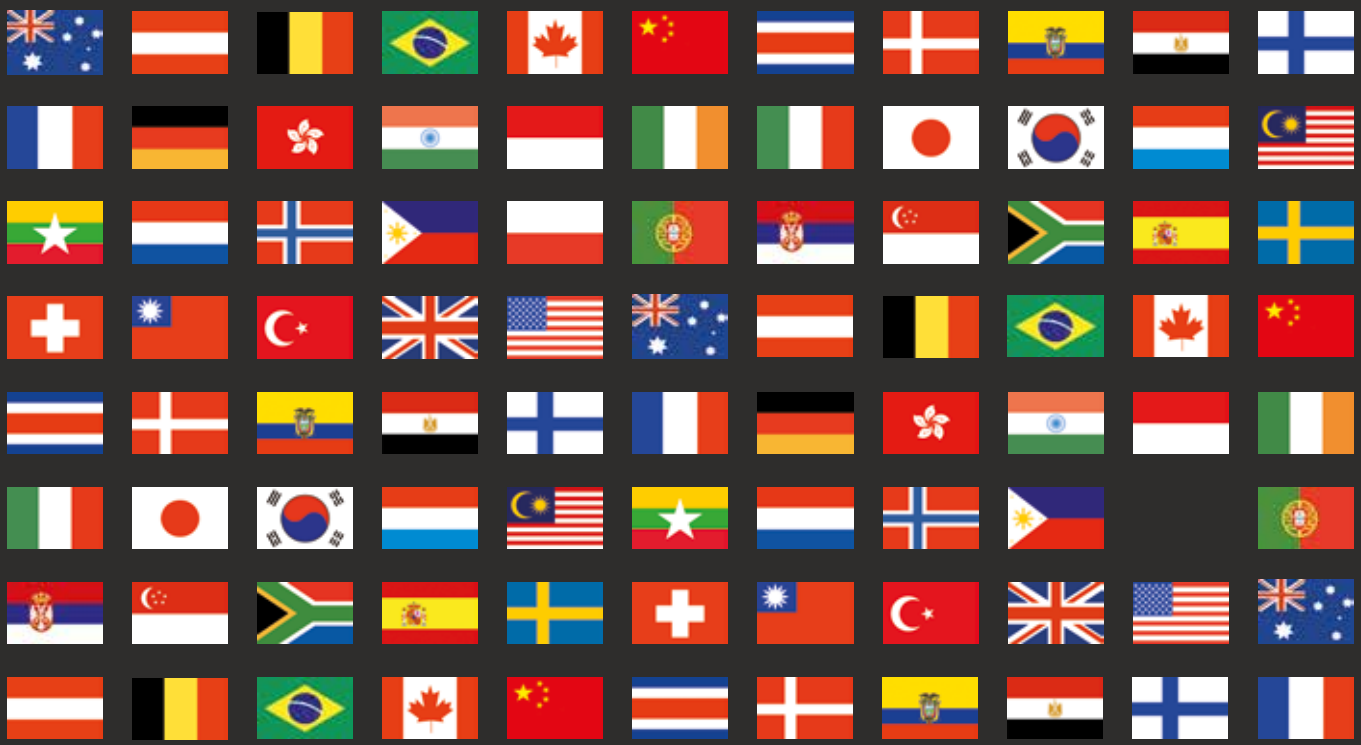
Private M&A

Contributing editors
Will Pearce and John Bick



2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Private M&A 2019

Contributing editors

Will Pearce and John Bick
Davis Polk & Wardwell LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in October 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 2017
Second edition
ISBN 978-1-78915-055-1

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

CONTENTS

Preface

Private M&A 2019

Second edition

Getting the Deal Through is delighted to publish the second edition of *Private M&A*, 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 Brazil, Costa Rica, Ecuador, Egypt, Indonesia, Malaysia, Myanmar, Philippines, Singapore 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, Will Pearce and John Bick of Davis Polk & Wardwell, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
September 2018

Data privacy and cybersecurity in global dealmaking

Pritesh Shah and Daniel Forester
Davis Polk & Wardwell LLP

Over the years, data privacy and cybersecurity concerns have risen from the depths of being an industry- and deal-specific concern to requiring consideration in every deal. While sufficiently complicated in any given jurisdiction, increasingly global deals are forcing buyers and sellers to confront these issues directly commencing at the deal-structuring stage, through diligence, ultimate risk allocation and post-closing integration activities. The last year has only solidified the recognition and importance of these issues as developments in the data privacy landscape have made front-page news, ranging from the effectiveness of the European Union's General Data Protection Regulation (GDPR) to the role played by and influence of organisations like Cambridge Analytica.

