes collecting and keeping the PII of pupils, parents, teachers and other employees;
- Pension and Disability Insurance Act 2003 on collecting and keeping PII within the sector of pension and disability insurance;
- Health Insurance Act 2005 on collecting and keeping PII within the health insurance sector; and
- E-Commerce Act 2009, Consumer Protection Act 2014 and Advertising Act 2016 on obtaining consent for direct marketing targeting the consumer.

8 PII formats

What forms of PII are covered by the law?

The DP Act covers all forms of PII. It defines personal data as 'any information relating to a natural person, regardless of the form in which it is manifested or the medium used (paper, tape, film, electronic media, and similar)'.

9 Extraterritoriality

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

The DP Act applies to all PII owners, users and processors who process PII in the territory of the Republic of Serbia, regardless of where they have been established or where their seat is.

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?

The DP Act covers all forms of use or other processing of PII. The Act defines PII processing as any action taken in connection with the information, including: collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, as well as other actions carried out in connection with the PII, regardless of whether such actions are automated, semi-automated, or carried out otherwise.

There is a statutory distinction between those who own PII and those who process PII on behalf of the owners. The former have the status of 'data controllers' and are entirely responsible for PII. They are in charge of establishing and maintaining PII processing records, notifying the Commissioner of their intent to establish a PII file, registering a PII file with the Central Data Filing System Register, responding to individuals' requests to access the PII, and so on. The latter have the status of 'data processors' and are responsible for processing the entrusted PII properly, in accordance with law or contract provisions, and also for the implementation of adequate security measures.

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?

The processing has to be grounded in either a statutory provision or the data subject's consent. The consent must be given in a proper form (ie, in writing or orally on the record).

12 Legitimate processing – types of PII

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

The DP Act has strict requirements concerning the processing of 'particularly sensitive data', defined as PII relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, status of a victim of violence, criminal record and sex life. Only the data subject's consent may constitute legal basis for the processing of particularly sensitive PII. The form of the consent, as prescribed by the DP Act, is more stringent than the form of consent for the processing of other types of PII. Exceptionally, PII relating to political party affiliation, health status or receipt of social support may be processed without consent, if a law permits it. Processing of particularly sensitive PII must be specially marked and protected by safeguards.

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?

The PII owner has to inform individuals on all relevant aspects of the PII processing. The notice, as a rule, has to be provided before the PII is collected and has to contain information about:
- the name and address or business name of the PII owner or the identity of another person responsible for PII processing (if any);
- the purpose of PII collection and the subsequent processing;
- the manner in which the PII will be used;
- the identity or categories of the users of the PII;
- the mandatory nature of, and the legal basis for, the processing; or, conversely, the voluntary nature of providing the PII;
- the individual's right to withdraw his or her consent to the processing and the legal consequences in the event of a withdrawal (the individual should compensate the PII owner for any reasonable costs and damages caused by the withdrawal);
- the individual's rights in the case of unlawful processing (eg, the right to request deletion of PII and suspension of the processing); and
- any other information, which, if withheld, could be considered contrary to 'conscientious practice'.

In addition, a PII owner who collects PII from a third party must inform the individual about it, without delay and in any event no later than at the time of the first processing.

14 Exemption from notification

When is notice not required?

Notice is not required when giving a notice would be impossible, evidently unnecessary, or unsuitable, especially if the individual has already been informed or the individual is unavailable. The Commissioner has provided little guidance on this issue.

When a PII owner collects PII from a third party, notice to the individual is not required if notification is impossible, unnecessary, or requires excessive use of time or efforts. Examples of when notification is unnecessary include the following:
- the individual has been already informed;
- the individual is unavailable; and
- a law provides for collection and processing of the PII obtained from a third party.

However, even in these cases the PII owner must notify the individual as soon as reasonably possible or, if the notification was evidently unnecessary, at the data subject's request.

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?

Individuals may control use of their PII by not consenting to the PII processing, as well as by exercising the right to access their personal information held by PII owners and other substantive rights (rectification, modification, update and deletion of PII) (see questions 37 and 38).

16 Data accuracy

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

The DP Act prescribes in a general manner that the processing of PII is impermissible if the information is inaccurate or incomplete, or if it is not based on a credible source or is out of date.

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?

The DP Act sets forth as one of its main principles that the amount of PII that may be processed has to be proportionate to the purpose of the processing. The Act does not prescribe any particular length of time during which the PII may be lawfully held, but the law indirectly imposes limits on the duration by forbidding further processing if the purpose of the processing has been modified or achieved.

18 Finality principle

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

The DP Act adopts the 'finality principle': the purpose of the processing of PII has to be clearly determined and permissible. As a rule, processing for the purposes other than those specified is not allowed.

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?

