Global Data and Cyber Handbook - United States

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

In 2024, US privacy and cybersecurity law continued to evolve, reflecting a continued focus on consumer protection and data governance.

Key federal developments include the Federal Trade Commission's initial enforcement of the updated **Health Breach Notification Rule (HBNR)**, which emphasizes accountability for unauthorized health data disclosures. The Cybersecurity and Infrastructure Security Agency (CISA) developed a Notice of Proposed Rulemaking, and has begun reviewing public comments as it moves towards promulgating the Final Rules for the **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).** President Biden's **Executive Order 14117** and the **"Protecting Americans' Data from Foreign Adversaries Act"** were both passed to heighten the review processes for transferring personal data to countries of concern and allow the federal government to block transactions involving sensitive data transfers that pose national security risks.

Several states also expanded their consumer privacy protections. **Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Rhode Island** enacted new privacy laws. Some laws, on the other hand, faced constitutional scrutiny. Notably, the **California Age-Appropriate Design Code** faced a preliminary injunction from the Ninth Circuit in light of its data protection impact assessment requirement.

Additionally, the California Privacy Protection Agency (CPPA) commenced formal rulemaking on Draft Regulations that will impose new requirements on the use of AI and automated decision-making tools, cybersecurity audits and risk assessments.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 31 December 2024*

☒  omnibus – all personal data.

A number of states have enacted omnibus statutes, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia. Certain laws are already in effect (California, Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, Oregon, Texas, Utah, and Virginia), while the laws of the other states will be effective in a staggered way in 2025-2026. All states have data breach notification laws, but the definition of personal data varies.

☒  sector-specific

Most federal privacy and cybersecurity laws are sector-specific, including laws protecting medical, banking/finance, and children's data. Certain state privacy laws specific to consumer health data have been enacted (e.g., California, Connecticut, Nevada, and Washington). States have also enacted privacy laws governing a variety of sectors, including biometric information, children’s and teenagers' data, credit data and other types of data.

## What are the key data privacy laws and regulations?

*Last review date: 31 December 2024*

Key federal data privacy include:

[Gramm-Leach-Bliley Act](https://www.sec.gov/about/laws/glba.pdf) (GLBA)

[Health Insurance Portability and Accountability Act](https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf) (HIPAA)

[Controlling the Assault of Non-Solicited Pornography and Marketing Act](https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf) (CAN SPAM Act)

[Children's Online Privacy Protection Act](https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa) (COPPA)

[Fair Credit Reporting Act](https://www.ecfr.gov/cgi-bin/text-idx?SID=2b1fab8de5438fc52f2a326fc6592874&amp;amp;amp;amp;amp;mc=true&amp;amp;amp;amp;amp;tpl=/ecfrbrowse/Title16/16CIsubchapF.tpl) (FCRA)

[Section 5 of the Federal Trade Commission Act](https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf) (FTC Act)

[Telemarketing Sales Rule](https://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&amp;amp;amp;amp;amp;mc=true&amp;amp;amp;amp;amp;tpl=/ecfrbrowse/Title16/16cfr310_main_02.tpl) (TSR)

[Telephone Consumer Protection Act](https://www.govinfo.gov/content/pkg/FR-2012-06-11/pdf/2012-13862.pdf) (TCPA)

Key state data privacy laws include:

[California Consumer Privacy Act](file:///C:/Users/chigxh/Downloads/20170SB1121_90%20(7).pdf) (CCPA), as amended by the [California Privacy Rights Act](https://oag.ca.gov/privacy/ccpa) (CPRA)

[California Online Privacy Protection Act](https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&amp;amp;amp;amp;amp;chapter=22.&amp;amp;amp;amp;amp;lawCode=BPC) (CalOPPA)

[California Age-Appropriate Design Code Act](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273) (CalAADCA), which is currently subject to a constitutional challenge

[Colorado Privacy Act](https://leg.colorado.gov/bills/sb21-190) (CPA)

[Colorado Artificial Intelligence Act](https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf) (CAIA)

[Connecticut Data Privacy Act](https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act) (CTDPA)

[Delaware Personal Data Privacy Act](https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=140388&amp;legislationTypeId=1&amp;docTypeId=2&amp;legislationName=HB154) (DPDPA)

[Indiana Consumer Data Protection Act](https://iga.in.gov/legislative/2023/bills/senate/5/details) (INCDPA)

[Iowa Consumer Data Protection Act](https://www.legis.iowa.gov/legislation/BillBook?ga=90&amp;ba=SF%20262) (IACDPA)

[Kentucky Consumer Data Protection Act](https://apps.legislature.ky.gov/recorddocuments/bill/24RS/hb15/bill.pdf) (Kentucky CDPA)

[Maryland Age-Appropriate Design Code Act](https://mgaleg.maryland.gov/2024RS/Chapters_noln/CH_461_hb0603t.pdf)

[Maryland Online Data Privacy Act](https://mgaleg.maryland.gov/2024RS/bills/hb/hb0567E.pdf)

[Minnesota Consumer Data Privacy Act (MCDPA)](https://www.revisor.mn.gov/bills/text.php?number=HF4757&amp;type=bill&amp;version=4&amp;session=ls93&amp;session_year=2024&amp;session_number=0&amp;format=pdf)

[Montana Consumer Data Privacy Act](https://archive.legmt.gov/bills/2023/billpdf/SB0384.pdf) (MTCDPA)