Regulatory and legal developments

Whether the consequences are primarily reputational or felt immediately at the negotiating table, the upshot remains that all parties to a deal must be cognisant of the implications of an evolving data security and privacy landscape. In the US, while holistic data security and privacy regulations have been slow to emerge at a federal level, states such as California have been aggressive in leading the way with broad legislation similar to that in the EU. One of the most anticipated data security and privacy regulations to date, the GDPR, came into effect 25 May 2018 in the EU and has changed the compliance landscape with its extraterritorial scope, weighty obligations and significant penalties.

California's Consumer Privacy Act of 2018

Unlike the EU, the US has not yet implemented a comprehensive, federal data security and privacy regulatory framework. Recent trends, however, have seen states take the lead on enacting significant legislation that impacts corporations looking to conduct business within certain jurisdictions or with citizens of those jurisdictions. One such instance was the enactment on 28 June 2018 of the California Consumer Privacy Act (CCPA) of 2018. The CCPA provides many consumer protections and compliance obligations reminiscent of the GDPR. Although it excludes publicly available information, the CCPA adopts a particularly broad definition of 'personal information' that sweeps in the information of any Californian residents that 'identifies, relates to, describes, is capable of being associated with, or that could reasonably be linked, directly or indirectly, with a particular consumer or household'.

Effective January 2020, the CCPA provides, among other things, certain 'rights to be forgotten', including the requirement that businesses must delete personal information upon request if such information is not necessary for a specific business purpose, legal compliance, or other expected internal uses. The CCPA also establishes a consumer right to request from businesses details about collected information, the purpose for such collection and third parties with whom the information has been shared. Furthermore, a consumer may request that businesses provide disclosures regarding sale of consumer data as well as an opt-out from such sale without discriminating against those who exercise the option.

While the CCPA is limited in application to businesses above certain revenue thresholds or whose business model involves transacting in the personal information of its consumers, the law will reach international entities with sufficient exposure to California residents and researchers have estimated that it will apply to over 500,000 companies in the US alone. Furthermore, the CCPA provides exemptions for de-identified and aggregated data that cannot reasonably be linked to the underlying individuals, as well as exemptions for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and certain other legal regimes.

Non-compliance with the CCPA presents a severe risk to businesses, allowing a private right of action for Californian residents, whether individually or through class actions, with statutory penalties between US$100 and US$750 per individual per incident or injunctive or declaratory relief without a requirement for the individual to prove actual harm. The California Attorney General is also empowered under the CCPA to pursue enforcement against business for penalties of up to US$7,500 for each intentional violation of the CCPA. Additionally, penalties of up to US$2,500 may be imposed for any violation of the CCPA that has not been cured within 30 days of notice of any alleged non-compliance. The CCPA is not clear regarding whether each violation, as used in calculation of damages for the California Attorney General, is on a per individual per incident basis or simply a per incident basis. An amendment to the law or further regulatory guidance on this distinction will be crucial in evaluating a business's risk of non-compliance.

The EU's GDPR

Discussed in greater length further below, the GDPR became effective on 25 May 2018. The GDPR governs the processing of personal data by data 'controllers' and 'processors'. A data controller is a person or entity who determines the purposes and means of the processing of personal data. A data processor is a person or entity who processes personal data on behalf of the data controller. Under the GDPR, the terms 'processing' and 'personal data' are defined broadly enough to capture essentially any activity performed on data related to an individual. Specifically, the definition of 'personal data' covers 'any information relating to an identified or identifiable natural person ('data subject')' and 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. Processing of personal data subject to the GDPR must be done lawfully, fairly and in a transparent manner and personal data may be collected only for a specified, explicit and legitimate purpose.

Among other operational, contractual, governance and notification obligations on data controllers and processors discussed below, the GDPR provides that controllers must implement 'appropriate technical and organizational [security] measures' for data protection and may use only processors who provide 'sufficient guarantees' to implement such measures. The GDPR also provides data subjects with certain rights with respect to their personal data, including, among others, the right to demand prompt erasure of any personal data collected (the 'right to be forgotten'), the right to withdraw consent for or object to the processing of personal data, the right to restrict processing of personal data and the right to obtain the identities of third parties to whom their personal data is being disclosed.

Complying with data transfer requirements

The various data security and privacy regulatory regimes upped the ante with respect to the technical measures companies need to implement for compliance purposes as well as the rights afforded to consumers whose data has been collected. In addition to these obligations, one of the most impactful trends when it comes to M&A has been data transfer restrictions, in particular in the EU, China, Russia and certain other jurisdictions. To the extent that a target has activities in those jurisdictions, appropriate consideration will be due with respect to whether personal data in those jurisdictions can be transferred out of the jurisdiction at all, potentially complicating business consolidation goals.

