ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

USA

Aaron P. Simpson

Hunton & Williams

Chris D. Hydak

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no comprehensive, consolidated data protection law in the U.S. Data protection in the U.S. is primarily regulated through a number of (i) sector specific federal laws, and (ii) state laws.

1.2 Is there any other general legislation that impacts data protection?

Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce". The Federal Trade Commission ("FTC") has brought several enforcement actions under Section 5 of the FTC Act related to data processing practices which it considers unfair or deceptive.

1.3 Is there any sector specific legislation that impacts data protection?

Yes, there are several sector specific laws that impact data protection. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") applies to protected health information and the Gramm-Leach-Bliley Act ("GLB") applies to financial institutions and "nonpublic personal information." Below are additional examples of federal sector specific laws that impact data protection:

- The Children's Online Privacy Protection Act ("COPPA") regulates the online collection and processing of the personal data of children under the age of 13.
- The Telecommunications Act regulates telecommunications carriers' use of customer information.
- The Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transactions Act govern data protection in the consumer reporting industry.
- The Video Privacy Protection Act restricts certain entities from processing personal data that identifies a consumer as having requested or obtained specific video materials or services.

1.4 What is the relevant data protection regulatory authority(ies)?

There are a number of regulatory authorities with respect to data protection, including the FTC, the Consumer Financial Protection Bureau, the Department of Health and Human Services ("HHS") and the 50 state Attorneys General.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  There is no overarching definition of "personal data" under relevant U.S. laws. Each law has its own definition of personal data.
- **"Sensitive Personal Data"**

  U.S. laws generally do not define "sensitive personal data". Certain U.S. laws, however, do provide heightened requirements for certain elements of personal data. For example, many state laws restrict an entity's ability to process Social Security numbers. State laws often impose notification requirements when there are security breaches involving certain data elements deemed sensitive.
- **"Processing"**

  Relevant U.S. laws generally do not define "processing", but in practice processing typically includes collection, usage, storage, disclosure and disposal.
- **"Data Controller"**

  Relevant U.S. laws do not define "data controller". There are similar concepts under certain U.S. laws, however. For example, U.S. state breach notification laws often include the concept of "data owners", which are typically entities that own or license the pertinent information.
- **"Data Processor"**

  Relevant U.S. laws do not define "data processor". Similar to "data controller", however, there are similar concepts under certain U.S. laws.
- **"Data Subject"**

  Relevant U.S. laws do not define "data subject".
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Pseudonymous Data"**

    Relevant U.S. laws do not define "pseudonymous data".
  - **"Direct Personal Data"**

    Relevant U.S. laws do not define "direct personal data".
  - **"Indirect Personal Data"**

    Relevant U.S. laws do not define "indirect personal data".

- **"Data Owner"**

  Certain U.S. laws (e.g., state breach notification laws) refer to data owners. Typically, these are entities that own or license the relevant information (i.e., not data subjects or service providers).

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  There are no overarching principles derived from law for processing personal data. Certain U.S. laws require entities to provide notice when they collect or process certain data. For example, two state laws (i.e., the California Online Privacy Protection Act ("CalOPPA") and the Delaware Online and Personal Privacy Protection Act ("DOPPPA")) require operators of websites and mobile apps to include a notice detailing certain of their information processing practices for data collected through the website or mobile app.

- **Lawful basis for processing**

  There is no overarching requirement to have a lawful basis to process personal data. U.S. laws do, however, restrict an entity's ability to process personal data in certain circumstances. For example, certain state laws restrict retailers from collecting or processing personal data at the point-of-sale when a customer purchases merchandise with a payment card.

- **Purpose limitation**

  There is no overarching principle regarding purpose limitation but certain U.S. laws do require entities to notify individuals of the purposes for which they may collect and process their personal data. In addition, the FTC regularly brings enforcement actions against companies that materially deviate from the purposes for which they collected the information (as articulated in their privacy notice).

- **Data minimisation**

  While there is no overarching principle regarding data minimisation, the FTC has recommended that companies adhere to the principle by only collecting data needed for a specific purpose.

- **Proportionality**

  There is no overarching principle regarding proportionality.

- **Retention**

  There are over 13,000 records retention laws at the state and federal level in the U.S. These laws generally are not specific to personal data but are important to comply with in order to appropriately safeguard records containing personal data.

- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  U.S. laws generally do not provide individuals with a right to access their data. Certain U.S. laws (e.g., HIPAA), however, do provide individuals with access rights.

- **Correction and deletion**

  U.S. laws generally do not provide individuals with a right to correct or delete their data. Certain U.S. laws (e.g., FCRA), however, do grant individuals the right to dispute incomplete or inaccurate information and impose a duty on certain entities to correct the inaccurate or incomplete information.