[Nebraska Data Privacy Act](https://nebraskalegislature.gov/FloorDocs/108/PDF/Slip/LB1074.pdf) (NDPA)

[Nevada Consumer Health Privacy Act (Nevada Senate Bill 370](https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text))

[New Hampshire Consumer Privacy Law (New Hampshire Senate Bill 255](https://legiscan.com/NH/text/SB255/id/2871280))

[New Jersey Data Privacy Law](https://www.njleg.state.nj.us/bill-search/2022/S332/bill-text?f=S0500&amp;n=332_R6) (NJDPA)

[Oregon Consumer Privacy Act](https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled) (OCPA)

[Rhode Island Data Transparency and Privacy Protect Act](https://legiscan.com/RI/text/S2500/2024)

[Tennessee Information Protect Act](https://www.capitol.tn.gov/Bills/113/Bill/HB1181.pdf) (TIPA)

[Texas Data Privacy and Security Act](https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm)

[Utah Consumer Privacy Act](https://le.utah.gov/~2022/bills/static/SB0227.html) (UCPA)

[Virginia Consumer Data Protection Act](https://law.lis.virginia.gov/vacode/title59.1/chapter53/) (VCDPA)

[Washington My Health My Data Act](https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf?q=20230418051959https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf?q=202https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf?q=2023041805195930418051959) (MHMDA)

[New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies](https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf) (NYDFS CR)

State laws establishing data protection and breach notification requirements; most of these laws focus on the protection of Social Security Numbers, individual identification numbers, financial account numbers, health/medical data, and other sensitive personal data

## What are the key cybersecurity laws and regulations?

*Last review date: 31 December 2024*

[Section 5 of the Federal Trade Commission Act](https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf) (FTC Act)

[FTC Health Breach Notification Rule](https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule) (HBNR)

[Gramm-Leach-Bliley Act](https://www.sec.gov/about/laws/glba.pdf) (GLBA)

[Health Insurance Portability and Accountability Act](https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf) (HIPAA)

[Federal Information Security Management Act](https://www.cisa.gov/federal-information-security-modernization-act) (FISMA)

[Securities and Exchange Commission (SEC) Cybersecurity Rules](https://www.sec.gov/rules-regulations/2023/07/s7-09-22#33-11216)

[Cyber Incident Reporting for Critical Infrastructure Act of 2022](https://www.congress.gov/bill/117th-congress/house-bill/2471/text) (CIRCIA)

[Defense Federal Acquisition Regulation Supplement](https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.) (DFARS) - Safeguarding Covered Defense Information and Cyber Incident Reporting

[Cybersecurity and Infrastructure Security Agency Act](https://www.congress.gov/bill/115th-congress/house-bill/3359) (CISAA)

[New York State Department of Financial Services Cybersecurity Requirements](https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf) (NYDFS) CR and [New York SHIELD Act](https://ag.ny.gov/internet/data-breach)

Payment Card Industry Data Security Standard (PCI DSS)

State data security and breach notification laws

## What are the key laws and regulations relating to non-personal data?

*Last review date: 31 December 2024*

[Section 5 of the Federal Trade Commission Act](https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf) (FTC Act)

Prohibits unfair or deceptive practices, including misuse of non-personal data

[Computer Fraud and Abuse Act](https://www.justice.gov/jm/jm-9-48000-computer-fraud) (CFAA)

Regulates unauthorized access/misuse of non-personal computer data and systems

[Cyber Incident Reporting for Critical Infrastructure Act of 2022](https://www.congress.gov/bill/117th-congress/house-bill/2471/text) (CIRCIA)

[Cybersecurity Information Sharing Act](https://www.congress.gov/bill/114th-congress/senate-bill/754) (CISA)

Facilitates sharing of cyber threat indicators between government and private entities

[Defend Trade Secrets Act](https://www.congress.gov/bill/114th-congress/senate-bill/1890) (DTSA)

Protects misappropriation of trade secrets by providing for federal civil remedies

[Export Administration Regulations](https://www.bis.gov/regulations) (EAR)

Controls the export of commercial, dual-use, and some non-personal technical data for national security

[International Traffic in Arms Regulation](https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&amp;sys_id=24d528fddbfc930044f9ff621f961987) (ITAR)

Regulates the export of defense-related articles, services, and technical non-personal data for military purposes

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 31 December 2024*

Yes. A number of states (i.e., Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia) have joined California in enacting consumer privacy laws that impose broad obligations on businesses to provide consumers with transparency and control of personal data. More states are expected to enact similar legislation. There has also been a movement towards federal consumer privacy legislation (such as the proposal of the "American Privacy Rights Act of 2024"). Most of these laws also impose security obligations on businesses. The NY DFS has outlined cybersecurity regulations for covered financial services companies. Nevada and Washington have enacted broad and prescriptive consumer health privacy laws that include signed authorization requirements for regulated entities that "sell" consumer health data. A number of states, including Arkansas, California, Connecticut, Florida, Louisiana, Texas, and Utah have also recently enacted children's privacy and protection laws, some of which are currently being challenged on constitutional grounds. Colorado has enacted a comprehensive law relating to the development and deployment of certain artificial intelligence systems. The California Privacy Protection Agency (CPPA) is concurrently considering a regulatory framework for automated decision-making technologies. Additional changes to privacy and cybersecurity enforcement are anticipated under the incoming administration.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 31 December 2024*

