

Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto



HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity



Keep the trust you've earned.

Complying with global privacy, data protection and cybersecurity rules is challenging, especially for businesses that operate across borders. Our top-ranked privacy team, in combination with the firm's Centre for Information Policy Leadership, advises on all aspects of US and European data protection law and cybersecurity events. We help businesses develop global compliance frameworks addressing regulatory obligations in the US, the EU and across the world. The firm is widely recognized globally as a leading privacy and data security firm.

For more information, visit www.huntonprivacyblog.com.

Publisher

Tom Barnes
tom.barnes@lbresearch.com

Subscriptions

Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager

Adam Sargent
adam.sargent@gettingthedealthrough.com

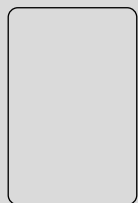
Published by

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

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between May and August 2020. Be advised that this is a developing area.

© Law Business Research Ltd 2020
No photocopying without a CLA licence.
First published 2012
Ninth edition
ISBN 978-1-83862-322-7

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



Data Protection & Privacy

2021

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

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

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

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

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

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

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



London
August 2020

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

Contents

Introduction	5	Germany	95
Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP		Peter Huppertz Hoffmann Liebs Fritsch & Partner	
EU overview	9	Greece	102
Aaron P Simpson, Claire François and James Henderson Hunton Andrews Kurth LLP		Vasiliki Christou Vasiliki Christou, Attorney at Law	
The Privacy Shield	12	Hong Kong	109
Aaron P Simpson and Maeve Olney Hunton Andrews Kurth LLP		Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown	
Australia	17	Hungary	118
Alex Hutchens, Jeremy Perier and Meena Muthuraman McCullough Robertson		Endre Várady and Eszter Kata Tamás VJT & Partners Law Firm	
Austria	25	India	126
Rainer Knyrim Knyrim Trieb Rechtsanwälte		Stephen Mathias and Naqeeb Ahmed Kazia Kochhar & Co	
Belgium	33	Indonesia	133
David Dumont and Laura Léonard Hunton Andrews Kurth LLP		Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Noor Prayoga Mokoginta AKSET Law	
Brazil	45	Italy	142
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados		Paolo Balboni, Luca Bolognini, Antonio Landi and Davide Baldini ICT Legal Consulting	
Canada	53	Japan	150
Doug Tait and Catherine Hamilton Thompson Dorfman Sweatman LLP		Akemi Suzuki and Tomohiro Sekiguchi Nagashima Ohno & Tsunematsu	
Chile	60	Malaysia	159
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya Magliona Abogados		Jillian Chia Yan Ping and Natalie Lim SKRINE	
China	67	Malta	166
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown		Terence Cassar, Ian Gauci and Bernice Saliba GTG Advocates	
Colombia	76	Mexico	174
María Claudia Martínez and Daniela Huertas Vergara DLA Piper		Abraham Diaz and Gustavo A Alcocer OLIVARES	
France	83	Netherlands	182
Benjamin May and Farah Bencheliha Aramis Law Firm		Inge de Laat and Margie Breugem Rutgers Posch Visée Endedijk NV	

New Zealand	190	Sweden	253
Derek Roth-Biester and Megan Pearce Anderson Lloyd Lawyers		Henrik Nilsson Wesslau Söderqvist Advokatbyrå	
Portugal	197	Switzerland	261
Helena Tapp Barroso and Tiago Félix da Costa Morais Leitão, Galvão Teles, Soares da Silva & Associados		Lukas Morscher and Leo Rusterholz Lenz & Staehelin	
Romania	206	Taiwan	271
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Laura Dinu MPR Partners Maravela, Popescu & Asociații		Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang Formosa Transnational Attorneys at Law	
Russia	214	Turkey	278
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian L Zimble Morgan Lewis		Esin Çamlıbel, Beste Yıldızlı Ergül and Naz Esen Turunç	
Serbia	222	United Kingdom	286
Bogdan Ivanišević and Milica Basta BDK Advokati		Aaron P Simpson, James Henderson and Jonathan Wright Hunton Andrews Kurth LLP	
Singapore	229	United States	296
Lim Chong Kin and Charis Seow Drew & Napier LLC		Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP	
South Korea	243		
Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim LAB Partners			