Personal information collected and processed for a particular purpose may also be processed for historical, statistical, or research and development purposes. In that case, the information has to be properly secured and cannot be used as a basis for rendering decisions or taking measures against the individual.

Security

20 Security obligations

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

The DP Act does not impose specific obligations on PII owners and other processors concerning data security, but provides for their general duty to undertake proper 'technical, human resources, and organisational measures to protect the data in accordance with established standards and procedures in order to protect data from loss, damage, inadmissible access, modification, publication and any other abuse'.

The DP Act stipulates that the government should enact a decree specifying protection measures for particularly sensitive PII. In the nine years since the implementation of the law, the government has not adopted such an act.

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?

The DP Act does not require PII owners to notify the Commissioner or the affected individuals of a data breach. The Commissioner has not issued any guidance in relation to this matter. The Electronic Communications Act (2010, as amended) states that an 'operator' (a person or entity carrying out or authorised to carry out electronic communications activities) must notify the Regulatory Agency for Electronic Communications and Postal Services of any breach of security and integrity of public communication networks or services affecting the operator's work, and especially of breaches that undermine the protection of personal data or impinge on subscribers' or users' right to privacy.

Internal controls

22 Data protection officer

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

The appointment of a data protection officer is not mandatory.

23 Record keeping

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

PII owners are required to establish and maintain PII processing records that contain relevant information on the categories of the PII, name of the PII file, types of the processing activities, purpose of the processing, among others. PII owners do not have to maintain such records if:

- PII is processed solely for family or other personal purposes and is unavailable to the third parties;
- PII is processed for the purpose of maintaining registers required by law;
- the PII file contains publicly available PII only; or
- PII relates to persons whose identity is not determined and the PII owner, processor or user is not authorised to determine such person's identity.

The Decree on the Form and Manner of Keeping Records of Personal Data Processing lays down the rules on the form that the processing records should take.

PII processors are not required to maintain internal records or establish internal processes or documentation.

24 New processing regulations

Are there any obligations in relation to new processing operations?

The only obligation in relation to new processing operations is to notify the Commissioner of the intended processing, so that the Commissioner may conduct a prior checking procedure and determine whether the processing would entail specific and significant risk for the rights and freedoms of data subjects. The data controller may not commence the processing operations until the prior checking procedure has been completed with the issuance of the Commissioner's approval.

Registration and notification

25 Registration

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

PII owners are required to notify the Commissioner of the intended processing of PII, as well as to register with the Commissioner the PII processing records (filing systems) and any subsequent change in the records. The Commissioner maintains the Central Data Filing Systems Register, which includes both the notifications and the PII processing records. The obligation to notify about the intended processing does not exist if a specific law determines the purpose of the processing, the categories of PII to be processed, the categories of users of the PII, and the period during which the PII will be held. In contrast, there are no exceptions to the obligation to register the PII processing records. PII processors do not have an obligation to register with the supervisory authority.

26 Formalities

What are the formalities for registration?

When PII owners submit to the Commissioner the PII processing records, the records have to include the information referred to in the response to question 23 (categories of PII, name of the PII file, types of processing activities, purpose of the processing, and other information).

There is no payable fee for registration. Registration is valid for an indefinite period of time, so it does not have to be periodically renewed.

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?

Under the DP Act, failure of the PII owner to register a data filing system or changes in the system within the required 15-day period constitutes a misdemeanour. The fine ranges from 50,000 to 1 million Serbian dinars for PII owners with the status of legal entities, and from 20,000 to 500,000 Serbian dinars for entrepreneurs. The fine for a natural person is 5,000 to 50,000 Serbian dinars. The same penalty applies to the responsible officer of a legal entity, state agency, or a governing body of the territorial autonomy or local self-government.

28 Refusal of registration

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

The Commissioner may decide, when reviewing the notification files, that conditions for a lawful processing of PII are not met owing to a lack of statutory basis for the processing or lack of consent, impermissible or undetermined purpose, impermissible means of processing, inadequacy of the PII for the achievement of the purpose, disproportionate amount or categories of the PII, or non-truthfulness or incompleteness of the information. If the prior checking results in a positive finding, the Commissioner has to allow an entry on the register.

29 Public access

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

The Central Data Filing System Register is publicly available on the official site of the Commissioner, at www.poverenik.rs/registar/index.php?lang=yu. The information on the site is in Serbian only. Upon request of the PII owner, the Commissioner may deny general access to the details about the filing system, if this is necessary for the achievement of a prevailing interest of national or public safety, national defence, performance of tasks by public authorities, or financial interests of the state, or if a law or other type of regulation provides for confidentiality of the information in the filing system.

30 Effect of registration

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

The main purpose of an entry on the Central Data Filing Systems Register is to ensure transparency of the PII processing. That is, to make the information about the filing systems and the PII owners available to the general public.

31 Other transparency duties

Are there any other public transparency duties?

There are no other public transparency duties.

