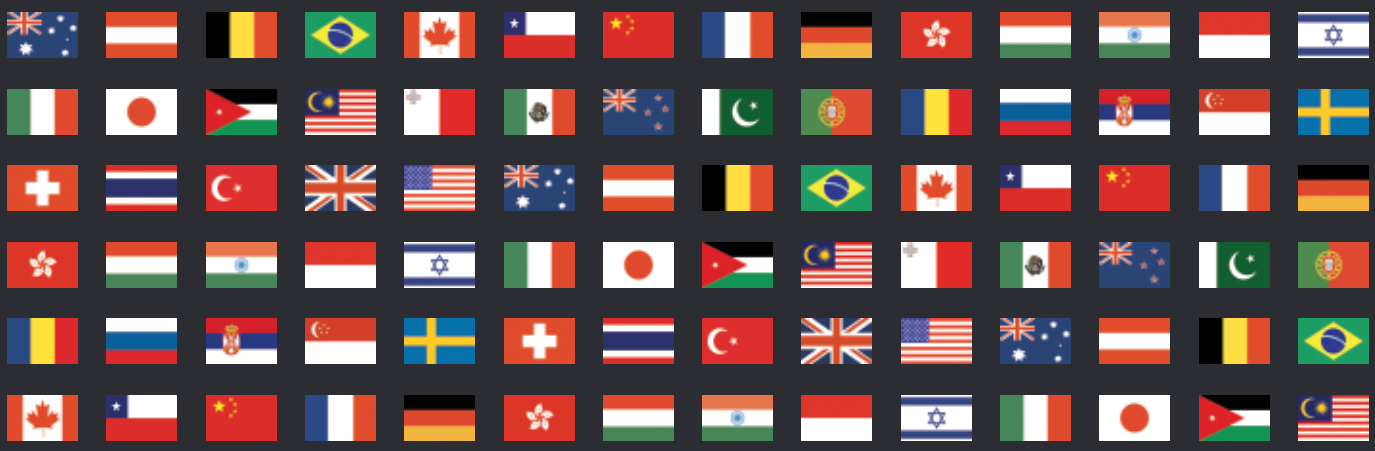
Data Protection & Privacy 2022

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

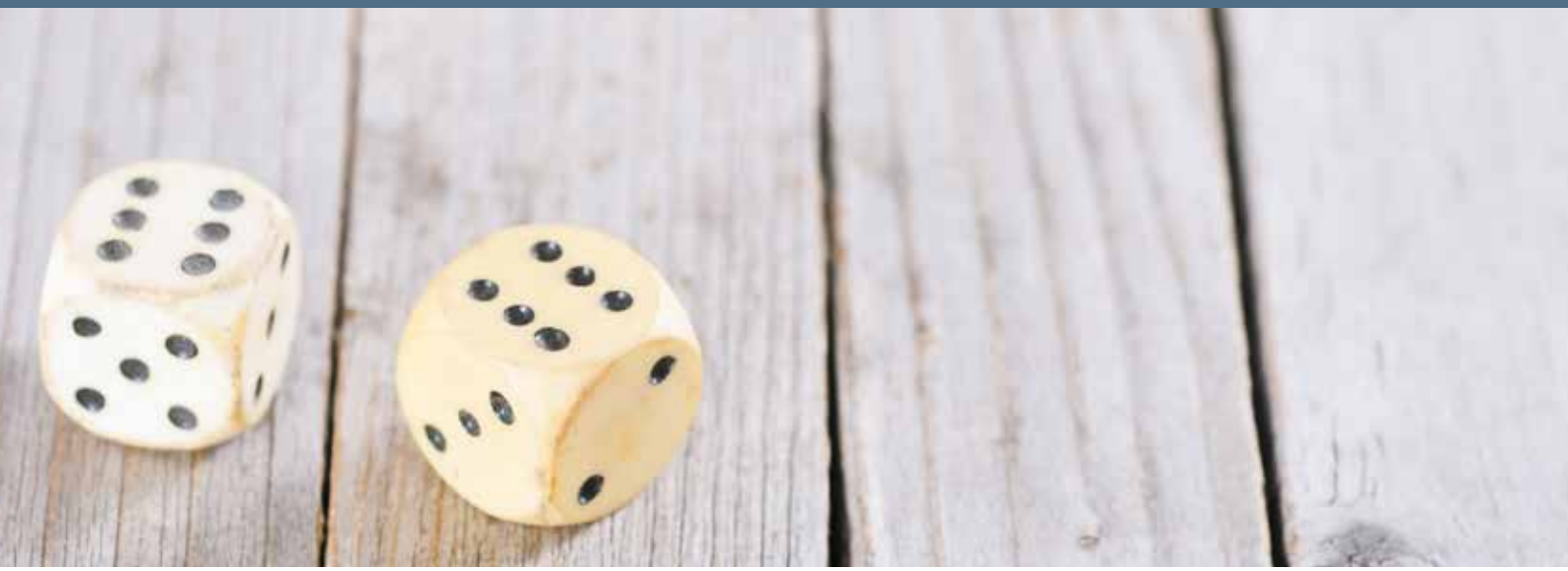


LEXOLOGY
Getting The Deal Through

HUNTON
ANDREWS KURTH

HUNTON
ANDREWS KURTH

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.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

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

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth 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 Jordan, Pakistan and Thailand.

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

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

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

LEXOLOGY
Getting The Deal Through

London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

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

EU overview 11
Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki
Hunton Andrews Kurth LLP

The Privacy Shield 14
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 20
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 28
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 37
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 49
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 57
Doug Tait and Kendall N Dyck
Thompson Dorfman Sweatman LLP

Chile 65
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 72
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

France 82
Benjamin May and Marianne Long
Aramis Law Firm

Germany 96
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Hong Kong 104
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 113
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 121
Arjun Sinha, Mriganki Nagpal and Siddhartha Tandon
AP & Partners

Indonesia 128
Rusmaini Lenggogeni and Charvia Tjhai
SSEK Legal Consultants

Israel 136
Adi El Rom and Hilla Shribman
Amit Pollak Matalon & Co

Italy 145
Paolo Balboni, Luca Bolognini, Davide Baldini and Antonio Landi
ICT Legal Consulting

Japan 154
Akemi Suzuki and Takeshi Hayakawa
Nagashima Ohno & Tsunematsu

Jordan 164
Ma'in Nsair, Haya Al-Erqsousi and Mariana Abu-Dayah
Nsair & Partners - Lawyers

Malaysia 170
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 178
Paul Gonzi and Sarah Cannataci
Fenech & Fenech Advocates

Mexico 187
Abraham Díaz and Gustavo A Alcocer
OLIVARES

New Zealand 195
Derek Roth-Biester, Megan Pearce and Victoria Wilson
Anderson Lloyd

Pakistan 202
Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates Corporate & Legal Consultants

Portugal 209
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 218
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Alina Popescu
MPR Partners

Russia 226
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskoromyuk
Morgan, Lewis & Bockius LLP

Serbia 235
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 242
Lim Chong Kin
Drew & Napier LLC

Sweden 257
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 265
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 276
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Thailand 284
John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Patchamon Purikasem
Formichella & Sritawat Attorneys at Law Co, Ltd

Turkey 291
Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Nazlı Bahar Bilhan
Turunç

United Kingdom 299
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 309
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

The Privacy Shield

Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Twenty-first-century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals are clamouring for governments to do more to safeguard their personal data. A prominent outgrowth of this global cacophony has been a reinvigorated regulatory focus on cross-border data transfers. Russia made headlines because it enacted a law in 2015 that requires companies to store the personal data of Russians on servers in Russia. While this is an extreme example of 'data localisation', Russia is not alone in its effort to create impediments to the free flow of data across borders. The Safe Harbor framework, which was a popular tool used to facilitate data flows from the European Union to the United States for nearly 15 years, was invalidated by the Court of Justice of the European Union (CJEU) in 2015, in part as a result of the PRISM scandal that arose in the wake of Edward Snowden's 2013 revelations. The invalidation of Safe Harbor raised challenging questions regarding the future of transatlantic data flows. A successor framework, the EU–US Privacy Shield, was unveiled by the European Commission in February 2016 and in July 2016 was formally approved by the European Union. In 2017, the Swiss government announced its approval of a Swiss–US Privacy Shield framework. Four years after it was formally approved, the EU–US Privacy Shield was invalidated by the CJEU on 16 July 2020, again as a result of concerns arising from the US surveillance framework. The CJEU's decision to invalidate the EU–US Privacy Shield left Shield-certified organisations scrambling to identify and implement alternative data transfer mechanisms to lawfully transfer EU personal data to the United States.

Contrasting approaches to privacy regulation in the European Union and the United States

Privacy regulation tends to differ from country to country, as it represents a culturally bound window into a nation's attitudes about the appropriate use of information, whether by government or private industry. This is certainly true of the approaches to privacy regulation taken in the European Union and the United States, which historically have been both literally and figuratively an ocean apart. Policymakers in the European Union and the United States were able to set aside these differences in 2000 when they created the Safe Harbor framework, which was developed explicitly to bridge the gap between the differing regulatory approaches taken in the European Union and the United States. With the onset of the Privacy Shield, policymakers again sought to bridge the gap between the different regulatory approaches in the European Union and the United States.

The EU approach to data protection regulation

Largely as a result of the role of data accumulation and misuse in the human rights atrocities perpetrated in mid-20th-century Europe, the region has a hard-line approach to data protection. The processing of personal data about individuals in the European Union is strictly regulated on a pan-EU basis by Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). Unlike its predecessor, Directive 95/46/EC (the Data Protection Directive), the GDPR is not implemented differently at the EU member-state level but applies directly across the European Union.

Extraterritorial considerations are an important component of the data protection regulatory scheme in the European Union, as policymakers have no interest in allowing companies to circumvent EU data protection regulations simply by transferring personal data outside of the European Union. These extraterritorial restrictions are triggered when personal data is exported from the European Union to the vast majority of jurisdictions around the world that have not been deemed adequate by the European Commission; chief among them, from a global commerce perspective, is the United States.

The US approach to privacy regulation

Unlike in the European Union, and for its own cultural and historical reasons, the United States does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Although it is beginning to change with the onset of more comprehensive laws at the state level such as the California Consumer Privacy Act, the California Privacy Rights Act and the Virginia Consumer Data Protection Act, the United States generally favours a sectoral approach to privacy regulation. As a result, in the United States, numerous privacy laws operate at the federal and state levels, and they further differ depending on the industry within the scope of the law. The financial services industry, for example, is regulated by the Gramm-Leach-Bliley Act, while the healthcare industry is regulated by the Health Insurance Portability and Accountability Act of 1996. Issues that fall outside the purview of specific statutes and regulations are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the United States allows courts to play an important quasi-regulatory role in holding businesses and governments accountable for privacy and data security missteps.

The development of the Privacy Shield framework

As globalisation ensued at an exponential pace during the Internet boom of the 1990s, the differences in the regulatory approaches favoured in the European Union versus the United States became a significant issue for global commerce. Massive data flows between the European Union and the United States were (and continue to be) relied upon by multinationals, and EU data transfer restrictions threatened to halt those transfers. Instead of allowing this to happen, in 2000, the European Commission and the US Department of Commerce joined forces and developed the Safe Harbor framework.

The Safe Harbor framework was an agreement between the European Commission and the US Department of Commerce whereby data transfers from the European Union to the United States made pursuant to the accord were considered adequate under EU law. Previously, to achieve the adequacy protection provided by the framework, data importers in the United States were required to make specific

and actionable public representations regarding the processing of personal data they imported from the European Union. In particular, US importers had to comply with the seven Safe Harbor principles of notice, choice, onward transfer, security, access, integrity and enforcement. Not only did US importers have to comply with these principles, but they also had to publicly certify their compliance with the US Department of Commerce and thus subject themselves to enforcement by the US Federal Trade Commission (FTC) to the extent their certification materially misrepresented any aspect of their processing of personal data imported from the European Union.

From its inception, Safe Harbor was popular with a wide variety of US companies whose operations involved the importing of personal data from the European Union. While many of the companies that certified to the framework in the United States did so to facilitate intra-company transfers of employee and customer data from the European Union to the United States, there are a wide variety of others who certified for different reasons. Many of these include third-party IT vendors whose business operations call for the storage of client data in the United States, including personal data regarding a client's customers and employees. In the years immediately following the inception of the Safe Harbor framework, a company's participation in the Safe Harbor framework, in general, went largely unnoticed outside the privacy community. In the more recent past, however, that relative anonymity changed, as the Safe Harbor framework faced an increasing amount of pressure from critics in the European Union and, ultimately, was invalidated in 2015.

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from the European Union began in earnest in 2010. In large part, the criticism stemmed from the perception that the Safe Harbor was too permissive of third-party access to personal data in the United States, including access by the US government. The Düsseldorfer Kreises, the group of German state data-protection authorities, first voiced these concerns and issued a resolution in 2010 requiring German exporters of data to the United States through the framework to employ extra precautions when engaging in such data transfers.

After the Düsseldorfer Kreises expressed its concerns, the pressure intensified and spread beyond Germany to the highest levels of government across the Europe Union. This pressure intensified in the wake of the PRISM scandal in the summer of 2013, when Edward Snowden alleged that the US government was secretly obtaining individuals' (including EU residents') electronic communications from numerous online service providers. Following these explosive allegations, regulatory focus in the European Union shifted in part to the Safe Harbor framework, which was blamed in some circles for facilitating the US government's access to personal data exported from the European Union.

As a practical matter, in the summer of 2013, the European Parliament asked the European Commission to examine the Safe Harbor framework closely. In autumn 2013, the European Commission published the results of this investigation, concluding that the framework lacked transparency and calling for its revision. In particular, the European Commission recommended more robust enforcement of the framework in the United States and more clarity regarding US government access to personal data exported from the European Union under the Safe Harbor framework.

In October 2015, Safe Harbor was invalidated by the CJEU in a highly publicised case brought by an Austrian privacy advocate who challenged the Irish Data Protection Commissioner's assertion that the Safe Harbor agreement precludes the Irish agency from stopping the data transfers of a US company certified to the Safe Harbor from Ireland to the United States. In its decision regarding the authority of the Irish Data Protection Commissioner, the CJEU assessed the validity of the Safe Harbor adequacy decision and held it invalid. The CJEU's decision was based, in large part, on the collection of personal data by US government authorities. For example, the CJEU stated that the Safe Harbor framework did not restrict the US government's ability to collect and use personal data or grant individuals sufficient legal remedies when their personal data was collected by the US government.

The Privacy Shield

Following the invalidation of Safe Harbor, the European Commission and US Department of Commerce negotiated and released a successor framework, the EU–US Privacy Shield, in February 2016. Both the EU–US and Swiss–US Privacy Shield frameworks (collectively, the 'Privacy Shield') have since been approved by the European Commission and the Swiss government respectively. The Privacy Shield is similar to Safe Harbor and contains seven privacy principles to which US companies may publicly certify their compliance. Before the invalidation of the EU–US Privacy Shield on 16 July 2020, after certification, entities certified to the Privacy Shield could import personal data from the European Union without the need for another cross-border data transfer mechanism, such as standard contractual clauses. The Swiss–US Privacy Shield similarly permits certified organisations to import personal data from Switzerland without the need for another transfer mechanism. The privacy principles in the Privacy Shield are substantively comparable to those in Safe Harbor but are more robust and more explicit concerning the actions an organisation must take to comply with the principles. In developing the Privacy Shield principles and accompanying framework, policymakers attempted to respond to the shortcomings of the Safe Harbor privacy principles and framework identified by the CJEU.

After releasing the Privacy Shield, some regulators and authorities in the European Union (including the former Article 29 Working Party (WP29), the European Parliament and the European Data Protection Supervisor) criticised certain aspects of the Privacy Shield as not sufficient to protect personal data. For example, the lack of clear rules regarding data retention was heavily criticised. In response to these criticisms, policymakers negotiated revisions to the Privacy Shield framework to address the shortcomings and increase its odds of approval in the European Union. Based on this feedback, the revised Privacy Shield framework was released in July 2016 and formally approved by the European Union. In addition, WP29, which was previously the group of European Union member state data-protection authorities, subsequently offered its support, albeit half-hearted, for the new framework.