For example, under the GDPR in the EU, personal data can generally be transferred out of the European Economic Area only if the recipient jurisdiction has been deemed adequate by the European Commission. Absent such a determination (which the US has not obtained), another appropriate safeguard or derogation will be required and may complicate the data transfers process. Impermissible transfers are subject to the higher tier of fines under the GDPR, up to the larger of 4 per cent of global annual revenue or €20 million.

Impact on M&A transactions

For a well-advised purchaser or seller in an M&A transaction, the evolving landscape of data security and privacy necessitates understanding the impact these regulatory regimes have on risk allocation, structure and business flexibility.

In particular, parties to an M&A transaction need to be mindful of:

- the extended jurisdiction of the GDPR encompasses companies with establishments in the EU as well as companies, regardless of domicile, that process the personal data related to the offering of goods or services to data subjects in the EU;
- the risk of substantial fines based on global revenue increases the importance of conducting thorough due diligence on a target's compliance with data protection laws; and
- transaction structuring and risk allocation mechanisms should expressly contemplate data protection to ensure compliance, and allocate the risk of non-compliance, with the GDPR.

Due diligence

Purchasers and investors should first consider whether the target's data processing is subject to the GDPR. Under the GDPR, processing of personal data is defined broadly to include nearly any act that is performed on personal data, including collection, organisation, storage, use, and even the destruction of personal data. The GDPR covers processing of personal data that (i) occurs in the context of the activities of an establishment in the EU, (ii) is related to the offering of goods or services, regardless of whether payment is required, to individuals in the EU, or (iii) is related to the monitoring of individuals' behaviour in the EU. The 'offering of goods or services' may be broadly construed and depends on 'factors such as the use of a language or a currency generally used in one or more member states with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the [European] Union'. As a result, the GDPR may apply to companies that do not have substantial EU activities and have not previously focused on EU data privacy laws.

Practice tips

- Do not rely on the target's explanation that it does not have material EU operations. Go beyond diligence questions and investigate the company's online presence, including whether visitors to the target's website from the EU are provided with local language or shipping options.
- If the target appears to be subject to the GDPR, consider whether the purchaser will have access to personal data as part of diligence or in the data room. If so, the purchaser could be subject to the GDPR as well and non-disclosure agreements may need to be tailored accordingly. Unless necessary, some purchasers may prefer to affirmatively exclude any personal data from the data room or diligence process to avoid being subject to the GDPR.
- For sellers, anticipate purchaser GDPR questions and consider practicing diligence responses with outside counsel to prepare for calls. Given the uncertainties regarding interpretation and enforcement, perfect confidence in GDPR compliance is unlikely to be expected, but being able to conversantly discuss the topics will give purchasers comfort that the issue is being thoughtfully considered.

To the extent that a company may be subject to the GDPR, a purchaser may need to re-evaluate and reorient the target's data processing activities after the transaction. Such review may look into the process by which the company obtains 'freely given, specific, informed and unambiguous' consent from individuals, the company's use of the data and whether it is consistent with the GDPR's data processing principles, and the support of data subjects' rights (including the right to access, rectification, erasure (the 'right to be forgotten') and portability). Under the GDPR, companies must maintain records of their processing activities, including the purposes of the processing, a description of the categories of data subjects and personal data, the categories of recipients, duration of processing, third-country transfers and general descriptions of the applicable technical and organisational security measures.

Practice tips

- The target's records of processing activities will often be a good starting point to approach the key questions, including: (i) whose personal data is being processed? What kind of personal data is being processed? For what purpose? For how long? Is data transferred to other parties? Is data transferred out of the EU? And what security measures are in place?

Careful diligence should be conducted on the target's contracts with third parties that are processing data on its behalf, as amendments may be necessary to conform to the GDPR's requirements that such contracts contain specific provisions relating to the processing of personal data. Under the GDPR, the transfer of personal data outside the EU may typically be made only to countries where the European Commission has determined that the country has an adequate level of protection for personal data. Absent such an adequacy determination (and the US has not been deemed adequate), transfers may be made only on the basis of (i) implementation of appropriate safeguards or (ii) enumerated derogations. Diligence should be conducted with a focus on the existence of such transfers of data outside the EU (which, in the case of a US target, may be likely absent local servers) and the applicable justifications for such transfers.

In addition to heightened obligations regarding the processing of personal data, the GDPR also imposes an affirmative requirement for companies to implement appropriate technical and organisational measures to ensure a level of data security appropriate to the risks presented by the nature, scope, context and purposes of the company's data processing and to ensure such measures are taken by a company's third-party processors as well.