- **Objection to processing**

  U.S. laws generally do not provide individuals with a right to object to the processing of their data.

- **Objection to marketing**

  Many sector specific U.S. laws allow individuals to object to being contacted for marketing purposes. For example, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") requires that entities sending marketing or promotional emails to consumers provide a mechanism for consumers to opt out from future marketing or promotional emails.

- **Complaint to relevant data protection authority(ies)**

  U.S. consumers may report violations of relevant privacy laws to government regulators, such as the FTC and state Attorneys General, but there are no data protection-specific regulators in the U.S. at this time.

- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no circumstances in which an organisation has to register or notify a data protection authority prior to the general processing of personal data. There are notification requirements with respect to data breaches, as discussed in section 13.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

This is not applicable.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This is not applicable.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

This is not applicable.

5.5 What are the sanctions for failure to register/notify where required?

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no U.S. law with respect to appointing a Data Protection Officer. "Covered entities" under HIPAA, however, must appoint a privacy officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Post – This is not applicable.

Telephone and SMS text message – Among other relevant laws, the Telephone Consumer Protection Act ("TCPA") requires that entities obtain the "prior express written consent" of a consumer before marketing to him or her via a telephone call or SMS text message to a mobile phone sent using auto dialling equipment or a prerecorded or artificial voice. The TCPA also requires "prior express written consent" for calls to residential lines using an artificial or prerecorded voice.

Email – CAN-SPAM requires entities marketing via email to provide consumers with a clear and conspicuous mechanism for opting out of future marketing emails.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The FTC is active in enforcing violations of the Telemarketing Sales Rule ("TSR"), which is similar to the TCPA in that it requires prior consumer consent for telemarketing calls. In addition, the Federal Communications Commission ("FCC") is somewhat active in enforcing the TCPA but, as the TCPA contains a private right of action, the vast majority of TCPA litigation is initiated by private plaintiffs, not the FCC. Accordingly, entities that conduct telemarketing are generally more concerned with the TCPA than the TSR because the TCPA (i) provides aggrieved consumers with a private right of action, and (ii) is broader in scope than the TSR. The FTC also is active in enforcing against companies that use personal data, including with respect to marketing, in ways that materially deviate from representations they have made in public.

7.3 Are companies required to screen against any "do not contact" list or registry?

Generally, telemarketers are required to screen against the national do-not-call registry.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Each email that violates CAN-SPAM is subject to a maximum penalty of $16,000. Each telephone call or text message that violates the TCPA is subject to a maximum penalty of $1,500.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

No type of cookies requires opt-in consent.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

There is no U.S. law specifically addressing consent to cookies. CalOPPA and DOPPPA do require, in certain circumstances, operators of commercial websites and online services that collect personal data to disclose (i) how the operator responds to "do not track" signals from web browsers, and (ii) whether third parties on the operator's website or online service may collect personal data about users' online activities over time and across third-party websites.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The FTC has brought enforcement actions related an entity's information processing practices that included cookie use. For example, the FTC has brought enforcement actions against companies alleged to have violated COPPA or Section 5 of the FTC Act through, in part, their use of cookies.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

There is no U.S. law that specifically addresses cookies.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

There are no restrictions on cross-border transfers of personal data.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

This is not applicable.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

This is not applicable.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The Sarbanes-Oxley Act ("SOX") requires publicly listed companies to implement a whistle-blowing hotline or other complaint notification system for the receipt of complaints related to accounting, internal accounting controls or auditing matters. SOX also provides protections to restrict retaliatory actions against whistle-blowers. There are no limitations, however, imposed by data protection or other laws on the scope of whistle-blower hotlines with respect to (i) issues that may be reported, (ii) the persons who may submit a report, or (iii) the persons whom a report may concern.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

This is not applicable.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

This is not applicable.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

This is not applicable.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

If a workforce is unionised, the trade union would need to be notified or consulted only if the agreement between the union and the employer requires notification or consultation, which is unlikely.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

All types of employee monitoring (e.g., monitoring phone calls, computer use, email use, etc.) are permitted if the monitoring is for a legitimate business purpose. In addition, employee monitoring without a legitimate business purpose may be permitted in certain circumstances (e.g., with notice and consent). However, certain monitoring activities that would be highly offensive, such as using CCTV in the employee lavatory, are generally not permitted.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Certain U.S. laws require employers to provide notice of electronic employee monitoring. Neither notice for other forms of monitoring nor consent is strictly required to monitor employees for a legitimate

business purpose. Many employers in the U.S., however, provide notice and obtain consent to their monitoring practices to help ensure that data subjects clearly understand that monitoring is occurring. Notice and consent is typically obtained via an employee policy (e.g., an Acceptable Use Policy or specific monitoring policy) and/or a network login banner.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no data protection requirement to notify or consult with works councils, trade unions or employee representatives.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, processing personal data in the cloud is permitted. There are no specific laws regarding processing personal data in the cloud.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