Given the patchwork of federal and state privacy and cybersecurity laws, companies are exposed to enforcement from various state and federal sources. Data privacy laws are enforced at the state level by the Attorney General in each state, and at the federal level by consumer protection agencies and regulators, including:

[Federal Trade Commission](https://www.ftc.gov/) (FTC)

[Federal Communications Commission](https://www.fcc.gov/) (FCC)

[Federal Consumer Financial Protection Bureau](https://www.consumerfinance.gov/) (CFPB)

[Department of Health and Human Services](http://www.hhs.gov/) (HHS) Office of Civil Rights (OCR)

[Department of Justice](https://www.justice.gov/) (DOJ)

Office of Foreign Assets Control (OFAC) of the US Department of the Treasury

[Securities and Exchange Commission](https://www.sec.gov/) (SEC)

[California Privacy Protection Agency](https://cppa.ca.gov/) (CPPA), which has enforced the CCPA in cooperation with the California Attorney General since 1 July 2023.

[NY Department of Financial Services](https://www.dfs.ny.gov/)

## How active is each of the regulator(s)?

*Last review date: 31 December 2024*

Very active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 31 December 2024*

Under the incoming administration, federal enforcement activity will likely decrease, and certain state enforcement activity will likely increase.

The Federal Trade Commission ([FTC](https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement)) and the US Department of Health and Human Services ([HHS](https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html)) report on privacy and cybersecurity enforcement actions. Most of the FTC's enforcement actions charge defendants with unfair and deceptive acts and practices, and/or for violations of COPPA. The FTC issued a policy statement in September 2021, warning health apps and connected device companies to comply with the Health Breach Notification Rule's (HBNR) notification requirements to consumers, the FTC, and, in some cases, the media when personal health records are disclosed or acquired without the consumers' authorization. Following this statement, in 2022, the FTC published a new interactive tool for mobile health application developers to help them understand which federal regulations might apply to their products. The agency has since pursued two enforcement actions under its HBNR authority.

The California Office of the Attorney General and California Privacy Protection Agency are expected to continue and strengthen their [enforcement of the amended CCPA](https://oag.ca.gov/privacy/ccpa/enforcement), focusing on lack of privacy notice to consumers, insufficient "do not sell my personal information" opt-out tools, inaccurate disclosures of data collection and use practices, and insufficient processes for accepting and responding to rights requests. California privacy authorities have also released announcements of investigative sweeps, including with respect to connected cars, employers' processing of personnel data, and mobile apps in the retail, travel, and food service sectors. Attorneys General in Colorado and Connecticut have similarly begun pursuing privacy enforcement actions, with the Texas Attorney General taking a firm stance against unlawful biometric data collection.

The Washington Attorney General's office is expected to enforce violations of the Washington My Health My Data Act under the Washington Consumer Protection Act.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 31 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒  Common

If applicable, they are:

☒  Increasing

Class actions/group actions under data or cyber regulation are:

☒  Common

Most state privacy legislation precludes private rights of action, but the Children’s Internet Protection Act (CIPA) and the Illinois Biometric Information Privacy Act (BIPA) attract a significant number of class action claims.

If applicable, they are:

☒  Increasing

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 31 December 2024*

There are:

☒   administrative remedies/civil penalties imposed by regulators and law enforcement

Many privacy laws at the federal and state levels establish administrative remedies/civil penalties for non-compliance. For example, HHS may impose a civil money penalty on any person who violates the HIPAA Privacy Standards ranging from USD 100 to USD 50,000 per violation, with a total of USD 25,000 to USD 1.5 million for all violations of a single requirement in a calendar year.

The FTC may bring civil actions for civil monetary penalties of up to USD 40,000 per violation of the FTC Act or COPPA. Each day that non-compliance continues is considered a separate "violation" for purposes of the law.

If an organization enters into a consent decree with the FTC, any subsequent violations of the consent decree are subject to penalties of up to approximately USD 42,000 (periodically adjusted for inflation) per violation.

The FTC and financial regulatory authorities also have the power to bring civil actions for damages related to GLBA. In the context of the FTC, potential consequences include: rescission or reformation of contracts; monetary refunds or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary penalties; public notification of the violation; and limits on the violator's functions. Civil monetary penalties range from USD 5,000 to USD 1 million per day of violation if an individual knowingly violates the law.

States also impose consequences for non-compliance with state privacy laws. For example, the CCPA imposes civil penalties for data breaches that range from USD 2,500 to USD 7,500 per violation. The VCDPA imposes civil penalties of up to USD 7,500 per violation and injunctive relief. The CPA imposes civil penalties of up to USD 20,000 per violation and injunctive relief.

☒   criminal penalties from regulators and law enforcement

Violations of HIPAA can include criminal penalties, including up to ten years’ imprisonment in certain cases.

☒   private remedies

CCPA allows an individual to bring a private right of action against businesses and imposes statutory damages ranging from USD 100 to USD 750 per consumer, per incident, or actual damages, whichever is greater. Illinois' Biometric Information Privacy Act (BIPA) provides a private right of action for the unauthorized collection, use, or disclosure of biometric data, allowing individuals to seek statutory damages of USD 1000 per negligent violation.

## If data subjects have private remedies, what form can these remedies take?

*Last review date: 31 December 2024*

☒   individual personal actions

☒  representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒   class actions

# Key Definitions

## Personal data

*Last review date: 31 December 2024*

Some US privacy laws use the term "personal data" while others use similar varying terms, such as "personal information" or "personally identifying information."  However, these terms are not consistently defined in US law.

For example, the CCPA refers to two different definitions of the same term "personal information." The first definition broadly defines "[p]ersonal information" as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” Cal. Civ. Code § 1798.140(v)(1).  This definition applies to privacy-related rights and obligations under CCPA.

The second definition of "personal information" is narrow and applies to "reasonable security procedures and practices" and includes:

An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

Social Security number

Driver's license number, identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual

Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

Medical information

Health insurance information

Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes

Information or data collected through the use or operation of an automated license plate recognition system

Genetic data

A username or email address in combination with a password or security question and answer that would permit access to an online account. Cal. Civ. Code § 1798.81.5(d)(1) and § 1798.82.

HIPAA regulates protected health information (PHI), which is defined as demographic data that either identifies or could reasonably identify an individual and which relates to:

Past, present, or future physical or mental health condition of an individual

The provision of health care to an individual

Past, present, or future payment for the provision of health care to an individual

GLBA regulates the use of (non-public) personal information in the financial services industry. The Act broadly defines "non-public personal information" as personally identifiable financial information that includes a consumer's name, contact details, and financial transaction information.

In the Washington My Health My Data Act, consumer health data is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." The act specifies that the definition includes "any information that a regulated entity or a small business or their respective processor processes to associate or identify a consumer with" certain enumerated health data elements "that is derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)."

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 31 December 2024*

Sensitive data includes:

☒   personal data revealing racial or ethnic origin

☒   personal data revealing political opinions

☒   personal data revealing religious or philosophical belief

☒   personal data revealing trade union membership

☒   genetic data

☒   precise geolocation data

☒   biometric data for the purpose of uniquely identifying a natural person

☒   data concerning health/medical information

☒   data concerning a natural person's sex life or sexual orientation

☒   financial information

☒   government identity card or number information

☒   passwords

☒   other

Citizenship

Immigration status

California's data breach notification laws define "personal information" as a consumer's social security, driver's license, state identification card, or passport number; a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's precise geolocation; the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; a consumer's genetic data.

The CCPA defines sensitive personal information (SPI) as a subset of personal information that is more sensitive in nature. SPI includes: (i) government identifiers including Social Security numbers, driver's licenses, state IDs, or passport numbers; (ii) financial account information, which includes account logins, financial account numbers, debit card numbers, or credit card numbers, along with any required security codes, passwords, or credentials; (iii) precise geolocation; (iv) contents of a consumer's mail, email, and text messages, unless the business is the intended recipient: (v) genetic data; (vi) biometric information; (vii) information concerning a consumer's health, sex life, or sexual orientation; and (viii) information about a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

## Controller vs Processor

*Last review date: 31 December 2024*

Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** Yes, depending on the state. Some US privacy laws use the terms "controller" and "processor," including the consumer privacy laws in Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia. In addition, many US privacy laws utilize similar concepts like "service providers" (even if they do not specifically refer to "controllers" and "processors") and apply different obligations depending on the roles of the parties. For example, the CCPA applies different obligations to "businesses," "third parties," "service providers," and "contractors" with most obligations flowing to businesses, and HIPAA similarly establishes different obligations for covered entities and business associates (entities acting essentially as a service provider to the covered entities). Moreover, most data breach notification laws impose notice obligations on the "data owners," and typically require service providers (which maintain data on behalf of a data owner) to notify the data owner of the breach. All other notification obligations would generally flow to the data owner.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 31 December 2024*

☒   applies to organizations located in the jurisdiction

☒   applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction

☒   applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

☒   other

US laws define their territorial scope differently, with some establishing broad application and others having a more narrow application. Nevertheless, many US privacy laws, particularly the CCPA, VCDPA, CPA, CTDPA, and UCPA and state breach notification laws, are tied to the residency of impacted individuals. Notably, Nevada and Washington's recent consumer health privacy laws broadly protect natural persons whose consumer health data is collected in those states.

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 31 December 2024*

No.

The following are potential legal bases for processing non-sensitive personal data:

☒   other

US laws generally allow processing of personal data by default, and companies do not have to show a "legal basis" as required by the privacy laws of other jurisdictions, with certain limited exceptions (e.g., COPPA generally requires a verifiable parental consent before collection of personal data online from children under 13 years of age and various state consumer privacy laws prohibit processing sensitive data without consent). The CCPA requires businesses to limit businesses' collection, use, retention, and sharing of personal information of California residents to what is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes," Cal. Civil Code §1798.100(c).

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 31 December 2024*

Yes, under some circumstances under some state privacy laws.

Depending on the law and circumstances at issue, the following may be potential legal bases for processing special categories of personal data:

☒   the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data

☒   the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☒   processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

☒   processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☒   processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☒   processing relates to personal data which are manifestly made public by the data subject

☒   processing is necessary for the establishment, exercise or defense of legal claims

☒   processing is necessary for reasons of substantial public interest

☒   processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☒   processing is necessary for reasons of public interest in the area of public health

☒   processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

☒   other

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 31 December 2024*

Yes. COPPA governs the collection and use of personal information from children under the age of 13. The CCPA applies additional requirements for children under the age of 16, while the California Age-Appropriate Design Code, which is subject to a constitutional challenge, applies additional requirements to children under the age of 18. A number of children's privacy and protection laws, including in Arkansas, Connecticut, Florida, Louisiana, Texas, and Utah may also impose privacy and other obligations on companies that process minors' personal information in certain circumstances.

## In what circumstances do these special requirements apply?

*Last review date: 31 December 2024*

COPPA applies to online data collection of minors under 13 years of age and requires that consent must be obtained from a parent or guardian under certain circumstances (including if a website is directed at minors or the operator knowingly collects personal data from minors). The CCPA requires parental consent for minors under the age of 13 to sell personal data of such minors and the consent of minors between 13 and under the age of 16 to sell their personal data. The California Age-Appropriate Design Code Act, if it is found to be constitutional, applies to the online data collection of children under the age of 18 and requires companies to take a privacy by design approach to the design of new online products or services targeted to California minors. The Ninth Circuit recently issued a preliminary injunction against the law's enforcement in light of its data protection impact assessment (DPIA) requirement. Maryland's Age-Appropriate Design Code Act is expected to face similar scrutiny, Other state children's privacy laws apply in different circumstances.

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 31 December 2024*

☒  consent must be given or authorized by the parent/ guardian of the minor

☒  additional data subject rights are granted to minors (e.g., deletion, access, transparency)

Under California law, minors must be able to revoke posts on social media about themselves.

☒  additional data security requirements may apply.

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 31 December 2024*

☒   the identity and the contact details of the controller and, where applicable, of the controller's representative

☒   the purposes of the processing for which the personal data is intended

☒   the categories of personal data concerned

☒   the source from which the personal data originates and, if applicable, whether it came from publicly accessible sources

☒   the recipients or categories of recipients of the personal data, if any

☒   the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

☒   the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

☒   the existence of the right to withdraw consent if processing is based on consent

☒   the security provided to the data

☒   the right to lodge a complaint with a supervisory authority.

☒   whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

☒   if applicable, information regarding automated decision making, including profiling (Note: the CCPA, CPA, CTDPA, and VCDPA, for example, include a right to opt-out of profiling; the UCPA does not).

☒   other.

Each law contains different requirements regarding the format, content and organization of privacy notices. The CCPA contains particularly prescriptive and detailed requirements, including the obligation for companies to notify consumers about their rights. It also details the types of disclosures of personal data, including disclosures that qualify as a "sale" or "share" under the CCPA, and the types of third parties to whom such disclosures are made. In other examples, the Washington My Health My Data Act uniquely requires regulated entities to disclose in their online privacy disclosures by name every affiliate not acting as a data processor that consumer health data is disclosed to. COPPA requires that a separate privacy notice be issued directly to parents of children from whom a covered operator collects personal information.

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 31 December 2024*

Yes.  Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒   right to access the data subject's own personal data

☒   right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒   right to erasure of personal data

☒   right to restrict data processing

☒   right to data portability

☒   right to object to the processing of personal data

☒   right to withdraw consent

☒   other

CCPA offers California residents, e.g., data access, deletion, and portability rights, as well as the right to opt-out of the sale of their personal data. Additionally, from 1 January 2023, California residents also have the right to correct personal information and limit the use of sensitive personal information. HIPAA offers access rights to patients.

## Are there accountability and governance requirements?

*Last review date: 31 December 2024*

Yes. There are accountability and governance requirements to:

☒   take privacy by default and design measures for all processing of personal data

☒   perform and document data protection impact assessments (DPIAs) for high-risk processing:

☒   implement appropriate measures to comply with data privacy and security

☒   demonstrate compliance with data privacy and security

☒   identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒   provide training to employees

☒   audit or supervise data processors

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 31 December 2024*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: 31 December 2024*

Yes

If yes, under what circumstances?

☒   other

Privacy and security officer requirement under HIPAA. Additionally, under the GLBA's Safeguards Rule passed in 2021 by the FTC, a financial institution must have a "qualified individual" overseeing the implementation of its information security program. In addition, the NYDFS CR requires the designation of a chief information security officer.

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 31 December 2024*

Yes.

If yes, what are these requirements?

☒   other

HIPAA does not set out express requirements, but the HIPAA privacy and security officers must be qualified to administer the respective obligations under the HIPAA Privacy and Security Rules. The GLBA states that qualified individuals overseeing information security programs must have "some level of information security training and knowledge." NYDFS CR specifies that the designated chief information security officer must be qualified and responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy and must report in writing at least annually to the covered entity's board of directors or equivalent governing body.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 31 December 2024*

No, but exceptions do apply. For example, Vermont and California require data brokers to register and there are other registration requirements that are emerging.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 31 December 2024*

Yes. The obligations are as follows:

☒   controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

☒   controllers must only use processors subject to a written agreement that complies with specific requirements. The CCPA requires businesses to enter into written contracts with service providers. The VCDPA and the CPA also require data controllers to enter into contracts with processors that govern the processor's data processing procedures performed on behalf of the controller.

☒   other

The GLBA Safeguards Rule requires covered financial institutions to conduct periodic assessments of the security practices of service providers.