EU overview

Aaron P Simpson, Claire François and James Henderson

Hunton Andrews Kurth LLP

The EU General Data Protection Regulation (GDPR) became directly applicable in all EU member states from 25 May 2018 and in the European Economic Area European Free Trade Association member states (Iceland, Liechtenstein and Norway) in July 2018. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) dated 24 October 1995, and established a single set of rules throughout the EU, although EU member state data protection laws complement these rules in certain areas. The EU data protection authorities (DPAs) now gathered in the European Data Protection Board (EDPB) have published a number of guidelines on how to interpret and implement the new legal framework. This provides useful guidance to businesses on how to align their existing data protection practices with the GDPR.

Impact on businesses

The GDPR largely builds on the existing core principles of EU data protection law and expands them further while introducing new concepts that address the challenges of today's data-driven economy. In addition, the GDPR launches a new governance model that increases the enforcement powers of DPAs, enhances cooperation between them and promotes a consistent application of the new rules. The most significant concepts of the GDPR affecting businesses are outlined below.

Territorial scope

The GDPR is relevant to both EU businesses and non-EU businesses processing personal data of individuals in the EU. With regard to businesses established in the EU, the GDPR applies to all data processing activities carried out in the context of the activities of their EU establishments, regardless of whether the data processing takes place in or outside of the EU. The GDPR applies to non-EU businesses if they 'target' individuals in the EU by offering them products or services, or if they monitor the behaviour of individuals in the EU. Many online businesses that were previously not directly required to comply with EU data protection rules are now fully affected by the GDPR.

One-stop shop

One of the most important innovations introduced by the GDPR is the one-stop shop. The GDPR makes it possible for businesses with EU establishments to have their cross-border data protection issues handled by one DPA acting as a lead DPA. In addition to the lead DPA concept, the GDPR introduces the concept of a 'concerned' DPA to ensure that the lead DPA model will not prevent other relevant DPAs from having a say in how a matter is dealt with. The GDPR also introduces a detailed cooperation and consistency mechanism, in the context of which DPAs will exchange information, conduct joint investigations and coordinate enforcement actions. In case of a disagreement among DPAs with regard to possible enforcement action, the matter can be escalated to the European Data Protection Board (EDPB) for a final decision. Purely local complaints without a cross-border element can be handled by the concerned DPA at member state level, provided that the lead DPA has been informed and agrees to the proposed course of

action. In some member states, such as France, businesses will have to approach the DPA they consider as their lead DPA by filing a specific form for the designation of the lead DPA.

Accountability

Under the GDPR, businesses are held accountable with regard to their data processing operations and compliance obligations, and the GDPR includes a general accountability principle that requires controllers to be able to demonstrate their compliance with the GDPR's obligations. The GDPR also imposes a number of specific obligations on data controllers and data processors in this respect. Data controllers are required to implement and update – where necessary – appropriate technical and organisational measures to ensure that their data processing activities are carried out in compliance with the GDPR, and to document these measures to demonstrate such compliance at any time. This includes the obligation to apply the EU data protection principles at an early stage of product development and by default (privacy by design/default). It also includes the implementation of various compliance tools to be adjusted depending on the risks presented by the data processing activities for the privacy rights of individuals. Data protection impact assessments (DPIAs) are such tools, which will have to be conducted in cases of high-risk data processing, and certain other specified processing activities, such as those that involve processing of sensitive data on a large scale. Data processors are required to assist data controllers in ensuring compliance with their accountability obligations, including DPIAs, the implementation of appropriate security measures, and the handling of data subject rights requests. In addition, data controllers and data processors have to implement robust data security measures and keep internal records of their data processing activities, a system that replaces the previous requirement to register with the DPAs at member state level. Furthermore, in some cases, data controllers and data processors are required to appoint a data protection officer (DPO), for example, if their core activities involve regular and systematic monitoring of individuals or the processing of sensitive data on a large scale. The accountability obligations of the GDPR therefore require businesses to have comprehensive data protection compliance programmes in place.

