# Data Protection & Privacy

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

# Data Protection & Privacy 2018

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910


First published 2012
Sixth edition
ISSN 2051-1280



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

CONTENTS

# Safe Harbor and the Privacy Shield

**Aaron P Simpson**
**Hunton & Williams**

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, especially in the wake of Edward Snowden's explosive revelations in 2013 regarding government snooping. 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. The invalidation of Safe Harbor has 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 as of July 2016 has been formally approved in Europe.

**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-twentieth century Europe, the region takes an understandably hard line approach to data protection. The processing of personal data about EU citizens is, at the time of publication, strictly regulated through Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive is implemented by the member states of the EU, which impose onerous obligations through their national laws regarding the collection, use, sharing and safeguarding of personal data, both locally and extraterritorially. This legal landscape is in the midst of change, as the General Data Protection Regulation will be replacing the Directive in May 2018. While the General Data Protection Regulation will usher in a host of new changes, the hard line approach to data protection will continue.

These 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 Safe Harbor 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 import 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 invalided in October 2015.

**Invalidation of the Safe Harbor framework**

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In a large part, the criticism stems from the perception that the Safe Harbor is 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. 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, 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 Article 29 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 will conduct 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.

HUNTON& WILLIAMS

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

30 St Mary Axe
London EC3A 8EP
United Kingdom

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

*Getting the Deal Through*

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
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 Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
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

Law Business Research

*Data Protection & Privacy*
*ISSN 2051-1280*

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

*Official Partner of the Latin American Corporate Counsel Association*

ABA Section of International Law
*Your Gateway to International Practice*

*Strategic Research Sponsor of the ABA Section of International Law*