ABC STRATEGIC PRIVACY COMPLIANCE GUIDE IN THE UNITED STATES

OLARTEMOURE
OLARTE MOURE & ASOCIADOS
Abogados - Attorneys

Contact us: info@olartemoure.com

Introduction

The regulation of personal data protection in the United States is characterized by a sectoral approach, as there is no comprehensive federal law covering all scenarios of personal data processing, unlike the European Union's General Data Protection Regulation (GDPR), Colombia's Law 1581 of 2012, and other national regulations in various jurisdictions. At the federal level, only sector-specific or data-type-specific statutes apply (for example, the Health Insurance Portability and Accountability Act – HIPAA, the Gramm-Leach-Bliley Act – GLBA, the Children's Online Privacy Protection Act – COPPA, and the Fair Credit Reporting Act – FCRA, among others).

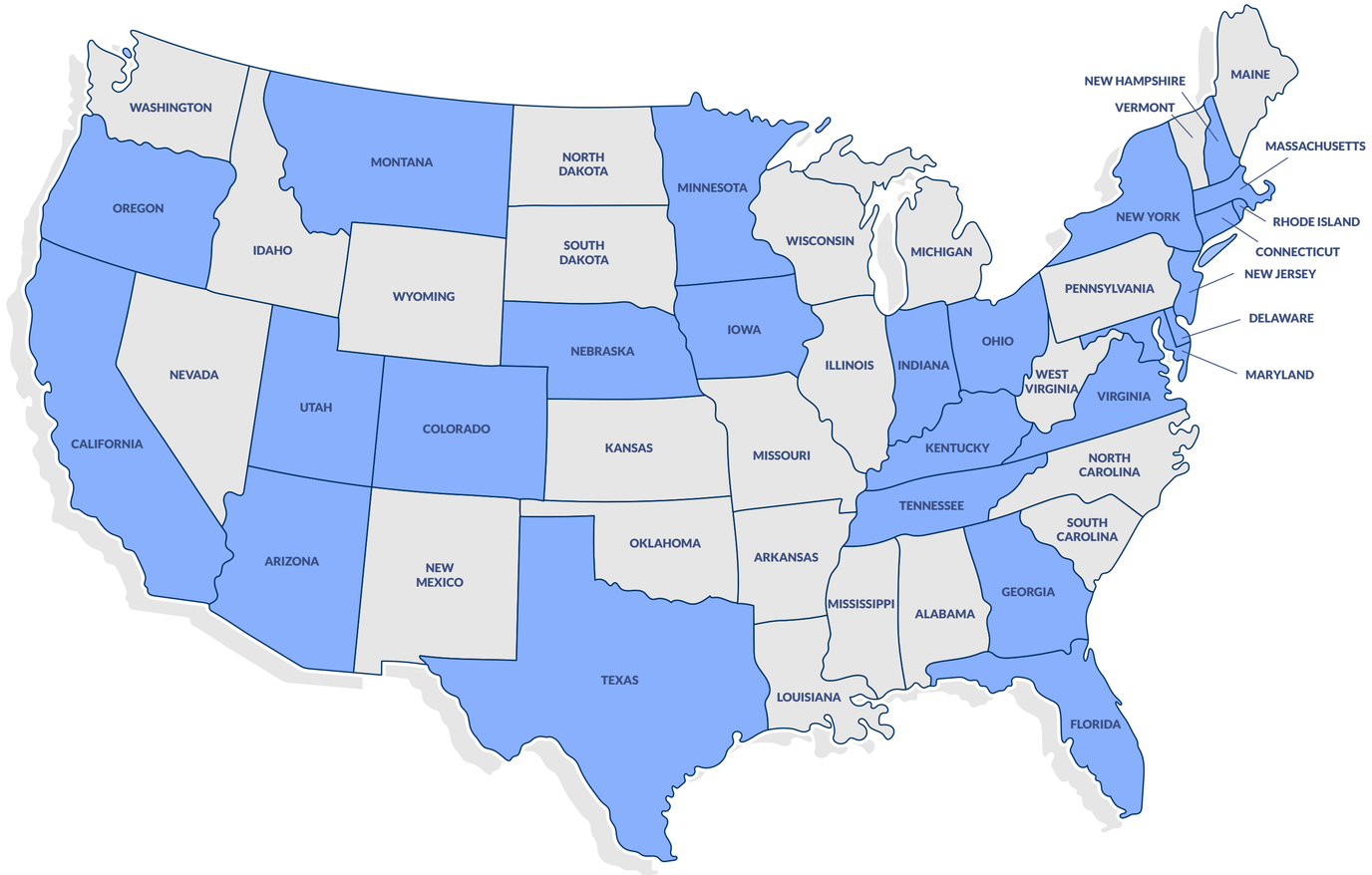
Since 2018, several states have enacted their own comprehensive privacy laws. California, as a pioneer in this field, enacted the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). In subsequent years, many other states followed suit. Currently, around 25 states have enacted broad data protection laws that are either in force or will become effective by 2026. It should be noted, however, that a significant number of these regulations are primarily consumer-oriented.

In addition to general state laws, some states have enacted specific regulations for certain sectors or types of data processing. For example, Illinois has enforced since 2008 the Biometric Information Privacy Act (BIPA), one of the most stringent biometric data protection laws in the U.S. Other states, such as Nevada and Delaware, require businesses to provide individuals with the possibility to opt-out of the sale of their personal data. This model assumes that data can be sold by default unless the consumer objects, standing in contrast to the opt-in model, under which data sales or transfers may occur only when the consumer has granted prior, informed, and explicit consent.