Data breach notification

The GDPR introduces a general data breach notification requirement applicable to all industries. All data controllers now have to notify data breaches to the DPAs without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Delayed notifications must be accompanied by a reasoned justification and the information related to the breach can be provided in phases. In addition, data controllers have to notify affected individuals if the breach is likely to result in a high risk to the individuals' rights and freedoms. Businesses face the challenge of developing data breach response plans and taking other breach readiness measures to avoid fines and the

negative publicity associated with data breaches. Data processors are required to notify data controllers of personal data breaches, but do not have an independent obligation to notify DPAs or affected individuals.

Data processing agreements

The GDPR imposes minimum language that needs to be included in agreements with service providers acting as data processors. The GDPR requires, for example, that data processing agreements include documented instructions from the data controller regarding the processing and transfer of personal data to third countries (ie, outside of the EU), a requirement for the processor to implement appropriate data security measures, the possibility for the data controller (or a third party mandated by the data controller) to carry out audits and inspections, and an obligation to delete or return personal data to the data controller upon termination of the services. The new requirements for data processing agreements under the GDPR require many businesses to review and renegotiate existing vendor and outsourcing agreements. The EDPB and some DPAs (such as the French and Spanish DPAs) have developed template clauses to help businesses ensure compliance with those requirements.

Consent

Under the GDPR, consent must be based on a clear affirmative action and be freely given, specific, informed and unambiguous. Consent language hidden in terms and conditions, pre-ticked boxes or inferred from silence is not valid. Also, consent is unlikely to be valid where there is a clear imbalance of power between the individual and the data controller seeking the consent, such as in employment matters. Electronic consent is acceptable, but it has to be clear, concise and not unnecessarily disruptive. In the context of a service, the provision of the service should not be made conditional on customers consenting to the processing of personal data that is not necessary for the service. Further, the GDPR requires data controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent. Given the stringent consent regime in the GDPR, businesses relying on consent for their core activities should carefully review their consent practices.

Transparency

Under the GDPR, privacy notices must be provided in a concise, transparent, intelligible and easily accessible form to enhance transparency for individuals. In addition to the information that privacy notices already had to include under the previous regime, the GDPR requires that privacy notices specify the contact details of the DPO (if any), the legal basis for the processing, any legitimate interests pursued by the data controller or a third party (where the data controller relies on such interests as a legal basis for the processing), the controller's data retention practices, how individuals can obtain a copy of the data transfer mechanisms that have been implemented, and whether personal data is used for profiling purposes. When personal data is obtained from a source other than the individual concerned, the data controller must also inform individuals of the source from which the personal data originated and the categories of personal data obtained. In light of the volume of the information required, DPAs recommend adopting a layered approach to the provision of information to individuals (such as the use of a layered privacy notice in a digital context). These new transparency requirements require businesses to review their privacy notices.

Rights of individuals

The GDPR strengthens the existing rights of individuals and introduces additional rights. For instance, the GDPR strengthens the right of individuals to object to the processing of their personal data. In addition,

the GDPR enhances the right to have personal data erased by introducing a 'right to be forgotten'. This right applies when personal data is no longer necessary or, more generally, where the processing of personal data does not comply with or no longer complies with the GDPR. Furthermore, the GDPR introduces the right to data portability, based on which individuals can request to have their personal data returned to them or transmitted to another data controller in a structured, commonly used and machine-readable format. The right to data portability applies only with regard to automated processing based on consent or processing that is necessary for the performance of a contract. Businesses need to review their existing practices for handling individuals' requests and consider how to give effect to the new rights of individuals under the GDPR. Individuals may also have a right to restrict the processing of personal data in some circumstances, such as while the accuracy of personal data is verified by the data controller. When processing of personal data is restricted, the data controller may only:

- store the data;
- process the data to establish or exercise legal claims;
- protect the rights of another natural or legal person;
- process the personal data for reasons of public interest; or
- process the personal data for other purposes with the data subject's consent.

Data transfers

The GDPR maintains the general prohibition of data transfers to countries outside of the EU that do not provide an 'adequate' level of data protection, and applies stricter conditions for obtaining an 'adequate' status. The GDPR introduces alternative tools for transferring personal data outside of the EU, such as codes of conduct and certification mechanisms, although none have been approved by regulators to date. The previous contractual options for data transfers have been expanded and made easier; going forward, regulators may also adopt standard contractual clauses to be approved by the European Commission, and it is now no longer required to obtain the DPAs' prior authorisation for transferring personal data outside of the EU and submit copies of executed standard contractual clauses (which was previously required in some member states). In addition, the GDPR formally recognises binding corporate rules (BCRs) – internal codes of conduct used by businesses to transfer personal data to group members outside of the EU – as a valid data transfer mechanism for both data controllers and data processors. That said, as a result of the *Schrems II* decision, the EU-US Privacy Shield Framework is no longer a valid mechanism for transferring personal data to the US. Organisations that rely on standard contractual clauses (and other transfer mechanisms, such as BCRs) must now assess each data transfer on a case-by-case basis to determine whether there is an adequate level of protection for personal data that is to be transferred outside of the EU.

Administrative fines and right of individuals to effective judicial remedy

In the previous regime, some DPAs (such as the Belgian DPA) did not have the power to impose administrative fines. The GDPR gives this power to all DPAs and introduces high administrative fines that will significantly change the currently fragmented enforcement landscape. Member state DPAs may now impose administrative fines of up to the greater of €10 million or 2 per cent of a company's total worldwide annual turnover, or the greater of €20 million or 4 per cent of a company's total worldwide annual turn-over, depending on the nature of the violation. In addition, the GDPR expressly enables individuals to bring proceedings against data controllers and data processors, in particular to obtain compensation for damage suffered as a result of a violation of the GDPR.

The WP29 's and EDPB GDPR guidance

The Article 29 Working Party (WP29), composed of representatives of DPAs, has ceased to exist and was replaced by the EDPB as of 25 May 2018. During its first plenary meeting on 25 May 2018, the EDPB endorsed all the GDPR guidelines adopted by the WP29. In total, the WP29 adopted 16 GDPR guidelines and related documents clarifying key concepts and new requirements of the GDPR, including:

- guidelines on the right to data portability;
- guidelines on DPOs;
- guidelines for identifying a data controller or processor's lead DPA;
- guidelines on DPIA and determining whether processing is likely to result in a high risk to the individuals' rights and freedoms;
- guidelines on automated individual decision-making and profiling;
- guidelines on data breach notifications;
- guidelines on administrative fines;
- BCR referential for data controllers;
- BCR referential for data processors;
- adequacy referential;
- guidelines on transparency;
- guidelines on consent;
- updated working document on BCR approval procedure;
- revised BCR application form for controller BCRs;
- revised BCR application form for processor BCRs; and
- position paper on the derogations from the obligation to maintain internal records of processing activities.

In addition, the EDPB also has adopted guidelines that relate to the following:

- consent under the GDPR;
- processing of personal data through video devices;
- processing in the context of the provision of online services to data subjects;
- accreditation of certification bodies under article 43;
- territorial scope;
- derogations from the prohibition on data transfers;
- the use of location data and contact tracing tools, in the context of the covid-19 outbreak; and
- processing of data concerning health for the purpose of scientific research, in the context of the covid-19 outbreak.

EU member state complementing laws

Although the main objective of the GDPR is to harmonise data protection law across the EU, EU member states can and have introduced additional or more specific rules in certain areas; for example, if processing involves health data, genetic data, biometric data, employee data or national identification numbers, or if processing personal data serves archiving, scientific, historical research or statistical purposes. In addition, EU member state laws may require the appointment of a DPO in cases other than those listed in the GDPR. The German Federal Data Protection Act of 30 June 2017, for example, requires businesses to appoint a DPO if they permanently engage at least 10 persons in the data processing, if they carry out data processing activities subject to a DPIA, or if they commercially process personal data for market research purposes. EU member states may also provide for rules regarding the processing of personal data of deceased persons. The French Data Protection Act, as updated on June 21 2018, for example, includes such rules by granting individuals the right to define the way their personal data will be processed after their death, in addition to the GDPR rights. In the context of online services directed to children, the GDPR requires parental consent for children below the age of 16, but EU member state law may prescribe a lower age limit, provided it is not lower than the age of 13. This limit is lowered to the age of 13, for example, in the UK Data Protection Act 2018 and the age of 14 in the Austrian Data