This is not applicable.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, it is permitted. There is no specific diligence required under applicable law or binding guidance to use big data and analytics in the U.S.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no overarching data security standards imposed by U.S. law. Certain sector specific federal laws impose data security requirements on particular entities. For example, GLB requires financial institutions to implement an information security programme, and regularly monitor and test the information security programme. HIPAA requires covered entities and business associates to take specific steps to safeguard electronically protected health information, including the implementation of administrative, physical and technical safeguards. In addition, some U.S. states have enacted laws imposing minimum information security requirements on entities that process information about a resident of those states. The most stringent of these state laws is the Massachusetts law, which requires, among other items, that applicable organisations develop, implement and maintain a comprehensive and written information security programme. The Massachusetts law requires the encryption of (i) files containing personal data that are transmitted across public networks, and (ii) data containing personal data that is transmitted wirelessly.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes, there is a legal requirement to report data breaches to certain data protection authorities. Approximately 20 states require entities to report data breaches to the relevant state regulator, such as the Attorney General. The exact requirements regarding the details and timeframe vary among the state laws. Most states do not include a requirement to provide notification within a prescribed timeframe, but some do. For example, Puerto Rico's breach notification law requires notice to the relevant regulator within 10 days after the incident has been detected and Vermont's law requires a preliminary notice within 14 business days of the date of discovery. The requirements regarding the content of the notice to government regulators vary, but generally include a description of the breach, the types of information impacted and what the entity has done to mitigate risk to affected individuals.

In addition, certain sector specific federal laws require entities to notify regulators in the event of a data breach. For example, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice requires financial institutions to notify their primary federal regulator. The Health Information Technology for Economic and Clinical Health ("HITECH") Act requires entities to notify HHS immediately for breaches that affect the protected health information of more than 500 individuals. Breaches that affect the protected health information of fewer than 500 individuals must be reported to HHS annually. HHS provides an electronic form for entities to report breaches. The form requests information such as a description of the breach and the subsequent actions taken by the entity to respond to the breach.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Forty-seven U.S. states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted data breach notification statutes requiring entities to notify affected individuals in the event of a data breach. The laws vary but generally require notification to affected individuals in the most expedient time possible and without unreasonable delay. Some state laws, however, require notification within a prescribed timeframe (e.g., 30 days in Florida). The content requirements regarding what information must be contained

in the notice to affected individuals vary among the relevant laws. Generally, however, the state data breach notification laws require the notice to contain a general description of the incident, the types of information affected and contact information where affected individuals may obtain additional information. With respect to federal laws, the HITECH Act requires notification to affected individuals within 60 days.

13.4 What are the maximum penalties for security breaches?

There are no penalties simply for suffering a data breach. There can be penalties, however, if a breached company did not or does not comply with relevant federal or state data breach notification statutes, information security statutes or other applicable laws. In addition, there can be penalties associated with a breach if a company was negligent, reckless, made deceptive comments about its information security practices or its information security practices were lax enough to be deemed "unfair".

Penalties can include enforcement actions from government regulators and class action lawsuits initiated by impacted individuals. The maximum penalties depend on the law at issue.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

The data protection authorities have wide-ranging enforcement powers, including the authority to issue civil investigative demands, subpoenas and generally investigate a company's information processing practices. Additionally, the enforcement authorities can impose sanctions, such as monetary penalties, and affirmative obligations, such as a mandate to implement a comprehensive information security programme, submit to independent audits and submit compliance reports on a regular basis to the relevant data protection authority. Often the requirement to implement a comprehensive information security programme includes monitoring by the authority for a lengthy period (e.g., 20 years).