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 31 December 2024*

Yes. Various federal and state privacy laws impose direct obligations on processors (or equivalent terms). For example, under HIPAA, business associates have various direct regulatory obligations related to data security and breach notification. Similarly, many state data breach notification laws impose direct obligations on service providers that maintain data on behalf of data owners to report data security incidents to the data owners.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 31 December 2024*

No, except in limited cases. The Biden Administration's Executive Order 14117 imposes heightened review processes for transfers of personal data and prohibits data sharing with foreign entities linked to "countries of concern." Pursuant to EO 14117, the US Department of Justice issued a new rule "Pertaining to Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 4410-PF, 28 CFR Part 202, Docket No. NSD 104, RIN 1124-AA01 to regulate, restrict, and in some cases prohibit the sharing of United States Government-related data or bulk US Sensitive Personal data with "countries of concern." The Rule contains very complex and broad definitions and will affect companies or businesses operating within the "countries of concern." The "Protecting Americans' Data from Foreign Adversaries Act" further authorizes the federal government to block transactions involving sensitive data transfers that pose national security risks.

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 31 December 2024*

Yes. Under California privacy laws, a number of companies have been sued based on unfair competition and misrepresentation theories for failure to provide adequate disclosures regarding cookies in privacy policies, attempts to disable consumer attempts to block or delete certain types of cookies and placement of certain particularly intrusive tracking technologies without consent. Under CalOPPA, operators of websites and online services must disclose in privacy policies how they respond to "Do Not Track" signals and similar privacy protection measures selected by consumers and if and to what extent third parties collect personal data regarding consumers on websites or via online services. In addition, under the CCPA, CPA, the VCDPA, and other state privacy laws, the use of cookies and related data sharing for advertising purposes may be subject to opt-out rights depending on the circumstances. Private individuals have used CIPA and VPPA to bring claims against companies for unlawfully intercepting or disclosing personal information collected through cookies, web tracking technologies, or other online monitoring tools.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 31 December 2024*

Yes. At the federal level, the CAN SPAM Act, 15 U.S. Code § 7701 et seq., regulates commercial email marketing activities, and telemarketing practices are subject to regulation under the Telemarketing Sales Rule (TSR), 16 CFR PART 310, as well as the Telephone Consumer Protection Act (TCPA), 47 U.S. Code § 227 et seq. and its implementing rules. More broadly, given the current sector-, activity- and data type-specific framework of US privacy laws, the specific requirements vary based on industry marketing regulations and state-specific marketing laws.

**☒   email marketing**

☒opt-out or implied consent

**☒   telephone marketing**

☒prior opt-in consent. Tele-marketers using robocalls or auto-dialers must obtain prior express consent before using such methods in their marketing.

☒opt-out or implied consent. The TCPA also requires that opt-out options be provided to persons who receive certain exempted telemarketing calls.

**☒   SMS/text message marketing**

☒prior opt-in consent

**☒**   **online behavioral advertising targeting/social media targeting/ad personalization marketing**

☒   opt-out or implied consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 31 December 2024*

No. In the US, collecting personal data about employees is generally seen as a legitimate activity, provided that it is carried out for non-discriminatory and legitimate business purposes. General restrictions to personal information processing under the CCPA apply in the employment context.

## Can consent be validly obtained in the employment context?

*Last review date: 31 December 2024*

Yes.

☒  Yes, same as for data subjects outside the employment context.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

Yes

Yes, the FTC and EEOC have issued guidance on the use of artificial intelligence (AI). The California Privacy Protection Agency has commenced formal rulemaking to impose transparency, opt-out, privacy impact assessment and other requirements on the use of AI and automated decision-making tools in certain circumstances. Read our most recent update [here](https://www.connectontech.com/off-to-the-races-california-advances-ccpa-regulations-on-cyber-risk-ai/).

In an employment context, certain local laws impose restrictions on the use of AI and automated decision-making. For example, New York City's Department of Consumer and Worker Protection (DCWP) adopted new rules regarding automated employment decision tools (AEDT), which took effect on 5 July 2023. Local Law 144 of 2021 prohibits employers and employment agencies from using AEDT tools unless the tool has been subject to a bias audit within one year of the use of the tool, information about the bias audit is publicly available, and certain notices have been provided to employees or job candidates. Read our alert [here](https://www.theemployerreport.com/2023/05/enforcement-of-new-york-citys-artificial-intelligence-rule-begins-july-5-2023-heres-what-employers-need-to-know/).

In August 2024, Illinois passed a law amending the Illinois Human Rights Act under which employers are subject to civil rights claims if they use AI tools in hiring and other employment decisions and cause discrimination. Employers will be required to notify employees whenever they use AI tools with respect to the "recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the terms, privileges, or conditions of employment." The amended law applies to discrimination based on the list of protected classes under Illinois law, as well as using "zip codes as a proxy for protected classes." The changes in law are set to take effect on 1 January 2026.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 31 December 2024*

Yes.

The restrictions or requirements are as follows:

☒   qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒   right to information / transparency requirement

☒   to request human review of the automated decision making

☒   other.

In 2018, California enacted a "[Bot Disclosure Law](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001)," effective from July 2019, under which online service providers must disclose the deployment of AI tools for online chats to prevent misleading consumers about whether they are communicating with a human or a machine. Utah enacted similar disclosure obligations in the Utah Artificial Intelligence Policy Act, which took effect in May 2024.