HUNTON ANDREWS KURTH

Aaron P Simpson

asimpson@huntonak.com

Claire François

cfrancois@huntonak.com

James Henderson

jhenderson@huntonak.com

30 St Mary Axe
London EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772

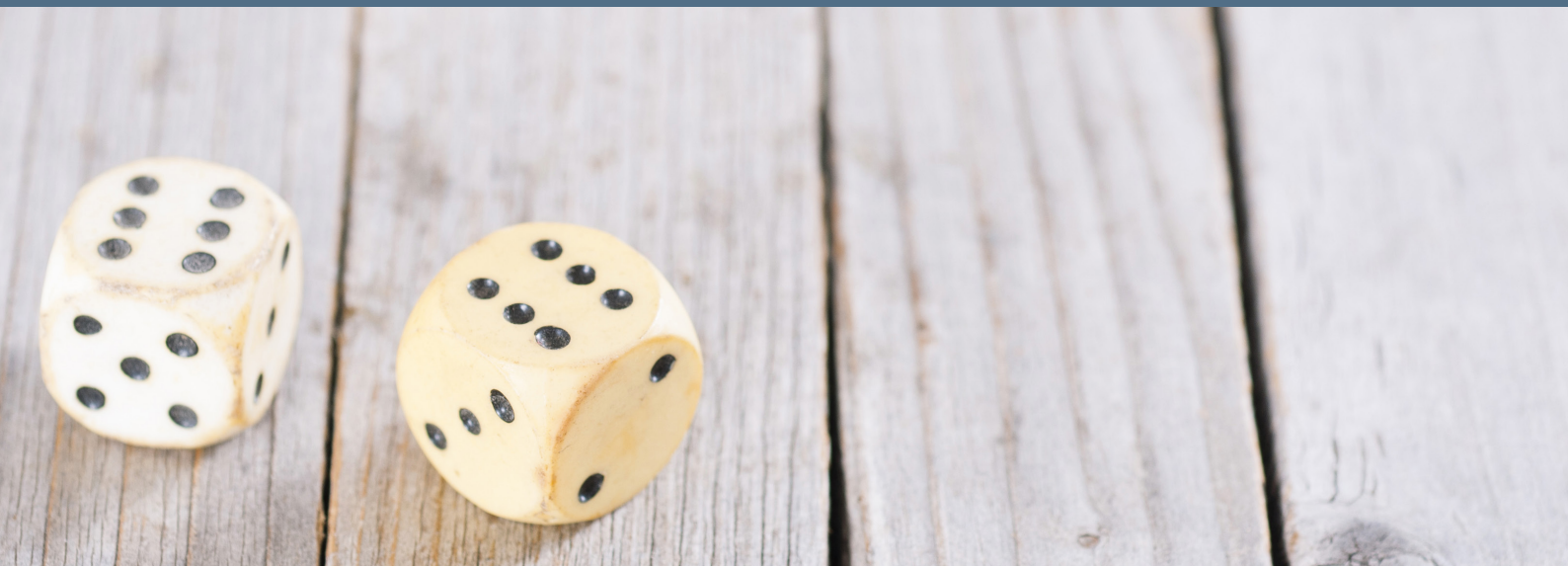
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
Tel: +32 2 643 58 00
Fax: +32 2 643 58 22

www.huntonak.com

Protection Amendment Act 2018. At the time of writing, all EU member states other than Slovenia have adopted their new national data protection laws. This creates additional layers of complexity for businesses, which should closely monitor these developments in the relevant member states and assess the territorial scope of the specific national rules, where applicable.

In summary, it is fair to say that the GDPR has created a more robust and mature data protection framework in the EU, while EU member state laws complement that framework. The new rules affect virtually any business dealing with personal data relating to individuals in the EU. Businesses should at the very least be able to demonstrate that they have engaged in a GDPR compliance programme, in light of the enhanced enforcement powers available to DPAs under the GDPR and the increasing focus on data protection issues since the GDPR entered into effect.

Leaders in Handling High-Stakes Cybersecurity Events



Luck is not a strategy.

**Increase your company's resilience and
responsiveness to cyber attacks.**

Hunton Andrews Kurth LLP's privacy and cybersecurity practice assists global organizations in managing data through every step of the information life cycle. We help businesses prepare for and respond to cybersecurity incidents all over the world. The firm is ranked as a top law firm globally for privacy and data security.

For more information, visit www.huntonprivacyblog.com.

Other titles available in this series

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

Also available digitally

[lexology.com/gtdt](https://www.lexology.com/gtdt)