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?

There are no specific provisions regulating the transfer of PII to entities providing processing services to the PII owners. Under the DP Act, 'data processor' is a subject to whom the PII owner delegates certain processing-related activities on the basis of a law or contract.

Update and trends

The DP Act is in the process of being changed. The new Act will mirror the provisions of the GDPR, as Serbia is a candidate for membership of the EU. The Ministry of Justice prepared the new Act in November 2017, and Parliament is expected to adopt a new law by the end of 2018.

33 Restrictions on disclosure

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

PII owners may disclose the PII to other recipients (PII users) only on the basis of a statutory provision or consent of the data subject. The purpose of the disclosure must be legitimate.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The cross-border transfer of PII from the Republic of Serbia to a country that is party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is not restricted nor subject to any authorisation. In a case of this kind, lawful processing of PII is the sole condition that PII owners have to meet in order to transfer the information lawfully. On the other hand, for cross-border transfer to countries that are not parties to Convention 108 and to international organisations, it is necessary to obtain prior approval from the Commissioner.

35 Notification of cross-border transfer

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

Prior approval from the Commissioner is necessary for cross-border transfers of PII to countries not parties to Convention 108 and to international organisations. In such cases, PII owners have to submit requests to the Commissioner, designating the PII filing systems they intend to transfer, the countries or international organisations to whom they want to transfer the PII, the identity of the subject abroad to whom they want to transfer the PII, and other relevant information about the transfer. The PII owners also have to submit copies of the transfer agreements with the importers. The Commissioner then assesses the safeguard measures and other relevant circumstances of the intended transfer, and issues a decision. The procedure may take any time from a few months to one year, or even more.

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?

There are no specific provisions regulating further transfers of PII. However, according to the recent practice of the Commissioner, such transfers do not require prior approvals.

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.

Individuals have the right to be accurately and fully informed about the processing of their PII, the right to access the PII and the right to obtain a copy of the PII. In order to exercise these rights, the individual must submit a request to the PII owner, in the form prescribed by the DP Act. Restrictions on the enjoyment of the rights include the situation in which the individual requests information pertaining to the PII already in the public domain, whether in public registers or otherwise, and the situation in which the individual abuses his or her rights.

38 Other rights

Do individuals have other substantive rights?

Upon obtaining access to the PII, individuals have the right to require from the PII owners to correct, modify, update or delete the PII. They also may require suspension of the processing.

Individuals have the right to require deletion of their PII when:

- the purpose of the processing is not clearly specified;
- the purpose of the processing has changed and requirements for processing with the different purposes are not met;
- the purpose of the processing has been achieved or the PII is no longer needed for such purpose;
- the PII is processed by impermissible means;
- the scope or type of the PII processed is disproportionate to the purpose of the processing;
- the PII is inaccurate and it is not possible under the circumstances to replace it with accurate PII by means of a correction; or
- the PII is processed without consent or statutory authorisation.

Individuals may obtain suspension of the processing if they successfully contest how accurate, complete or up to date the PII is. Pending a decision on the challenge, individuals may obtain designation of such PII as contested.

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 Obligations Act (1978), which contains general provisions on indemnity for torts, individuals are entitled to compensation of damage caused by violations of their right to protection of PII. PII owners may be liable both for actual damage and for moral damage (injury to feelings).

40 Enforcement

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

If the PII owner rejects or denies the individual's request for exercising his or her rights, fails to decide on a request within the specified time limit, as well as in other cases prescribed by the DP Act, the individual may lodge a complaint with the Commissioner. The Commissioner issues a ruling, which may be challenged in administrative proceedings before the Administrative Court.

Damages must be brought to a civil court.

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.

Not applicable.

Supervision

42 Judicial review

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

PII owners can appeal to the Administrative Court against orders of the Commissioner.

Specific data processing

43 Internet use

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

The Electronic Communications Act provides that the PII owner can store cookies on the individual's terminal equipment if the individual is provided with clear and comprehensive information about the purpose of the collection and processing of PII and given an opportunity to refuse such processing.

There have been no authoritative rulings by the Commissioner or the courts as to adequacy of the specific modes of cookie notification.

44 Electronic communications marketing

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

The E-commerce Act 2009 states that unsolicited commercial messages may be sent via email to individuals only if individuals have given their prior consent to such types of marketing.

45 Cloud services

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

There are no specific provisions in the legal system of the Republic of Serbia regulating cloud computing services.

BDK Advokati
Belgrade • Podgorica • Banja Luka

Bogdan Ivanišević **bogdan.ivanisevic@bdkadvokati.com**
Milica Basta **milica.basta@bdkadvokati.com**

Bulevar kralja Aleksandra 28
Belgrade 11000
Serbia

Tel: +381 11 3284 212
Fax: +381 11 3284 213
www.bdkadvokati.com

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