Under the CCPA, certain disclosures of personal information used to build consumer profiles must be disclosed and may be subject to a right to opt-out. The California Privacy Protection Agency is developing regulations on the processing of personal information for automated decision-making. Similarly, under some laws, such as the VCDPA and CPA, consumers have the right to opt-out of the use of their data for profiling purposes. Furthermore, under both of the same statutes, companies must carry out data protection impact assessments (DPIAs) on processes that involve processing data for the purpose of profiling consumers and other circumstances. As such, if AI is used in connection with targeted marketing, certain profiling, processing of sensitive personal data, or for purposes of making decisions with legal or substantially similar effects, there are obligations under these statutes to conduct and document a DPIA that meets local requirements.

Emerging AI laws include the right to request human review of automated decision making. For example, Colorado's Artificial Intelligence Act, due to take effect in February 2026, will require deployers using high-risk AI systems to make adverse consequential decisions concerning customers to provide such customers with a notice setting out the principal reason(s) for the consequential decision, information on how to correct any personal data inaccuracies that influenced the decision and how to appeal the decision, where the appeal must, if technically feasible, allow for human review.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 31 December 2024*

Yes. For example, the CCPA contains numerous exceptions and exemptions in deference to federal laws and the VCDPA contains exceptions regarding the kinds of "profiling" of consumer data allowed under the statute. Certain exceptions also apply to Colorado's Artificial Intelligence Act notice appeal provisions, including those for technical feasibility and the best interest of the consumer.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 31 December 2024*

Yes

***If yes, please provide brief details and a link.***

The FTC has issued guidance on AI. The California Privacy Protection Agency is currently soliciting public comment on its draft regulations that would, if enacted in their current form, impose transparency, opt-out, privacy impact assessment and other requirements on the use of AI and automated decision-making tools in certain circumstances. Read our most recent update [here](https://www.connectontech.com/off-to-the-races-california-advances-ccpa-regulations-on-cyber-risk-ai/).

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 31 December 2024*

☒  Enforcement activity against AI developer(s)

☒  Enforcement activity against AI user(s)/deployer(s)

☒  Enforcement activity under existing privacy, consumer protection or anti-discrimination law

☒  Enforcement activity by data or cyber regulator

☒  Enforcement activity by another regulator but relevant to AI, data or cyber compliance

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 31 December 2024*

☒   Yes, laws in force

☒   Draft legislation in progress

☒   Proposal for legislation or regulation at an early stage

☒   Non-binding guidance or principles issued or in progress

***If yes, please provide brief details and a link.***

There are numerous laws, regulations, judicial orders, executive orders and regulatory guidance documents in the US governing or addressing AI-related privacy topics.

For example, California enacted more than a dozen new AI-specific laws on concrete topics, including AB 2013 (Generative artificial intelligence: training data transparency), requiring developers of generative AI systems to publicly disclose information about the datasets used to train their models; SB 942 (California AI Transparency Act), requiring large AI developers to include watermarks for AI-generated content as well as provide tools for users to identify such content; AB 3030 (Health care services: artificial intelligence) requiring healthcare providers to disclose AI-generated patient communications that involve clinic information; SB 1120 (Health care coverage: utilization review) prohibiting health plans and insurers from using AI or other algorithms to supplant health care provider decision-making.

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 31 December 2024*

No

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 31 December 2024*

It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

## If so, how would any regulatory fines be calculated?

*Last review date: 31 December 2024*

Based on a metric other than those outlined above

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 31 December 2024*

Yes

## If so, how would any regulatory fines be calculated?

*Last review date: 31 December 2024*

Based on a metric other than those outlined above

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 31 December 2024*

Yes, although US laws vary. Some include requirements for:

☒   general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒   obligation to take specific security measures e.g., encryption

☒   requirement to undertake third party due diligence (security assessment of third party providers)

☒   reasonable security controls. The CCPA, CPA and the VCDPA require businesses to adopt reasonable security procedures and practices appropriate to the nature of the information held by the business.

☒   encryption.  Required under HIPAA, although not strictly required by US privacy laws, in most instances, encryption of personal data (where the encryption key is not compromised) will provide an exception to notification under US breach notification laws. The GLBA Safeguards Rule requires that entities regulated by GLBA encrypt information both in transit and at rest.

☒   other

Numerous state laws establish various affirmative security requirements for the protection of Social Security Numbers, financial account numbers, health/medical data, and other sensitive personal data.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 31 December 2024*

Yes.

☒  public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks).

On 26 July 2023, the US SEC approved final rules for Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Final Rules). The Final Rules require companies to disclose material cybersecurity incidents in a Form 8-K (or Form 6-K for Foreign Private Issuers) within four business days of a determination that the incident is material. Companies will be obligated to disclose their cybersecurity risks annually in their Form 10-Ks or Form 20-Fs, including with respect to any previous cybersecurity incidents that have materially affected the company or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition. Companies also have an obligation to explain how such cybersecurity incidents either affected or are reasonably likely to affect the company. The Final Rules also require the new disclosures to be tagged with Inline eXtensible Business Reporting Language (Inline XBRL).

☒   health regulatory requirements. The HIPAA Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information.

☒   financial services requirements. The Gramm-Leach-Bliley Act, as implemented through various regulatory actions, as well as various other federal and state financial privacy laws, requires safeguards for the protection of nonpublic personal information.

☒   telecommunication requirements. The Federal Communications Commission has implemented rules that require carriers to protect customer proprietary network information (CPNI) relating to customers, and other rules apply.

☒   providers of critical infrastructure. Under CIRCIA, covered entities will be required to report cyberattacks and ransomware payments within specified timeframes to the Cybersecurity and Infrastructure Security Agency once the final rule implementing CIRCIA's requirements goes into effect in early 2026.

☒   digital or connected (IoT) products

☒   other

The GLBA Safeguards Rule mandates financial institutions to employ data protection measures such as multifactor authentication.

If yes, please provide brief details of the relevant law or regulation.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last review date: 31 December 2024*

☒   Data privacy

☒   Securities or public company

☒   network information security

☒   health

☒   financial services

☒   telecommunications

☒   critical infrastructure

☒   other

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 31 December 2024*

Yes. Under various sector-specific federal regulations, breach notification obligations apply in particular sectors (e.g., energy, government contractors, healthcare, financial institutions, telecommunications, etc.). At the state level, each of the 50 states and Puerto Rico have established breach notification obligations that generally apply to unauthorized access or acquisition of categories of unencrypted sensitive personal data as specified in that state's law. Common data categories include Social Security Numbers, government-issued IDs, financial account information, health/medical information, and others. The definitions and conditions vary from state to state. For example, under California's security breach notification law, Cal. Civ. Code § 1798.82, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal data maintained by the person or business, where the "personal data" at issue can include a wide variety of government identifiers, financial information, health/medical information and more. Other rules, such as those issued by the SEC as described above, also apply.

## Controllers/Owners have to notify:

*Last review date: 31 December 2024*

US laws vary, but generally, a controller *may* have an obligation to notify:

☒   data protection authorities

Federal rules typically require notification to the appropriate federal regulators if the applicable thresholds are met. For example, HIPAA's Breach Notification Rule (45 C.F.R. §§164.400-414) requires covered entities to notify HHS and affected individuals for certain unauthorized acquisitions, accesses, uses or disclosures of protected health information (PHI) in certain circumstances.

Under certain state breach notification laws, in-scope entities that have experienced a data security breach must notify the applicable State Attorneys General if certain circumstances are met. For example, under Cal. Civ. Code § 1798.82(f), a company that is required to notify more than 500 individuals must also notify the California Attorney General. In certain states, such under Maryland Code, Commercial Law Section 14-3501 *et seq.*, the Attorney General must be notified prior to notification to any individuals.

☒   cybersecurity authorities. Telecommunications providers have duties to report cybersecurity incidents to law enforcement. Also, under CIRCIA, covered entities will be required to report cyberattacks and ransomware payments within specified timeframes to the Cybersecurity and Infrastructure Security Agency once the final rule implementing CIRCIA's requirements goes into effect.

☒   affected individuals, if applicable thresholds are met

☒   other

In certain circumstances and under various state laws, companies may be required to report certain cyber events to law enforcement and the United States Department of Defense. Depending on the volume of data impacted, state laws may require entities to notify consumer reporting agencies. Apart from privacy and regulatory duties, companies may also have contractual obligations to notify data incidents in certain cases, such as obligations to notify merchant banks and/or credit card brands of certain events involving payment card information.

## Processors/Agents have to notify:

*Last review date: 31 December 2024*

Under certain state-, sector-, activity- specific data breach notification laws, certain entities can functionally be considered "data processors," such as "business associates" under HIPAA, and "service providers" or "data maintainers" under state breach notice laws. Additionally, contractual terms between the "data processor" and "controller" may require the processor to notify others, including affected individuals and regulators.

☒   controller/owner

Typically, these entities will have duties to notify the controllers/owners of the data. For example, at the federal level, the HIPAA Breach Notification Rule requires business associates to notify the relevant covered entity of a discovered data breach. Similar requirements apply under other federal and state data breach notification laws.

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 31 December 2024*

Yes.

☒   public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)

☒   cybersecurity authorities (e.g., to notify CISA as described above)

☒   health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)

☒   financial services requirements (e.g., to notify financial regulatory authorities as per GLBA and other requirements)

☒   telecommunication requirements

☒   providers of critical infrastructure

☒   other

Organizations need to assess additional sector-specific or non-personal data security breach notification requirements on a case by case basis, including specific contractual obligations.

**If so, please provide brief details of the relevant law / guidance and indicate which body/bodies must be notified of the breach.**

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 31 December 2024*

Yes. Laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of personal data outside of the local jurisdiction:

☒   national security laws

☒   anti-investigatory/blocking statutes that restrict any activity on local territory that aids a foreign government investigation

☒   tax or financial record laws

☒   employment laws

☒   export control laws

☒   other

Sector-specific and state regulations may impose obligations to retain data in the US.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 31 December 2024*

☒  Obligation for public sector organizations to share or make accessible non-personal data

☒  Obligation for private organizations to share or make accessible non-personal health data

☒  Obligation for private organizations to share or make accessible non-personal financial data

☒  Obligation for private organizations to share or make accessible other non-personal data

***If so, please provide brief details of the relevant law or regulation.***

The Consumer Financial Protection Bureau's (CFPB) [open banking rules](https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/) enhance consumer rights over personal financial data, requiring financial institutions to provide consumer data to authorized third parties in a secure and reliable manner upon the consumer's request and at no cost. Covered data includes "information about transactions, costs, charges, and usage." Compliance will be in phases, with larger institutions needing to comply by 1 April 2026. Smaller covered institutions will have until 1 April 2030 to comply. Certain small banks and credit unions are exempt from these requirements.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 31 December 2024*

☒  Obligation to share data on request

☒  Obligation to share data proactively

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.