The GDPR also institutes the strictest data breach notification obligations of any generally applicable cybersecurity law. Companies must notify their 'competent supervisory authority' '...without undue delay and, where feasible, not later than 72 hours' after becoming aware of a data breach. For particularly egregious breaches, a company may also be required to notify the affected individuals. Whether notification is required or not, the company is required to maintain a breach register and document all breaches – the related facts, effects and remedial action taken – subject to verification by the supervisory authority. During diligence, requesting a copy of the target's breach documentation is prudent. If the target does not maintain a record of breaches then it may be operating in violation of applicable law and further diligence may be required to identify whether the target has suffered data breaches that may present future regulatory or litigation risk. Breach-related documentation may also be scrutinised for insight into the target's data breach remediation procedures and approach to risk management and compliance.

Practice tips

- GDPR compliance will not be satisfied – or considered properly covered by due diligence measures – by a check-the-box approach. Request a copy of the company's latest data map. The company will need to be able to provide it to a regulator on short notice and if it does not have one ready it may be a sign of an overall lax approach towards compliance.
- Companies outside of the EU may benefit from building direct relationships, typically through their data protection officer, with

appropriate data protection authorities in the EU to facilitate a smoother notification process, as a single data breach may trigger notification obligations in the US as well as the EU.
- For sellers, pre-empt onerous document requests by proactively providing high-level summaries of the target's personal data practices.

Non-compliance with the GDPR presents a serious risk. Relevant data authorities are empowered under the GDPR with broad investigatory and corrective powers. These include the power to compel companies to provide whatever information may be required to evaluate compliance with the GDPR and conduct data protection audits, including obtaining access to a company's premises. The corrective powers include injunctive relief (including modifying a company's data processing processes, forcing a company to provide notice of a data breach to a data subject or imposing a temporary or permanent ban on data processing) and the ability to impose administrative fines. Administrative fines under the GDPR are not merely compensatory for loss suffered by a data subject, but are rather structured to be 'effective, proportionate and dissuasive'. The GDPR provides limits to the administrative fines of up to the greater of €20 million or 4 per cent of global annual revenue for violations of core substantive requirements (including with respect to the GDPR's principles for processing, conditions for consent, data subject's rights, and international transfers of data). For more procedural violations, there is a lower threshold of the greater of €10 million or 2 per cent of global annual turnover.

With the recent implementation of the GDPR, business and legal communities are anxiously awaiting the first few enforcement actions to judge how and at what level these administrative fines will be levied.

Practice tips
- Investigate the company's history of cooperation with data privacy regulators in the EU, and its past handling of data breaches. A history of regulator cooperation may help mitigate future fines.
- Carefully probe the company's personal data retention practices with an eye towards confirming that the company only retains personal data as necessary.

Valuation considerations

Should the GDPR apply, consider (i) how consistent the valuation model is with the scope of the company's ability to use its personal data, (ii) the potential costs to bring the business into compliance with the GDPR from an operational, contractual and governance perspective, and (iii) reputational and financial risks associated with GDPR non-compliance.

One of the GDPR's core principles is the purpose limitation, which binds companies to the specified, explicit and legitimate purposes communicated to data subjects when their personal data is collected. Further processing beyond the original communicated purposes is allowed only to the extent that such processing is not incompatible with the original purpose. If the purchaser's valuation model relies on different or expanded use of the target's database of personal data, a purchaser may need to communicate a new privacy statement to each data subject and, in certain instances, obtain affirmative consent in order to be compliant. The cost and time associated with this exercise may impact the purchaser's business plan as the GDPR may require affirmative consents that may not be satisfied by, for example, simply updating a privacy policy on a website.

Practice tips
- Push financial modellers on their models and assumptions and communicate personal data-related assumptions to legal and business teams to focus on during diligence.
- For sellers, update privacy policies or obtain appropriate consent before the transaction to ensure that the company's database of personal data may be transferred in connection with a merger or similar transaction.

The implementation of certain operational, governance and contractual measures prescribed by the GDPR, including those described above, may impose additional financial costs. For instance, in a scenario where the acquisition expands the data processing activities of the target to constitute large-scale, regular and systematic monitoring of data subjects, the appointment of a data protection officer may be required. The company may also need to implement extensive documentation processes and conduct data protection impact assessments. This would be in addition to amending its existing contractual arrangements with third parties (which, beyond the diversion of resources, may require additional consideration) and the implementation of appropriate data protection measures. The total costs of such measures could be significant.