Unlike the United States, most countries have adopted comprehensive general data protection laws. Currently, more than 160 jurisdictions worldwide have enacted such legislation, including virtually all developed economies. In the European Union, the GDPR has applied since 2018 and is widely considered the international benchmark.

In Latin America, nearly all countries have enacted national laws over the past decade, including Colombia, Mexico, Brazil, Argentina, Chile, Ecuador, and Uruguay.

Data protection in the USA



They have personal data protection laws or similar regulations.

They do NOT have personal data protection laws or similar regulations.

Arizona	Data Breach Notification Law	Montana	Montana Consumer Data Privacy Act
California	California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)	Ohio	Ohio Data Protection Law
		Oregon	Oregon Consumer Privacy Act
Virginia	Virginia Consumer Data Protection Act (VCDPA)	Delaware	Delaware Personal Data Privacy Act
Colorado	Colorado Privacy Act (CPA)	New Hampshire	New Hampshire Privacy Act
Connecticut	Connecticut Data Privacy Act	New York	New York Privacy and Data Security Act
Utah	Utah Consumer Privacy Act (UCPA)	New Jersey	New Jersey Privacy Act (2022/23)
Iowa	Iowa Consumer Data Protection Act	Kentucky	Kentucky Privacy Act (2024)
Indiana	Indiana Consumer Privacy Act	Nebraska	Nebraska Privacy Act (2023)
Tennessee	Tennessee Information Protection Act	Rhode Island	Rhode Island Transparency and Privacy Act
Texas	Texas Data Privacy and Security Act (TDPSA)	Massachusetts	Massachusetts Information Privacy Act
Florida	Florida Digital Bill of Rights (FDBR)	Maryland	Maryland Online Data Privacy Act (MODPA)
Georgia	Georgia Personal Identity Protection Act	Minnesota	Minnesota Consumer Data Privacy Act

(Note: Several of these laws have only recently taken effect or will do so between 2025 and 2026, and their practical application is still developing.)

In general terms, these laws apply to companies that process personal data of state residents, provided that they exceed certain thresholds of data volume or revenue, and they often exclude small businesses. Importantly, these statutes do have an extraterritorial effect, as their applicability does not depend on whether the business is physically established in the state but rather on whether it processes the data of residents.

These laws grant individuals rights such as:

- access, correction, deletion, and copies of their data;
- the right to opt-out of the sale of personal data or targeted advertising; and
- restrictions on the processing of sensitive data.

At the same time, they impose obligations on companies in terms of transparency, security, and accountability, including: providing clear privacy notices, establishing limits on data use, protecting sensitive information, executing data protection contracts with service providers, conducting risk assessments in certain cases, and timely responding to consumer rights requests.

In states lacking a comprehensive privacy law, only the minimum federal framework and sector-specific state provisions apply, such as:

- data breach notification laws,
- health or education data regulations,
- restrictions on the use of Social Security numbers, and
- secure data disposal requirements.

Key Obligations of a Data Controller in the U.S.

Within the U.S. regulatory landscape, a Data Controller must adopt internal policies and procedures to ensure compliance with applicable laws. The principal obligations include:

1. PRIVACY POLICY:
Every business must publish a clear and updated privacy policy explaining how it collects, uses, shares, and protects personal data.

2. PRIVACY NOTICES:
Many laws require notices at the point of data collection (e.g., under CCPA/CPRA in California). For biometric data, Illinois' BIPA requires written consent and a notice specifying purpose and retention. COPPA mandates parental consent for children under 13, while California prohibits the sale of data of minors under 16 without express consent.

3. INFORMATION SECURITY MEASURES:
Businesses must implement "reasonable security measures" tailored to their size and the nature of the data, ensuring confidentiality, integrity, and availability.

4. INCIDENT AND BREACH MANAGEMENT:
All states require breach notification to affected individuals, and in some cases, to authorities. Controllers must establish incident response plans and comply with strict deadlines (typically 30–60 days).

5. CONTRACTS WITH PROCESSORS:
Data shared with processors must be governed by contracts that limit use, require security measures, ensure deletion or return of data, and provide for audits or incident cooperation.

6. PRIVACY IMPACT ASSESSMENTS (PIAS/DPIAS
Emerging state laws require assessments for high-risk processing, documenting purposes, risks, and safeguards.

7. ARTIFICIAL INTELLIGENCE POLICIES:
Newer state laws, particularly in California, impose transparency obligations regarding automated decision-making technologies (ADMT). Businesses are expected to adopt AI policies that describe their use and governance.

Is a DPO Required in the United States?

Unlike the GDPR, which mandates the designation of a Data Protection Officer (DPO) in certain cases, the U.S. does not impose a uniform DPO requirement. State privacy laws generally do not reference this role.

However, several state laws do require the designation of a responsible privacy officer. For instance, the new Minnesota law obliges businesses to appoint a Chief Privacy Officer (CPO).

Thus, while the U.S. legal framework does not mirror the European DPO model, there is a clear trend toward requiring organizations to assign an internal privacy lead. For best practice, businesses should appoint a privacy officer (CPO, DPO, or similar role) to oversee compliance, liaise with regulators, and prepare for future regulatory developments.

OLARTEMOURE

OLARTE MOURE & ASOCIADOS

Abogados - Attorneys

Contact us for more information.

info@olartemoure.com