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There are numerous regulators with authority to bring actions related to data protection and they do not follow a common approach. The FTC is the most active federal regulator in the data protection arena. A recent federal court decision related to an FTC enforcement action against a large hotel chain regarding the hotel chain's information security practices buttressed the FTC's authority to bring enforcement actions related to information security standards and practices. As a result of the decision, the FTC (and potentially other government regulators) may be more emboldened to bring future actions related to information security and data protection.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no particular rule regarding how U.S. companies may respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

15.2 What guidance has the data protection authority(ies) issued?

No guidance has been used.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

During the previous 12 months, there have been a few trends with respect to the enforcement of data protection laws. For example, it is becoming rather common, at both the federal and state levels, for regulators to send organisations that suffered a data breach written request for information regarding the breach, such as what specific information security measures the organisation had in place prior to the breach and what information security measures the organisation is implementing to correct any vulnerabilities identified as a result of the breach. Also within the previous 12 months, the FTC has brought several privacy and data security-related enforcement actions. For example, the FTC brought and settled enforcement actions against (i) a technology company that allows retailers to track consumer movement in-store alleging that the technology company misrepresented consumers' ability to opt out of such in-store tracking, and (ii) multiple data brokers alleging that the data brokers failed to provide reasonable security to protect consumer financial information. The FTC also recently released a report on the Internet of Things ("IoT"), which stated that the FTC will use its enforcement authority to bring actions against entities in the IoT space that violate laws the FTC has the authority to enforce.

In addition, the FCC has entered the information security arena. In October 2014, the FCC brought its first enforcement actions related to information security against two telecommunications carriers for allegedly failing to adequately safeguard their customers' personal data. In November 2015, the FCC settled its first information security-related enforcement action against a cable provider after the cable provider was the target of a cyberattack that compromised the personal data of certain of the provider's current and former customers.

16.2 What "hot topics" are currently a focus for the data protection regulator?

As described in question 16.1 above, cybersecurity remains a "hot topic" in the U.S. and is a priority for the Obama administration. In addition, Congress passed the Cybersecurity Information Sharing Act ("CISA"), which President Obama signed into law on December 18, 2015. CISA facilitates and encourages the sharing of Internet traffic information between and among the private sector and the federal government to prevent cyberattacks. The mobile ecosystem and the IoT are "hot topics" as well.

The transfer of personal data from the European Union ("EU") to the U.S. became a "hot topic" in October 2015 when the Court of Justice of the European Union ruled the U.S.-EU Safe Harbour invalid. Subsequent to the invalidation of Safe Harbour, the U.S. Department of Commerce and the European Commission reached agreement on the Privacy Shield, which will (if implemented) replace Safe Harbour as a valid basis for transferring personal data from the EU to the U.S. The European Commission released the legal texts that will implement the Privacy Shield on February 29, 2016. These legal texts must be approved by the College of Commissioners before the Privacy Shield is implemented.

Aaron P. Simpson
Hunton & Williams
200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1126
Email: asimpson@hunton.com
URL: www.hunton.com

Aaron P. Simpson is a partner in the New York office of Hunton & Williams. He advises clients on a broad range of complex privacy and cybersecurity matters, including state, federal and international privacy and data security requirements, and the remediation of large-scale data security incidents. He helps clients identify, evaluate and manage risks associated with their collection and use of information. Aaron is well-known as a top privacy professional and has been recognised by *Chambers & Partners*, *New York Super Lawyers*, *Computerworld* and *The Legal 500* for his work on behalf of clients. He is a sought-after media resource on privacy issues and has been quoted in publications such as *Bloomberg Businessweek Magazine*, *DataGuidance* and *TIME Magazine*. Aaron regularly speaks before industry groups, legal organisations, government agencies and educational institutions at conferences, seminars, roundtables and webinars. He has written and co-written numerous articles, book chapters and handbooks on privacy and cybersecurity issues.

Chris D. Hydak
Hunton & Williams
200 Park Avenue
New York, NY 10166
USA

Tel: +1 212 309 1012
Email: chydak@hunton.com
URL: www.hunton.com

Chris D. Hydak is an associate in the New York office of Hunton & Williams. He assists clients in identifying and managing privacy and information security risks, and advises clients on federal, state and international privacy obligations. His practice includes advising a wide array of clients including financial services businesses, technology companies, media companies, retailers, manufacturers and telecommunications companies. He has also assisted clients in the aftermath of a data breach, including in connection with a Federal Trade Commission investigation and subsequent enforcement action in federal court.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is known throughout the world for its deep experience, breadth of knowledge and outstanding client service. *Chambers & Partners*, *The Legal 500* and *Computerworld* have named Hunton & Williams as a top firm for privacy and cybersecurity. In addition to our legal practice, we distinguish ourselves through our Centre for Information Policy Leadership, which boasts the active participation of more than 35 leading multinational corporations. For the latest resources in privacy, data protection and cybersecurity, visit www.huntonprivacyblog.com and www.huntonregulationtracker.com.

This article appeared in the 2016 edition of The International Comparative Legal Guide to: Data Protection published by Global Legal Group Ltd, London. www.iclg.co.uk

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk