ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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
June 2018

Copyright © 2018
Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice.
Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

USA

Deborah Thoren-Peden

Pillsbury Winthrop Shaw Pittman LLP

Catherine D. Meyer

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The protection of data of US residents is regulated by laws enacted on both the national and the state level. There is no single principal data protection legislation. Federal statutes are primarily aimed at specific sectors, as described more fully below, while state statutes are more focused on protecting the privacy rights of individual consumers. The right to privacy is a common law right that has been incorporated into the state constitutions of many states and into the laws at both the state and federal level. Laws protecting data and consumer privacy are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by agreement, statute or disclosure. Data protection and privacy statutes in the US are enacted to protect the individuals residing in the US or one of its states. Federal laws apply to protect residents of all states. State laws are designed to protect their residents.

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

Most states have adopted laws protecting the personally identifiable information of their residents. These laws apply to the information about a resident of the particular state and require businesses to comply with the state's laws if the business collects, holds, transfers or processes information about a state resident, even if the business does not have a physical presence or business operation in the state.

The type of information protected varies depending on the statute. Some statutes apply to any information that relates to an identifiable individual while some apply to a more limited set of personally identifiable information – an individual's name together with a data element such as a Social Security Number, driver's licence number, financial account number, and medical or health information. A growing number of states include protection of biometric data under these laws.

These state laws may include an obligation:

- to protect personal information from unauthorised access, misuse or destruction;
- to take reasonable steps to securely destroy records containing personal information when it is to be discarded so that the information is rendered undecipherable;
- to protect Social Security Numbers against public disclosure;
- to restrict the collection and use of driver's licence information for any purpose other than age verification or identification;
- to provide written notification to any data subject whose sensitive personal information is accessed or acquired by an unauthorised person;
- to require vendors or service providers to protect data shared with them;
- to restrict the sale of email addresses;
- to restrict the collection of personal information in certain types of transactions;
- to adopt comprehensive written data security plans; and
- to encrypt personal information in transmission over the internet or in storage on portable devices.

Not all states have enacted all such laws and where multiple states address a specific topic, the laws in those states are not necessarily consistent with each other, but vary from state to state. Some states, like California, are more active in protecting its consumers, restricting disclosure of personal information for marketing purposes, requiring online privacy disclosures and granting minor children the right to be forgotten in their online postings. Massachusetts, for example, has strong data protection regulations (201 CMR 1700), requiring any entity that holds, transmits or collects "personal information" of a Massachusetts resident to implement and maintain a comprehensive written data security plan addressing 12 designated activities. New York has adopted Cyber Security Regulations applicable to financial institutions doing business in the state which require comprehensive plans to address cyber security risks.

A number of states restrict the collection of data from consumers, generally in the context of retail transactions with customers. These include limiting information that can be collected in a credit card or cheque transaction.

Most states have enacted legislation that restricts recording communications involving telephones (wiretap laws) or offline (eavesdropping laws) without obtaining consent from one or all parties. These laws apply to any call initiated in or connecting to a phone in the state, and some carry criminal penalties.

Finally, some states have enacted laws specifically protecting children residing in the state. These include Child Protection Registry laws which prohibit sending any child under the age of 18 to contact points listed with the registry communications promoting any product which the child is legally not permitted to own, purchase, view, possess or use; and requiring operators of online sites that allow children under the age of 18 to post information about themselves to provide the minors a means of deleting all such information upon request.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

Historically, US federal law has regulated data protection and consumer privacy on a sectoral basis, focusing specific regulations on financial services and health care providers. In addition, federal law imposes obligations on businesses generally to prohibit unfair or deceptive practices, to protect the intrusive use of consumer information when considering eligibility for insurance, employment or credit, and to regulate telephone, text, fax and email marketing.

The Gramm Leach Bliley Act (15 U.S. Code 6802(a) *et seq.*) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses "Non-Public Personal Information" (NPI) which includes any information that a financial service company collects from its customers in connection with the provision of its services. It imposes on financial service industry companies requirements for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Health Information Portability and Accountability Act (29 U.S. Code 1181 *et seq.*) protects information held by a covered entity that concerns health status, provision of health care or payment for health care that can be linked to an individual. Its Privacy Rule regulates the collection and disclosure of such information. Its Security Rule imposes requirements for securing this data.

Under the Federal Trade Commission Act (15 U.S. Code 41 *et seq.*), the US Federal Trade Commission (FTC) is broadly empowered to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. The FTC has taken the position that "deceptive practices" include a company's failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

The Driver's Privacy Protection Act of 1994 (18 U.S. Code 2721 *et seq.*) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The DPPA restricts how personal information is released. The DPPA defines personal information as information that identifies a person including photographs, Social Security Number (SSN), Client Identification Number (CID), name, address (but not the five-digit ZIP code), telephone number, medical information and disability information.

The Fair Credit Reporting Act, as amended by Fair and Accurate Credit Transactions Act (FACTA) (15 U.S. Code 1681), restricts use of information bearing on an individual's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires truncating credit card numbers on printed credit card receipts, requires securely destroying certain types of personal information and regulates the use of certain types of information received from affiliated companies for marketing purposes. Finally, it imposes obligations on financial institutions and creditors to institute programmes that detect and respond to instances of identity theft under its Identity Theft Red Flag Rule.

Unsolicited commercial emails are regulated under the CAN-SPAM Act (15 U.S. Code 7704), which requires certain technical information to be included in unsolicited emails and permits consumers to opt-out of the receipt of such emails.

The Telephone Consumer Protection Act (TCPA) and associated regulations regulate all calls and text messages to mobile phones and regulate calls to residential phones that are made for marketing purposes or using automated dialing systems or prerecorded messages under its Telemarketing Sales Rule.

Children's information is protected at the federal level under the Children's Online Privacy Protection Act (COPPA) (15 U.S. Code 6501), which prohibits the online collection of any information from a child under the age of 13, and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected.

The Video Privacy Protection Act (VPPA) (18 U.S. Code 2710 *et seq.*) was enacted to protect wrongful disclosure of video-tape rental or sale records or similar audio-visual materials, including online streaming.

Generally, where a federal statute covers a specific topic, the federal law pre-empts any similar state law on that topic. However, certain federal laws, like the Gramm Leach Bliley Act, for instance, specifies that it is not pre-emptive of state laws on the subject. As a result, some states have enacted sectoral laws similar to those federal statutes listed above, with some of those state laws being more restrictive than the federal laws.

1.4 What authority(ies) are responsible for data protection?

At the federal level, the FTC, the Office of the Comptroller of the Currency, and the Department of Health and Human Services.

2 Definitions

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

- **"Personal Data"**

  The definition of personal information in the US is not uniform across all states or all regulations. In addition, certain data may be considered to be personal information for one purpose but not for another. The breadth of the definition varies by statute as illustrated by the following chart referencing California statutes as examples.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

	First and last name	Home or physical address (street and city)	Email address	Telephone number	Social security number	Identifier allowing for physical or online contact	Signature	Passport number	Driver's license number / State issued ID	Physical characteristics or description	Insurance policy number	Education	Employment	Financial Account number	Medical Information	Health insurance information	Information capable of being associated with a particular individual	User name/email plus password for online account	Height, weight, gender, religion, political party affiliation, age, date of birth	Children's names, age, gender, number, email addresses
California Online Privacy Protection Act	X	x	x	x	x	x														
California Data Destruction Statute	X	x		x	x		x	x	x	x	x	x	x	x	x	x	x			
California Data Protection Statute	X with data point				x				x					x	x	x		x		
California Data Breach Notification Statute	X with data point				x				x					x	x	x		x		
California Disclosure of personal information for marketing purposes statute	X	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

- **"Processing"**

  This is not applicable.
- **"Controller"**

  This is not applicable.
- **"Processor"**

  This is not applicable.
- **"Data Subject"**

  The state data protection statutes reference either individuals residing within the state or a "consumer" residing within the state. A "consumer" is an individual who engages with a business for personal, family or household purposes.
- **"Sensitive Personal Data"**

