Data Protection & Privacy

Contributing editors
Aaron P Simpson and Lisa J Sotto

HUNTON
ANDREWS KURTH

2019

GETTING THE DEAL THROUGH

© Law Business Research 2018

HUNTON
ANDREWS KURTH

Leaders in GDPR Guidelines and Cybersecurity Best Practices

Keep the trust you've earned.

Complying with GDPR guidelines can be challenging, especially for organizations with offices—or customers—across borders. Our high-ranking European data protection lawyers offer assistance on all aspects of European data protection law, including the GDPR, data breaches, international data transfers and BCRs, privacy risk management and cross-border compliance. The firm is a leader in its field and has been ranked by *Computerworld* magazine in all surveys as the top law firm globally for privacy and data security. Hunton Andrews Kurth is also consistently recognized as a leading privacy and data security firm by widely reference legal guides, including *Chambers* and *Partners* and T*he Legal 500*.

For more information, visit www.huntonprivacyblog.com.

© 2018 Hunton Andrews Kurth LLP | HuntonAK.com

© Law Business Research 2018

GETTING THE DEAL THROUGH

Data Protection & Privacy 2019

Contributing editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

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

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

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

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

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

© Law Business Research Ltd 2018
No photocopying without a CLA licence.
First published 2012
Seventh edition
ISBN 978-1-78915-010-0

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 June and July 2018. Be advised that this is a developing area.

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

© Law Business Research 2018

CONTENTS

Introduction 7
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 11
Aaron P Simpson and Claire François
Hunton Andrews Kurth LLP

The Privacy Shield 14
Aaron P Simpson
Hunton Andrews Kurth LLP

Argentina 17
Diego Fernández
Marval, O'Farrell & Mairal

Australia 23
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 30
Rainer Knyrim
Knyrim Trieb Attorneys at Law

Belgium 37
Aaron P Simpson, David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 47
Jorge Cesa, Roberta Feiten and Conrado Steinbruck
Souto Correa Cesa Lummertz & Amaral Advogados

Chile 53
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
García Magliona & Cía Abogados

China 59
Vincent Zhang and John Bolin
Jincheng Tongda & Neal

Colombia 67
María Claudia Martínez Beltrán
DLA Piper Martínez Beltrán Abogados

France 73
Benjamin May and Farah Bencheliha
Aramis

Germany 81
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Greece 87
Vasiliki Christou
Vasiliki Christou

India 93
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Ireland 99
Anne-Marie Bohan
Matheson

Italy 108
Rocco Panetta and Federico Sartore
Panetta & Associati

Japan 117
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Korea 124
Seung Soo Choi and Seungmin Jasmine Jung
Jipyong LLC

Lithuania 130
Laimonas Marcinkevičius
Juridicon Law Firm

Malta 137
Ian Gauci and Michele Tufigno
Gatt Tufigno Gauci Advocates

Mexico 144
Gustavo A Alcocer and Abraham Díaz Arceo
Olivares

Portugal 150
Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Russia 157
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian Zimbler
Morgan, Lewis & Bockius LLP

Serbia 164
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 169
Lim Chong Kin
Drew & Napier LLC

Spain 184
Alejandro Padín, Daniel Caccamo, Katiana Otero, Álvaro Blanco, Pilar Vargas, Raquel Gómez and Laura Cantero
J&A Garrigues

Sweden 192
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 198
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

© Law Business Research 2018

Taiwan 206

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

Turkey 212

Ozan Karaduman and Selin Başaran Savuran
Gün + Partners

United Kingdom 219

Aaron P Simpson and James Henderson
Hunton Andrews Kurth LLP

United States 226

Lisa J Sotto and Aaron P Simpson
Hunton Andrews Kurth LLP

© Law Business Research 2018

Preface

Data Protection & Privacy 2019

Seventh edition

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

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

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Argentina, Colombia, Greece, Korea, Malta and Taiwan.

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

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

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

GETTING THE DEAL THROUGH

London
July 2018

© Law Business Research 2018

The Privacy Shield

Aaron P Simpson
Hunton Andrews Kurth LLP

Twenty-first century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals everywhere are clamouring for governments to do more to safeguard their personal data. A prominent outgrowth of this global cacophony has been reinvigorated regulatory focus on cross-border data transfers. Russia made headlines because it enacted a law in September 2015 that requires companies to store the personal data of Russians on servers in Russia. While this is an extreme example of 'data localisation', the Russian law 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 EU to the US for nearly 15 years, was invalidated by the Court of Justice of the European Union (CJEU) in October 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 in Europe. In January 2017, the Swiss government announced its approval of a Swiss–US Privacy Shield framework.

Contrasting approaches to privacy regulation in the EU and US

Privacy regulation tends to differ from country to country around the world, 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 EU and the US, which are literally and figuratively an ocean apart. Policymakers in the EU and the US 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 EU and the US. With the onset of the Privacy Shield, policymakers have again sought to bridge the gap between the different regulatory approaches in the EU and US.

The European 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 takes an understandably hard-line approach to data protection. The processing of personal data about individuals in the EU is strictly regulated on a pan-EU basis by the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. Unlike its predecessor, the Data Protection Directive 95/46/EC, the GDPR is not implemented differently at the member state level but instead applies directly across the EU as a Regulation.

Extraterritorial considerations are an important component of the data protection regulatory scheme in Europe, as policymakers have no interest in allowing companies to circumvent European data protection regulations simply by transferring personal data outside of Europe. These extraterritorial restrictions are triggered when personal data is exported from Europe 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 Europe, and for its own cultural and historical reasons, the US does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Instead, the US favours a sectoral approach to privacy regulation. As a result, in the US there are numerous privacy laws that 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 regulators are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the US 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 1990s internet boom, the differences in the regulatory approaches favoured in Europe versus the US became a significant issue for global commerce. Massive data flows between Europe and the US were (and continue to be) relied upon by multinationals, and European 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 Europe to the US made pursuant to the accord were considered adequate under European law. Previously, in order to achieve the adequacy protection provided by the framework, data importers in the US were required to make specific and actionable public representations regarding the processing of personal data they imported from Europe. 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, 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 to the extent their certification materially misrepresented any aspect of their processing of personal data imported from Europe.

Since its inception, Safe Harbor was popular with a wide variety of US companies whose operations involved the importing of personal data from Europe. While many of the companies that certified to the framework in the US did so to facilitate intra-company transfers of employee and customer data from Europe to the US, 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 US, 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 Europe and, ultimately, was invalidated in October 2015.

© Law Business Research 2018

Invalidation of the Safe Harbor framework

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In large part, the criticism stems from the perception that the Safe Harbor was too permissive of third-party access to personal data in the US, 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 US 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 Europe. 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 Europe 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 EU.

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 US and more clarity regarding US government access to personal data exported from the EU under the Safe Harbor framework.

In October 2013, Safe Harbor was invalided 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 US. 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 future of 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 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. After certification, entities certified to the Privacy Shield may import personal data from the European Union without the need for another cross-border data transfer mechanism, such as standard contractual clauses. The privacy principles in the Privacy Shield are substantively comparable to those in Safe Harbor but are more robust and more explicit with respect to the actions an organisation must take in order 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 Europe (including the Article 29 Working Party (the Working Party), 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 Europe. Based on this feedback, the revised Privacy Shield framework was released in July 2016 and formally approved in the European Union. In addition, the Working Party, which is the group of European Union member state data protection authorities, subsequently offered its support, albeit tepid, for the new framework.

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 with respect to government access requests for national security reasons, and how Privacy Shield-certified entities have sought to comply with their Privacy Shield obligations. In November 2017, the Working Party adopted an opinion on the review. The opinion noted that the Working Party '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 with respect to both the commercial and national security aspects of the Privacy Shield framework. The opinion indicated that, if the EU and US do not, within specified time-frames, adequately address the Working Party's concerns about the Privacy Shield, the Working Party may 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. With respect to the Privacy Shield's commercial aspects, the 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;

HUNTON ANDREWS KURTH

Aaron P Simpson **asimpson@HuntonAK.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.HuntonAK.com

© Law Business Research 2018

- strengthened enforcement through continued oversight by the Federal Trade Commission, 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.

With respect to 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 Privacy and Civil Liberties Oversight Board (PCLOB) with the aim of restoring 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 in relation to the transfer of their data to the US; and
- US legal developments take into account the Privacy Shield, such as Congress's reauthorisation of the Foreign Intelligence Surveillance Act's Section 702 (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 (LIBE) Committee of the European Parliament voted on a resolution to recommend that the European Commission suspend the Privacy Shield unless the US complied fully with the framework by 1 September 2018. This resolution is a non-binding recommendation, and the full European Parliament was due to vote on the resolution in July 2018. While the results of that full vote could impose additional pressure on the European Commission to take action with respect to the Privacy Shield, it also does not bind the European Commission with respect to the Privacy Shield framework.

© Law Business Research 2018

HUNTON
ANDREWS KURTH

Leaders in Privacy and Cybersecurity

Luck is not a strategy.

Protect your company before — and after — a cyber attack.

Hunton Andrews Kurth LLP's global privacy and cybersecurity practice helps companies manage data at every step of the information life cycle. The firm is a leader in its field and has been ranked by *Computerworld* magazine in all surveys as the top law firm globally for privacy and data security. Hunton Andrews Kurth is also consistently recognized as a leading privacy and data security firm by widely reference legal guides, including *Chambers* and *Partners* and *The Legal 500*.

For more information, visit www.huntonprivacyblog.com.

© 2018 Hunton Andrews Kurth LLP | HuntonAK.com

© Law Business Research 2018

Getting the Deal Through

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

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-010-0

© Law Business Research 2018