First annual review

Under the renegotiated framework, Privacy Shield was subject to annual reviews by the European Commission to ensure it functioned as intended. In September 2017, the US Department of Commerce and the European Commission conducted the first annual joint review of the Privacy Shield, focusing on any perceived weaknesses of the Privacy Shield, including concerning government access requests for national security reasons, and how Privacy Shield-certified entities sought to comply with their Privacy Shield obligations. In November 2017, WP29 adopted an opinion on the review. The opinion noted that WP29 'welcomes the various efforts made by US authorities to set up a comprehensive procedural framework to support the operation of the Privacy Shield'. The opinion also identified some remaining concerns and recommendations concerning both the commercial and national security aspects of the Privacy Shield framework. The opinion indicated that, if the European Union and the United States did not, within specified time frames, adequately address WP29's concerns about the Privacy Shield, WP29 might bring legal action to challenge the Privacy Shield's validity.

In March 2018, the US Department of Commerce provided an update summarising actions the agency had taken between January 2017 and March 2018 to support the EU–US and Swiss–US Privacy Shield frameworks. These measures addressed both commercial and national security issues associated with the Privacy Shield. Concerning the Privacy Shield's commercial aspects, the US Department of Commerce highlighted:

- an enhanced certification process, including more rigorous company reviews and reduced opportunities for false claims regarding Privacy Shield certification;
- additional monitoring of companies through expanded compliance reviews and proactive checks for false claims;
- active complaint resolution through the confirmation of a full list of arbitrators to support EU individuals' recourse to arbitration;
- strengthened enforcement through continued oversight by the FTC, which announced three Privacy Shield-related false claims actions in September 2017; and
- expanded outreach and education, including reaffirmation of the framework by federal officials and educational outreach to individuals, businesses and authorities.

Concerning national security, the US Department of Commerce noted measures taken to ensure:

- robust limitations and safeguards, including a reaffirmation by the intelligence community of its commitment to civil liberties, privacy and transparency through the updating and re-issuing of Intelligence Community Directive 107;
- independent oversight through the nomination of three individuals to the US Privacy and Civil Liberties Oversight Board (PCLOB) to restore the independent agency to quorum status;
- individual redress through the creation of the Privacy Shield Ombudsperson mechanism, which provides EU and Swiss individuals with an independent review channel concerning the transfer of their data to the US; and
- US legal developments take into account the Privacy Shield, such as Congress's reauthorisation of section 702 of the Foreign Intelligence Surveillance Act (reauthorising elements on which the European Commission's Privacy Shield adequacy determination was based) and enhanced advisory and oversight functions of the PCLOB.

In June 2018, the debate regarding the Privacy Shield resurfaced when the Civil Liberties Committee of the European Parliament (LIBE) voted on a resolution to recommend that the European Commission suspend the Privacy Shield unless the United States complied fully with the framework by 1 September 2018. This resolution, which passed by a vote of the full European Parliament on 5 July 2018, was a non-binding recommendation. Notwithstanding the result of the full vote, the Privacy Shield was not suspended at that time and continued with the Privacy Shield Principles unchanged.

Second annual review

In October 2018, the US Department of Commerce and the European Commission conducted the second annual review of the Privacy Shield, focusing on all aspects of Privacy Shield functionality. The review found significant growth in the programme since the first annual review and noted several key points, including:

- over 4,000 companies certified to the Privacy Shield since the framework's inception, and the US Department of Commerce's promise to revoke the certification of companies that do not comply with the Privacy Shield's principles;
- the appointment of three new members to the PCLOB by the United States, and the PCLOB's declassification of its report on a presidential directive that extended certain signals intelligence privacy protections to foreign citizens;
- the ongoing review of the Privacy Shield Ombudsperson Mechanism, and the need for the United States to promptly appoint a permanent Under Secretary; and
- recent privacy incidents affecting both US and EU residents reaffirming the 'need for strong privacy enforcement to protect our citizens and ensure trust in the digital economy'.

The European Commission's report on the second annual review (the 2018 Commission Report) of December 2018 furthered several of these points. The 2018 Commission Report concluded that the United States continued to ensure an adequate level of protection to the personal data transferred from the European Union to US companies under the EU–US Privacy Shield. The 2018 Commission Report found that US authorities took measures to implement the European Commission's recommendations from the previous year and several aspects of the functioning of the framework had improved. It also noted, however, several areas of concern, including companies' false claims of participation in and other non-compliance with the Privacy Shield, lack of clarity in Privacy Shield guidance developed by the US Department of Commerce and European Data Protection Authorities, and delayed appointment and uncertain effectiveness of a permanent Privacy Shield Ombudsman.

Subsequently, in January 2019, the European Data Protection Board (EDPB) also issued a report on the second annual review (the 2019 EDPB Report). Although not binding on EU or US authorities, the 2019 EDPB Report guided regulators in both jurisdictions regarding the implementation of the Privacy Shield and highlighted the EDPB's ongoing concerns concerning the Privacy Shield. The 2019 EDPB Report praised certain actions and efforts undertaken by US authorities and the European Commission to implement the Privacy Shield, including for example:

- efforts by the US Department of Commerce to adapt the certification process to minimise inaccurate or false claims of participation in the Privacy Shield;
- enforcement actions and other oversight measures taken by the US Department of Commerce and FTC regarding Privacy Shield compliance; and
- issuance of guidance for EU individuals on exercising their rights under the Privacy Shield, and for US businesses to clarify the requirements of the Privacy Shield.

The 2019 EDPB Report also raised similar concerns regarding:

- the US's ability to oversee and enforce compliance with all Privacy Shield principles (particularly the onward transfer principle);
- delay in the appointment of a permanent Privacy Shield Ombudsman;
- lack of clarity in guidance and conflicting interpretations of various topics, such as the definition of human resource data; and
- shortcomings of the re-certification process, which, according to the 2019 EDPB Report, leads to an outdated listing of Privacy Shield-certified companies and confusion for data subjects.

Third annual review

On 23 October 2019, the European Commission published its report on the third annual review of the Privacy Shield. The report confirmed that the United States continued to provide an adequate level of protection for personal data transferred pursuant to the Privacy Shield and noted several improvements made to the Privacy Shield framework following the second annual review. These improvements included efforts by US authorities to monitor participants' compliance with the Privacy Shield framework and the appointment of Keith Krach, Under Secretary of State for Economic Growth, Energy and the Environment, to the position of Privacy Shield Ombudsperson on a permanent basis (the vacancy of this position had been flagged in the two previous annual reviews). The

European Commission's report on the third annual review noted that the number of Privacy Shield-certified organisations exceeded 5,000 at the time of the report, surpassing the number of companies that had previously registered for the now-defunct Safe Harbor framework in the nearly 15 years that Safe Harbor operated.

In its report on the third annual review, the European Commission also made the following findings and recommendations:

- The European Commission recommended shortening the 'recertification grace period' from the 3.5 months currently permitted by the Department of Commerce to a maximum of 30 days. The European Commission also recommended that the Department of Commerce send warning letters to companies who fail to recertify within 30 days of their recertification deadline.
- The European Commission recommended that the Department of Commerce strengthen its efforts to identify companies that have never certified to the Privacy Shield but nevertheless falsely claim to be certified, noting that the Department of Commerce's verification efforts appear to have been focused on checking whether companies continue to claim Privacy Shield participation even after their certifications had lapsed.
- Concerning enforcement, the European Commission praised the FTC for bringing enforcement actions for violations of the Privacy Shield but recommended that the FTC ensure it can share 'meaningful Information on ongoing investigations' with the European Commission and European data protection authorities.
- The European Commission recommended that data protection authorities continue to refine the definition of what falls within human resources data, given differing interpretations of the term by the various authorities and the lack of clear joint guidance.

Applicability of the Privacy Shield after Brexit

On 20 December 2018, the US Department of Commerce updated its frequently asked questions (FAQs) on the EU–US and Swiss–US Privacy Shield Frameworks to clarify the effect of the United Kingdom's planned withdrawal from the European Union (Brexit). The FAQs, which were updated on 31 January 2020, provided information on the steps Privacy Shield participants would need to take to receive personal data from the United Kingdom in reliance on the Privacy Shield after Brexit. This included requirements for Shield-certified organisations to implement certain changes to their public-facing Privacy Shield representations to expressly state their commitment to apply the Privacy Shield Principles to UK personal data received in the United States in reliance on the Privacy Shield. Pursuant to the Withdrawal Agreement implementing the UK's departure from the European Union, EU law (including EU data protection law) continued to apply in the United Kingdom during the Transition Period of 31 January 2020 to 31 December 2020. During the Transition Period, the European Commission's decision on the adequacy of the protection for personal data provided by the Privacy Shield was to apply to transfers of personal data from the United Kingdom to Privacy Shield participants in the United States. As a result of the end of the Transition Period on 31 December 2020, in these FAQs, the Department of Commerce set a deadline of 31 December 2020 to implement these required changes for the Privacy Shield to serve as a mechanism to transfer UK personal data to the United States lawfully. In addition, the FAQs further stated that if a Privacy Shield participant opted to make such public commitments to continue receiving UK personal data in reliance on the Privacy Shield, the participant would be required to cooperate and comply with the UK Information Commissioner's Office concerning any such personal data received.

Before the UK's exit from the European Union, the United Kingdom adopted regulations that incorporated the GDPR into UK law, taking effect at the end of the Transition Period. The EU–US Privacy Shield was invalidated by the CJEU on 16 July 2020. As of the date of this writing:

- the Privacy Shield is thus no longer a lawful data transfer mechanism concerning UK personal data; and
- the Department of Commerce has not updated its UK-specific FAQs to discuss the impact of the invalidation specifically on the previously released requirements for Shield-certified organisations.

Given the Department of Commerce's stated intention to continue administration and enforcement of the Privacy Shield, to understand their obligations going forward, organisations must keep a careful eye on developments related to the overlapping impacts of the UK's withdrawal from the European Union and the decision to invalidate the Privacy Shield.

US Privacy Shield enforcement actions

The FTC brought numerous enforcement actions against companies for false claims of participation in and non-compliance with the Privacy Shield. In September 2018, the FTC announced settlement agreements with four companies – IDmission, LLC, (IDmission) mResource LLC (doing business as Loop Works, LLC) (mResource), SmartStart Employment Screening, Inc (SmartStart), and VenPath, Inc (VenPath) – over allegations that each company had falsely claimed to have valid certifications under the EU–US Privacy Shield framework. The FTC alleged that SmartStart, VenPath and mResource continued to post statements on their websites about their participation in the Privacy Shield after allowing their certifications to lapse. IDmission had applied for a Privacy Shield certification but never completed the necessary steps to be certified. In addition, the FTC alleged that both VenPath and SmartStart failed to comply with a provision under the Privacy Shield requiring companies that cease participation in the Privacy Shield framework to affirm to the US Department of Commerce that they will continue to apply the Privacy Shield protections to personal information collected while participating in the programme. As part of the FTC settlements, each company is prohibited from misrepresenting its participation in any privacy or data security programme sponsored by the government or any self-regulatory or standard-setting organisation and must comply with FTC reporting requirements. Further, VenPath and SmartStart must either continue to apply the Privacy Shield protections to personal information collected while participating in the Privacy Shield, protect it by another means authorised by the Privacy Shield framework, or return or delete the information within 10 days of the FTC's order.

Similarly, on 14 June 2019, the FTC announced a proposed settlement with a Florida-based background screening company, SecurTest, Inc, over allegations that SecurTest started, but did not complete, an application to certify to the Privacy Shield and nevertheless represented that it was Privacy Shield certified. The proposed settlement would prohibit SecurTest from misrepresenting the extent to which it is a member of any self-regulatory framework, including the Privacy Shield. That same month, the FTC announced it had sent warning letters to 13 US companies for falsely claiming participation in the now-defunct Safe Harbor Framework. In a press release, the FTC stated that it called on the 13 companies to remove from their websites, privacy policies, or any other public documents any statements claiming participation in Safe Harbor. The FTC noted that it would take legal action if the companies failed to remove such representations within 30 days. Taken together, the recent increase in FTC enforcement of the Privacy Shield demonstrates the agency's commitment to oversee and enforce compliance with the framework's principles.

Between November 2019 and January 2020, the FTC brought an additional 10 enforcement actions against companies alleged to have violated the Privacy Shield by falsely claiming to be certified to the framework. In November 2019, the FTC announced a settlement with Medable, Inc stemming from allegations that, although Medable did initiate an application with the Department of Commerce in December

2017, the company never completed the steps necessary to participate in the framework. Then, in December 2019, the FTC announced settlements in four separate Privacy Shield cases. Specifically, the FTC alleged that Click Labs, Inc, Incentive Services, Inc, Global Data Vault, LLC, and TDARX, Inc each falsely claimed to participate in the EU–US Privacy Shield framework. The FTC also alleged that Click Labs and Incentive Services falsely claimed to participate in the Swiss–US Privacy Shield framework and that Global Data and TDARX continued to claim participation in the EU–US Privacy Shield after their Privacy Shield certifications lapsed. The complaints further alleged that Global Data and TDARX failed to comply with the Privacy Shield framework, including by failing to:

- annually verify that statements about their Privacy Shield practices were accurate; and
- affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the programme.

The following month, in January 2020, the FTC announced five further Privacy Shield settlements. The FTC had alleged, in separate actions, that DCR Workforce, Inc, Thru, Inc, LotaData, Inc, and 214 Technologies, Inc, had made false claims on their websites that they were certified under the EU–US Privacy Shield. In the case of LotaData, the FTC also alleged that the company had falsely claimed certified participation in the Swiss–US Privacy Shield framework. Lastly, the FTC had alleged that EmpiriStat, Inc falsely claimed current participation in the EU–US Privacy Shield after its certification had lapsed, failed to verify annually that its statements related to its Privacy Shield practices were accurate, and failed to affirm it would continue to apply Privacy Shield protections to personal information it collected while participating in the framework. In each of these cases, as part of the settlements, each of the companies was prohibited from misrepresenting its participation in the Privacy Shield framework, as well as any other privacy or data security programme sponsored by any government, or any self-regulatory or standard-setting organisation.

Following the CJEU's decision to invalidate the EU–US Privacy Shield framework, the FTC stated that it continues to expect Shield-certified organisations to comply with their ongoing obligations concerning transfers made previously under the Privacy Shield, including ongoing compliance with the Privacy Shield principles. To that end, following the 16 July 2020 Schrems II decision, the FTC announced two Privacy Shield settlements. In October 2020, the FTC announced a settlement with data storage company NTT Global Data Centers Americas, Inc (NTT) in connection with allegations that NTT:

- falsely claimed current participation in the EU–US Privacy Shield after its certification had lapsed; and
- failed to comply with Privacy Shield requirements when participating in the framework.

Notably, when announcing the NTT settlement, the FTC stated that the CJEU's July 2020 decision to invalidate the Privacy Shield framework did not affect the validity of the FTC's decision and order relating to the company's misrepresentations about its participation in and compliance with the Privacy Shield programme. In January 2021, the FTC announced a settlement with fertility app developer Flo Health, Inc over allegations that included violations of the Privacy Shield's notice, choice, accountability for onward transfer, and data integrity and purpose limitation principles, as well as misrepresentations regarding adherence to Privacy Shield principles in the company's privacy policy. As part of these settlements, NTT and Flo Health were prohibited from misrepresenting compliance with or participation in the Privacy Shield framework, as well as any other privacy or data security programme sponsored by any government, or any self-regulatory or standard-setting organisation.

Invalidation of the Privacy Shield framework

On 16 July 2020, the CJEU issued a landmark judgment in a case brought by Max Schrems – the privacy activist who is credited with initiating the downfall of Safe Harbor – deemed Schrems II. Schrems II was originally heard by Ireland's High Court after Schrems brought a claim against Facebook questioning whether the methods under which technology firms transferred EU citizens' data to the United States afforded EU citizens adequate protection from US surveillance. Specifically, Schrems alleged that the EU Standard Contractual Clauses did not ensure an adequate level of protection for EU data subjects, on the basis that US law does not explicitly limit interference with an individual's right to protection of their personal data in the same way as EU data protection law. Following the complaint, the Irish data protection authority brought proceedings against Facebook in the Irish High Court. In June 2019, the Irish High Court referred the case to the CJEU to determine the legality of the methods used for data transfers through a set of 11 questions referred for a preliminary ruling. The preliminary questions addressed the validity of the Standard Contractual Clauses (SCCs) but also concerned the EU–US Privacy Shield framework.

In Schrems II, the CJEU ruled that the EU–US Privacy Shield was not a valid mechanism to lawfully transfer EU personal data to the US. In the decision, the CJEU held that:

> *the limitations on the protection of personal data arising from [US domestic law] on the access and use [of the transferred data] by US public authorities […] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.*

Further, the CJEU found that the EU–US Privacy Shield framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU–US Privacy Shield invalid.

In the aftermath of the Schrems II decision, organisations that previously relied on the Privacy Shield to lawfully transfer EU personal data to the United States were required to identify an alternative data transfer mechanism (or applicable derogation under article 49 of the GDPR) to continue transfers of personal data to the US. Following Schrems II, companies using SCCs as a transfer mechanism must:

- assess whether the laws in the importing jurisdiction provide an adequate level of protection for personal data transferred under the SCCs; and
- adopt any supplementary measures necessary to ensure adequate protection under EU law.

On 23 July 2020, the EDPB adopted a set of FAQs on the CJEU's decision. These FAQs confirmed that there was no grace period for companies that relied on the EU–US Privacy Shield framework during which they could continue transferring to the United States without assessing the legal basis relied on for those transfers. Transfers based on the EU–US Privacy Shield framework were now, according to the EDPB, illegal. Notably, in November 2020, the European Commission published a draft set of new SCCs that include language regarding the obligation to ensure that data protection laws in the data importer's country do not prevent the importer from complying with the SCCs' requirements, as well as on the data importer's obligations in connection with government access requests, such as notifying the exporter, reviewing the legality of the request and only providing the minimum permissible amount of information under law in response

to a request. That same month, the EDPB issued draft recommendations on supplementary measures transferring parties can implement in conjunction with SCCs to help ensure adequate levels of protection following Schrems II. In response to the draft SCCs, the US Department of Commerce submitted comments to the European Commission, and the EDPB adopted an opinion providing feedback on the draft clauses. The draft SCCs were finalised on 4 June 2021.

Certain EU data protection authorities also issued statements and guidance in the aftermath of the Schrems II decision, taking various stances on the implication of the ruling. For example, the UK Information Commissioner's Office issued a statement that it stood 'ready to support UK organisations . . . to ensure that global data flows may continue and that people's personal data is protected', and subsequently advised organisations to follow the EDPB FAQs on the use of SCCs as 'this guidance still applies to UK controllers and processors'. Certain German data protection authorities took a stronger approach, such as the Berlin data protection commissioner, who called on Berlin-based companies to return EU data currently stored in the United States back to the European Union. In March 2021, the Bavarian data protection authority found the use of email marketing service Mailchimp not to be compliant with Schrems II mitigation steps when email addresses were transferred to Mailchimp in the United States. The controller using Mailchimp had relied on SCCs to transfer email addresses to the United States from Germany, but in the Bavarian data protection authority's view, the controller failed to assess the risk of the transfer and implement supplementary measures along with the SCCs. The Bavarian data protection authority did not issue a fine, as the EDPB's draft recommendations on supplementary measures had not yet been finalised, the use of Mailchimp was limited to a small number of instances and the controller cooperated and committed to stop using Mailchimp. Separately, in April 2021, the Portuguese data protection authority highlighted that under Schrems II, data protection authorities are obliged to suspend or prohibit data transfers, even when those transfers are based on SCCs, if there are no guarantees that the SCCs can be complied with in the recipient country.

The US Department of Commerce also issued new Privacy Shield FAQs following the Schrems II ruling. The new FAQs state that although (as a result of the Schrems II ruling) the Privacy Shield:

> *is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States . . . this decision does not relieve participants in the EU–US Privacy Shield of their obligations under the EU–US Privacy Shield Framework.*

The FAQs further state that the Department of Commerce will continue to administer the Privacy Shield programme, including processing applications for self-certification and recertification and maintaining the list of Shield-certified organisations. The FAQs also make clear that organisations that wish to remain on the Privacy Shield list continue to be required to annually recertify to the Privacy Shield framework, including by paying the annual processing fee. As of the date of this writing, the Department of Commerce has taken the view that continued participation in the Privacy Shield 'demonstrates a serious commitment to protect personal information in accordance with a set of privacy principles that offer meaningful privacy protections and recourse for EU individuals'.

Regarding the Swiss–US Privacy Shield, the CJEU decision did not strictly affect the legality of that framework, so the Swiss–US Privacy Shield remained a valid transfer mechanism notwithstanding the ruling. On 16 July 2020, the Federal Data Protection and Information Commissioner of Switzerland (FDPIC) stated that the 'FDPIC has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgment in detail and comment on it in due course'. Subsequently, on 8 September 2020, the FDPIC issued an opinion concluding that the Swiss–US Privacy Shield framework does not provide an adequate level of protection for data transfers from Switzerland to the United States under Switzerland's Federal Act on Data Protection. Following this opinion, in practice, companies may no longer rely on the Swiss–US Privacy Shield framework as a valid mechanism for data transfers from Switzerland to the United States. The US Department of Commerce has stated that, consistent with its position regarding the impact of the Schrems II ruling, the FDPIC opinion does not relieve Swiss–US Shield participants of their obligations under the framework. The FDPIC has concluded that organisations must rely on alternative data transfer mechanisms, as well as to conduct a risk assessment and possibly implement additional safeguards to continue transfers of Swiss personal data to the United States.

Negotiation of a new data transfer framework

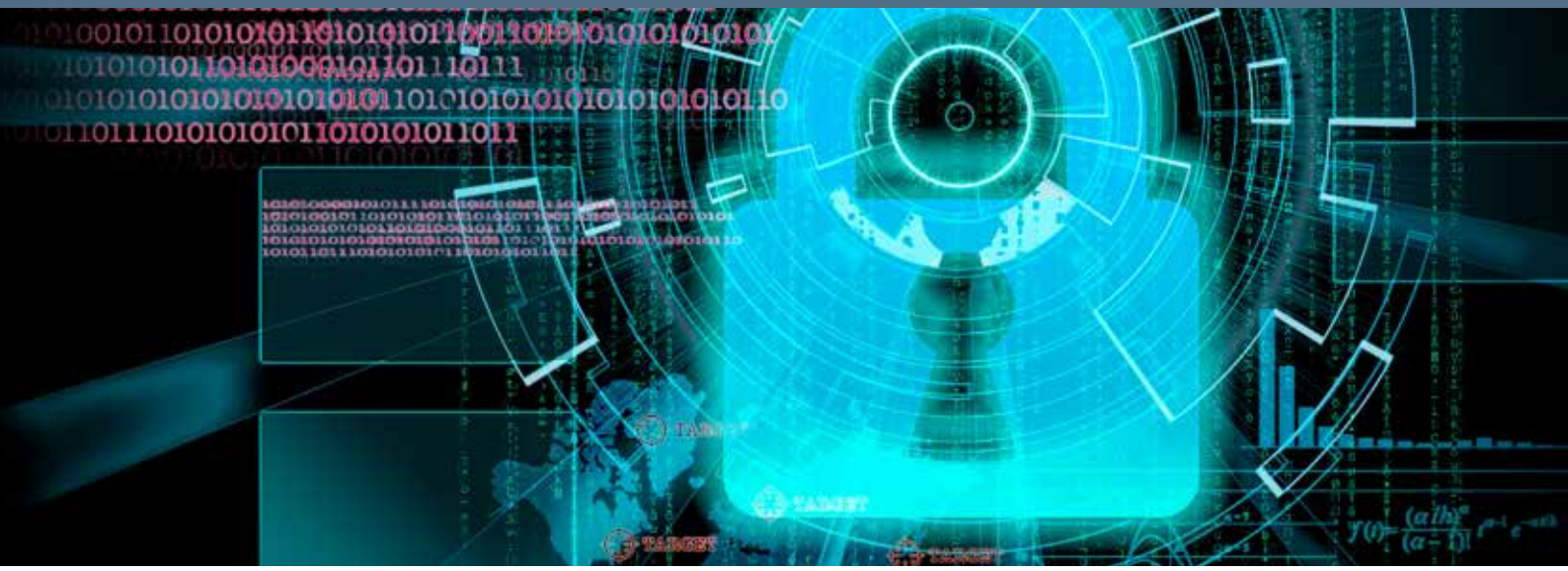
In August 2020, the US Department of Commerce and the European Commission announced discussions had been initiated to evaluate the potential for an enhanced EU–US Privacy Shield framework to comply with the CJEU's judgment in Schrems II. In March 2021, the US Congressional Research Service released an informational report for members of Congress on EU data transfer requirements and US intelligence laws that summarised potential solutions in the United States to issues raised by Schrems II, including:

- an Executive Order limiting bulk intelligence collection and providing additional redress mechanisms;
- a diplomatic agreement for a new framework to replace the Privacy Shield or a data transfer treaty; and
- legislation that limited bulk intelligence collection or created a cause of action for foreign subjects in the event of unlawful collection.

Later that month, on 25 March 2021, the US Secretary of Commerce, Gina Raimondo, and the European Commissioner for Justice, Didier Reynders, issued a joint statement declaring that the US government and the European Commission had decided to intensify negotiations on an enhanced, alternative data transfer framework to address the judgment of the CJEU in Schrems II. The statement noted that 'these negotiations underscore [the parties'] shared commitment to privacy, data protection and the rule of law and [their] mutual recognition of the importance of transatlantic data flows to [their] respective citizens, economies, and societies'. Following this statement, Commissioner Reynders declared in a speech on the digital transatlantic economy that finding a solution on transatlantic data flows 'is a priority in Brussels and in Washington, DC'. For its part, the US Department of Commerce's Privacy Shield press page declares that the 'Privacy Shield and transatlantic data flows are a top priority for the Biden Administration'. In public comments, EU negotiator Bruno Gencarelli of the European Commission and US negotiator Christopher Hoff of the Department of Commerce each indicated both parties' desire for a 'durable' successor framework.

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.

Other titles available in this series

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

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-644-0