  This is not applicable.
- **"Data Breach"**

  The definition of Data Breach depends on the individual statute.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  This is not applicable.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Businesses established in other jurisdictions are subject to federal data protection laws for all US residents and also to state data protection laws, based on the state of residence of any individual whose information the business collects, holds, transmits, processes or shares. This is based on a long-established principle articulated by the US Supreme Court in 1954 that a state "may regulate to protect interests of its own people, even though other phases of the same transactions might justify regulator legislation in other states" (*Watson v. Employer Liability Corp.* (1954) 348 U.S. 66 at 72). While each state may not regulate businesses that are entirely outside of it and have no contact with residents of the state, when a business interacts with the residents of a state, each state has a legitimate interest in protecting the health, life and safety of its citizens. Data protection falls under this principle.

4 Key Principles

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

- **Transparency**

  US data protection statutes are focused generally on security of the data. As such, the European principles of transparency, lawful basis for processing, purpose limitation, data minimisation, proportionality and data retention are not addressed in the statutes. We note that there is guidance regarding a minimum period of time in which certain documents, like employee records, must be retained, but there is not necessarily a requirement for the destruction of those records after that time has expired. This is left to a company's decision.
- **Lawful basis for processing**

  This is not applicable.
- **Purpose limitation**

  This is not applicable.
- **Data minimisation**

  This is not applicable.
- **Proportionality**

  This is not applicable.
- **Retention**

  This is not applicable.
- *Other key principles – please specify*

  This is not applicable.

5 Individual Rights

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

- **Right of access to data/copies of data**

  Under certain circumstances, employees are entitled to receive copies of data held by employers. Parents are entitled to receive copies of information collected online from children under the age of 13. Under the Health Insurance Portability and Accountability Act (HIPAA), individuals are entitled to request copies of medical information held by a health services provider. Under the Fair Credit Reporting

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Act, individuals are permitted to receive a copy of consumer report information that is maintained by a consumer reporting agency.

- **Right to rectification of errors**

  This is not applicable.

- **Right to deletion/right to be forgotten**

  One state (California) permits individuals to request deletion of information posted online while under the age of 18.

- **Right to object to processing**

  At the federal level, individuals are given the right to opt-out of receiving commercial (advertising) emails under CAN-SPAM and the right to not receive certain types of calls to residential or mobile telephone numbers without express consent under the Telephone Consumer Protection Act. At the state level, individuals have the right not to have telephone calls recorded without either consent of all parties to the call or consent of one party to the call.

- **Right to restrict processing**

  This is not applicable.

- **Right to data portability**

  Under the Health Insurance Portability and Accountability Act (HIPAA), individuals are entitled to request that medical information held by a health services provider be transferred to another health services provider.

- **Right to withdraw consent**

  Under the Telephone Consumer Protection Act, individuals are permitted to withdraw consent given to receive certain types of calls to residential or mobile telephone lines.

- **Right to object to marketing**

  Under CAN-SPAM, individuals are permitted to opt-out of receiving commercial (advertising) emails. Under the Telephone Consumer Protection Act, individuals must provide express written consent to receive marketing calls/texts to mobile telephone lines. California's Shine the Light Act requires companies that share personal information for the recipient's direct marketing purposes to either provide an opt-out or make certain disclosures of what information is shared and with whom.

- **Right to complain to the relevant data protection authority(ies)**

  This is not applicable.

- *Other key rights – please specify*

  This is not applicable.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is not.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 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.

6.4 Who must register with/notify the data protection authority (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.

6.5 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.

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

This is not applicable.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

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

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the statute. These include the Gramm Leach Bliley Act, HIPAA, and the Massachusetts Data Security Regulation, for example.

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

Potential enforcement action by the relevant regulator.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

This is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The designated individual must be an employee of the entity for which it acts.

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

This is not specified.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

General oversight of compliance with the regulation.

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

No, this is not a requirement.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No, this is not a requirement.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Under the laws of certain states, if a business shares certain categories of personal information with a vendor, the business is required to contractually bind the vendor to reasonable security practices. The form of the contract is not specified.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

See above.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

Prior express written consent is required under the Telephone Consumer Protect Act before marketing calls or texts may be sent to a mobile telephone line. Certain disclosures are required to be given regarding whether the calls will be made using an automatic dialing machine or a pre-recorded voice message, whether a purchase is required, and whether there is a charge for the text. The same statute authorised the establishment of the national Do-Not-Call list which allows individuals to submit their telephone numbers to a national registry inclusion which prohibits marketing calls to such number.

Other federal statutes do not require opt-in consent, just the provision of an opt-out. For instance, under CAN-SPAM, marketing emails may be sent to those not opting out provided the sender is accurately identified, the subject line and text of the email are not deceptive, the email contains the name and address of the sender, the email contains a free, simple mechanism to opt-out of future emails that remains operational for 60 days, and the sender honours opt-outs within 10 days of receipt.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.)

Marketing by telephone is regulated on the national level by the Telemarketing Sales Rule, a regulation under the Telephone Consumer Protection Act. This regulation established the national Do-Not-Call list of telephone numbers that cannot be used for marketing calls and disclosure requirements for companies engaging in telephone marketing. It also proscribes limitations on the use of telephone marketing, including, for instance, limiting times when marketing calls may be placed, requiring the caller to provide an opt-out of future calls, and limiting the use of pre-recorded messages.

There are no consent or opt-out requirements for sending marketing materials through the mail.

It should be noted that the Federal Trade Commission Act, which regulates deceptive practices, has been used to enforce, as a deceptive practice, the transmission of marketing emails or telemarketing calls by companies who have made promises in their publicly posted privacy policies that personal information will not be used for marketing purposes. Additionally, many states have deceptive practices statutes that are used to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed to be a deceptive practice under state law.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, if the recipient is within the United States.

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

The FTC and the Attorneys General of the states are active in enforcement in this area.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes; however, the purchaser of the list must scrub it against the national Do-Not-Call list and the purchaser's email opt-out lists. Some states forbid the sale of email addresses of individuals who have opted out of receiving marketing emails and some forbid the sale of information obtained in connection with a consumer's purchase transaction.

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

The penalties under CAN-SPAM are $16,000 per email for an isolated or unintentional violation; penalties can increase to the current maximum of $41,484 (as of 2018) for flagrant or repeated violations. The penalties under the Telephone Consumer Protection Act are $500 for each text message or call sent in violation of the Act, the amount of which may be trebled in the case of intentional or flagrant violations. By way of example, the FTC and the attorneys general of several states obtained a judgment of $260 million in 2017 for violation of the Telephone Consumer Protection Act.

Many states have their own deceptive practices statutes which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under the state statute.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Federal Consumer Fraud and Abuse Act has been used as the basis for enforcement actions against companies that use cookies for behavioural advertising, where the cookie enables deep packet inspection of the computer on which it is placed. At least one state (California) requires disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time.

In addition, the Federal Trade Commission Act and state deceptive practices acts have been used as the basis for regulatory enforcement and private class action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One such action was settled in 2012 with a payment of $22.5 million to the FTC; the same company agreed in 2016 to pay $5.5 million to settle a private class action involving the same conduct.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Computer Fraud and Abuse Act comes into play where cookies collect information from the computer on which they are placed and report that information to the entity placing the cookies.

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

Yes, on both the regulatory side through the FTC and on the privacy side through class action lawsuits.

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

Maximum penalties are not set by statute.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The US does not place restrictions on the transfer of personal data to other jurisdictions.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

This is left to the discretion of the company.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, they do not.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is a Federal Whistle-blower Protection Act protecting federal employees, and some states have similar statutes protecting state

© Published and reproduced with kind permission by Global Legal Group Ltd, London

employees. Public companies subject to the Sarbanes-Oxley Act are required to have a Whistle-blower Policy which must be approved by the board of directors and include a definition of whistle-blowing, the individuals covered, non-retaliation provisions, confidentiality, processes and enforcement measures.

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?

This is not specified.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV must comply with state criminal eavesdropping statutes which require posting signs where video monitoring is taking place.

13.2 Are there limits on the purposes for which CCTV data may be used?

The limitations would be based on the expectation of privacy that remains following disclosure of the CCTV recording by the company employing it, and any other policies issued by the company relating to data collected by this process.

14 Employee Monitoring

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

Employee privacy rights, like those of any individual, are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by agreement, statute or disclosure. Monitoring of employees is permitted where the employer makes clear disclosure regarding the type and scope of monitoring in which it engages.

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

Notice to employees is required in order to diminish their expectation of privacy.

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

This is not applicable.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Certain federal statutes and certain individual state statutes impose an obligation to ensure security of personal information. The Federal Gramm Leach Bliley Act and HIPAA impose such requirements on financial services and covered health care entities. Some states impose data security obligations on any entities that collect, hold or transmit limited types of personal information.

15.2 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.

At the federal level, data breach notification requirements are imposed under the Privacy Act (applicable to federal government agencies), the Federal Information Security Management Act (applicable to federal government agencies), the Office of Management and Budget Guidance (applicable to federal government agencies), the Veterans Affairs Information Security Act (applicable to the Department of Veterans Affairs), the Health Insurance Portability and Accountability Act (applicable to health plans, health care clearing houses, and health care providers who transmit financial and administrative transactions electronically and their business associates), the Health Information Technology for Economic and Clinical Health Act (applicable to health plans, health care clearing houses, and health care providers who transmit financial and administrative transactions electronically and their business associates), and the Gramm-Leach-Bliley Act (applicable to financial institutions and financial services entities).

HIPAA requires reporting an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information to the Department of Health and Human Services. If the breach involves more than 500 individuals, such notification must be made within 60 days of discovery of the breach. Information to be submitted includes information about the entity suffering the breach, the nature of the breach, the timing (start and end) of the breach, the timing of discovery of the breach, the type of information exposed, safeguards in place prior to the breach, and actions taken following the breach including notifications sent to impacted individuals and remedial actions.

While not specifically a data breach notification obligation, the Securities and Exchange Act and associated regulations, including Regulation S-K, requires public companies to provide notification through filings with the Securities and Exchange Commission when material events, including cyber incidents, occur. Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarise and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Some state statutes require reporting of data breaches to a state agency or attorney general under certain conditions. The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals and any services offered to impacted individuals such as credit monitoring. Some states require agency notification within a very short period of time (for example, New Jersey: 48 hours).

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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.

The Gramm Leach Bliley Act requires financial institutions and financial services entities to promptly report data breaches as defined in that Act to impacted individuals where a risk of harm is presented. HIPAA requires covered entities to report to impacted individuals, within 60 days, data breaches as defined in that statute.

As of May 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the US Virgin Islands have statutes that require reporting data breaches as defined in each statute to impacted individuals. These statutes are triggered by the exposure of personal information of a resident of the jurisdiction, so if a breach occurs involving residents of multiple states, then multiple state laws must be followed. Most statutes define a "breach of the security of the system" as involving unencrypted computerised personal data, but some states include personal data in any format. Triggering personal data varies by statute, with most including an individual's first name or first initial and last name together with a data point including the individual's Social Security Number, driver's licence or state identification card number or financial account number. Some states include data of birth, mother's maiden name, passport number, biometric data, employee identification number or user name and password as additional triggering data points. Standards for when disclosure is required vary from unauthorised access to personal information, to unauthorised acquisition of personal data, to misuse of or risk of harm to personal information. Most states require notification to be given as soon as practical, but at least one state (Florida) requires disclosure within 30 days of discovery of the incident and others within 45 days of discovery. The information to be submitted varies by state but generally includes a description of the incident, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, information about steps individuals should take to protect themselves, information resources and any services offered to impacted individuals such as credit monitoring.

15.4 What are the maximum penalties for data security breaches?

Not all states impose financial penalties for failure to report data security breaches, but Florida, for instance, can impose penalties of up to $500,000 for such a failure to timely report.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
See below.		

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The US does not have a central data protection authority. Authority to enforce is specified in the relevant statutes. Some include only federal government enforcement, some allow for federal or state government enforcement and some allow for enforcement through a private right of action by aggrieved consumers. Whether the sanctions are civil and/or criminal depends on the relevant statute.

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

This depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures.

16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

Extraterritorial enforcement of a US law would depend on a number of factors including whether the entity is subject to the jurisdiction of the US courts, the impact on US commerce and the impact on US residents, among other factors.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Typically, such requests must be processed through the local courts or law enforcement.

17.2 What guidance has/have the data protection authority(ies) issued?

Since there is no central data protection authority, and since the agencies tasked with enforcement of certain statutes also enforce non-data protection issues there is no central repository of guidance. By way of example, the FTC has issued guidance on a variety of issues including children's privacy, identity theft and telemarketing. State Attorneys General have, in some cases, offered resources on their websites for victims of identity theft and for companies suffering data security breaches. The Department of Health and Human Services has issued information on compliance with HIPAA.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

18 Trends and Developments

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

The FTC remains active in enforcing deceptive practices including those involving marketing and security, though not specifically in the area of data protection. The DHHS remains active in enforcing HIPAA violations. Class action lawsuits alleging improper telephone recording and text messaging remain active, particularly where the statute includes a minimum financial penalty.

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

See above.

Deborah Thoren-Peden
Pillsbury Winthrop Shaw Pittman LLP
725 South Figueroa Street
Los Angeles
CA 90017
USA

Tel: +1 213 488 7320
Email: deborah.thoren-peden@pillsburylaw.com
URL: www.pillsburylaw.com

Deborah Thoren-Peden focuses her practice on privacy, banking, e-commerce, anti-money laundering and Office of Foreign Assets Control regulations. She co-leads the firm's Cybersecurity, Data Protection & Privacy team. Ms. Thoren-Peden advises a spectrum of industries on the laws and regulations related to privacy, data mining, and the ability to use such information for marketing purposes and share it with others. She has prepared numerous privacy policies and procedures for a wide variety of companies, both domestic and international. She was the Chief Privacy Officer of PayMyBills.com and served on the Privacy Task force of the American Bankers Association.

Catherine D. Meyer
Pillsbury Winthrop Shaw Pittman LLP
725 South Figueroa Street
Los Angeles
CA 90017
USA

Tel: +1 213 488 7362
Email: catherine.meyer@pillsburylaw.com
URL: www.pillsburylaw.com

Catherine D. Meyer is recognised by *The Legal 500 U.S.* as an authority on data protection, privacy and cyber law. Her practice includes: advising individuals and businesses on financial privacy rights and compliance; protecting customers' privacy under state, federal and international statutes and regulations; assisting clients when personal information is compromised or threatened; and responding to data breaches. Well versed in regulations regarding the collection, use, sale, transfer and sharing of customer information for commercial purposes, Ms. Meyer regularly counsels on marketing issues applicable to various communications channels and compliance with international privacy directives.

Pillsbury is a leading international law firm with 700+ lawyers located around the world. The firm has been recognised as one of the Most Innovative Law Firms by *Financial Times* three years running, and is one of the 25 law firms most frequently recommended by general counsel according to a 2016 BTI Consulting Group survey. Recognised by *The Legal 500* as one of the world's foremost practices, Pillsbury offers unparalleled experience and knowledge in connection with critical cyber security, data protection and privacy law issues. Pillsbury has advised businesses on all manner of data privacy issues. Our uncommon insight, combined with an expansive network of government and regulatory connections at the highest levels, affords clients unparalleled resources for navigating and tackling their data-related challenges.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

© Published and reproduced with kind permission by Global Legal Group Ltd, London

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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 Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com