Practice tips
- The diligence gap analysis should include a review of technical cybersecurity and physical security operations as well as an appreciation of the headcount of the company's data privacy compliance function. IT upgrades can be a significant expense and, if the compliance function is understaffed, additional resources may be required.

Non-compliance with the GDPR risks severe financial and reputational harm. As discussed above, administrative fines for non-compliance can be punitive and the indirect costs of dealing with a data breach can also be significant, involving third-party costs of investigation and remediation (and may involve notifications and credit monitoring, where applicable). Reputational harm associated with a data breach can be even more problematic for companies that rely heavily on consumer trust.

Practice tips
- Nearly every company faces actual or attempted data security breaches with regularity. The more important question is whether the target company is aware of these attempts and taking measures to ensure its data is as secure as reasonably possible. Do not limit diligence to the target's legal staff; also speak with the chief information officer regarding penetration testing, patch and logging procedures, and the target's information security and breach response plans.
- For sellers, if the company has a history of data breaches, carefully summarise the scope of the breaches, the company's responses and any material impacts on the business.

Acquisition agreements

Prudent purchasers and investors are factoring GDPR compliance into their acquisition agreement structuring and risk allocation mechanisms. If the transaction is structured as an asset purchase, particular care will be needed to determine whether the transfer of the target's databases itself may violate the GDPR (eg, by exceeding the scope of the applicable consent or by transferring data outside of the EU to a jurisdiction that has not been deemed adequate by the European Commission). Covenants may be appropriate to ensure continued compliance (or development of a compliance programme) or notification of any new breaches between signing and closing the transaction. Risk allocation provisions should also be thoughtfully negotiated to ensure appropriate excluded liability, representation and indemnity coverage. Representations regarding compliance with law are insufficient to fully address data privacy risks and should be expanded to cover data-privacy related contract provisions, industry standards and practices, and existence and handling of data breaches. Representations to consider also include:
- operation in accordance with the company's written privacy policy;
- provision of all applicable privacy and cybersecurity policies;
- absence of written notices regarding related investigations;
- existence of a commercially reasonable information security programme;
- absence of restrictions with respect to target's successors' rights to use, sell, license, distribute, and disclose personal data; and
- absence of data security breaches, loss of data, and unauthorised disclosures of personal sensitive information.

Practice tips
- In an asset deal, consider making GDPR non-compliance an excluded liability. Include not only pre-closing operations, but also a reasonable period of time post-closing so that the purchaser has a covered window to bring the business into compliance.
- Depending on the duration between signing and closing, consider adding a covenant for the target to bring itself into compliance with

the GDPR before closing. Purchasers that are operating companies with their own robust privacy programmes may instead prefer to simply onboard the target as part of post-closing integration.

- To the extent possible as part of the larger deal dynamic, indemnities backing the related representations should be uncapped or subject to limitations of liability sufficiently high to cover the GDPR's global revenue-based fines.
- If a purchaser is planning to rely on representation and warranty insurance, ensure that data privacy is not on the list of exclusions and carefully discuss with outside counsel the extent to which data privacy diligence should be conducted (as known liabilities are typically excluded from the scope of coverage, regardless of whether they are ultimately disclosed as part of the transaction agreement). Also keep in mind that representation and warranty insurance, which is often capped at 10 per cent of purchase price in the US, may be insufficient to cover fines under the GDPR.

Post-closing

The post-closing process of transferring and integrating data can last for up to several years, especially if the acquisition involves a business carve-out with related transitional services arrangements. During this period, either the seller or the purchaser may be required to continue data processing for the other. In these cases, the GDPR may require the incorporation of specific contractual provisions between the parties in the applicable transitional services agreement, whether structured as a controller–processor or controller–controller relationship.

After the transaction, the purchaser may want to consolidate the target's data at the purchaser's existing data centers. If such transfers involve the movement of data outside the EU, specific measures must be complied with if the recipient country has not been deemed adequate with respect to the protection of personal data by the European Commission. The European Commission is in the process of negotiating additional adequacy determinations.

Conclusion

Although perhaps the most impactful to date, the GDPR remains just one instance, and likely only the beginning, of a broader global trend towards stricter and more comprehensive data privacy and cybersecurity regulation. As the implications of the GDPR and other such regulations may impact all phases of a deal, a well-advised party would do well to keep in mind such consideration starting in the deal-structuring stage, through diligence, ultimate risk allocation and post-closing integration activities.

Davis Polk

Pritesh Shah **pritesh.shah@davispolk.com**
Daniel Forester **daniel.forester@davispolk.com**

450 Lexington Avenue
New York, NY 10017
United States

Tel: +1 212 450 4000
Fax: +1 212 701 5800
www.davispolk.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 978-1-78915-055-1