Lowenstein Sandler

Privacy & Cybersecurity

July 31, 2023

State Data Protection Laws: What You Need To Know As States Ramp Up Enforcement

By Mary J. Hildebrand CIPP/US/E and Judith G. Rubin CIPP/US/E, CIPT

Key Takeaways:

- **States are adopting data protection laws at an accelerated rate, and this trend is expected to continue for the foreseeable future.**
- **New York and other states with significant clout, economic and otherwise, are actively debating comprehensive data protection laws that are likely to have an outsize impact on businesses similar in scope to California's CCPA and the new Texas law, which lacks any numerical criteria for its application.**
- **Compliance with even the "most strict" state data protection law is not equivalent to compliance with all state, national and regional laws that apply to your business *because they are all materially different*.**
- **Organizations with proactive leadership will come out ahead with consumers and regulatory authorities alike by realistically assessing these laws now and creating compliance road maps that reflect their business priorities and leverage any existing data protection frameworks.**

Congress has repeatedly failed to pass comprehensive national data protection legislation, and the states are rapidly filling the void with laws that impose different requirements on a state-by-state basis.

Most of these laws are sector-neutral, so all U.S. companies and foreign companies that operate in the U.S. need to know that by January 1, 2026, at least 13 states will have comprehensive laws on the books to protect the personal data of their residents ("consumers"), with more to come.

State data protection laws are different not only from one another but from the EU General Data Protection Regulation ("GDPR"), Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), and other national and regional laws, so compliance with one–even the "most strict"–is not equivalent to compliance with all applicable laws. Organizations that seek to retain a competitive edge and avoid regulatory and legal entanglements would be well advised to accelerate–or begin–compliance initiatives now.

Which states have enacted data protection laws, and when are they effective?

Since July 1, 2023, data protection laws have become effective in California, Virginia, Colorado, and Connecticut, with Utah to follow on December 31, 2023. An additional eight states will join the list by January 1, 2026: Texas, Florida, Montana, Oregon, Iowa, Tennessee, Indiana, and Delaware. While the Delaware law is waiting on the governor's signature, no delays are expected. As of today, comprehensive data protection laws are pending in about 15 additional states.

Who enforces these laws?

Except in California, violations of state data protection laws are primarily investigated and enforced by the state attorneys general. Under data

protection laws that are or will become effective in 2023, penalties for noncompliance range from $2,000 to $7,500 *per violation*, with enhanced penalties for intentional activities (e.g., a business continues to violate the law after consumer complaints or previous enforcement actions). In our digital economy, where processing the personal data of thousands or millions of consumers is routine, the fines could quickly add up to hundreds of thousands or even millions of dollars.

California created the first-of-its-kind California Privacy Protection Agency (CPPA) with a wide array of responsibilities under the California Consumer Privacy Act of 2018, as amended by the Consumer Privacy Rights Act of 2020 (collectively, CCPA), including rulemaking and administrative enforcement authority. The CPPA commissioners have indicated that they expect to vigorously monitor compliance and enforce the law. In addition, California consumers have the right to pursue private causes of action against regulated entities when their personal data is subject to a data breach because a business failed to implement and maintain reasonable security procedures and practices. Consumers are entitled to recover either actual damages or statutory damages of $100 to $750 per incident, whichever is greater, which means that consumers do not have to prove actual damages to prevail in court.

To whom do state data protection laws apply?

Entities are often shocked to learn their operations are regulated because state data protection laws define common terms in unexpected ways (e.g., disclosing, renting, sharing, releasing, making available, or transferring personal data may constitute a "sale"). These laws frequently apply to entities that have no locations, facilities, or employees in the state but otherwise meet the relevant criteria. Moreover, depending on the jurisdiction, state data protection laws may regulate nonprofits, joint ventures, or affiliates and subsidiaries of regulated entities.

State data protection laws typically apply to entities that conduct business in the state or target products/services to state residents (referred to as "consumers"), *and* satisfy one or a combination of these factors:

- Generate a specified minimum annual revenue
- Annually process personal data associated with a minimum number of state residents
- Derive a specified percentage (or more) of annual revenue from the sale or sharing of residents' personal data, as those terms are defined under the respective state law

One notable exception is the Texas Data Privacy and Security Act, which applies to any entity that conducts business in Texas or produces a product or service consumed in Texas, processes the personal data of Texas residents, and is not a small business as defined by the U.S. Small Business Administration (SBA). There are no data processing volume thresholds or numerical criteria of any kind except as applied by the SBA, and *the law's prohibition against selling sensitive personal data without consent applies to all businesses that operate in Texas, regardless of size*. Although the Texas law does not extend to the personal data of business contacts or employees, it appears that most companies that do any business in the state will be required to comply.

State data protection laws may exclude data and/or entities that are regulated by sector-specific laws. The CCPA, for example, exempts nonpublic personal information regulated by the Gramm-Leach-Bliley Act (GLBA) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA); however, *the regulated entities are still required to comply with the CCPA when processing other consumer personal information* (e.g., personal information related to employees or website visitors that reside in California). The Virginia Consumer Data Protection Act ("VCDPA") exempts data regulated by the GLBA and HIPAA, *and the entities that process such data*.

What types of data do state data protection laws protect?

State data protection laws safeguard the personal information of residents in their respective states. While laws vary, personal information is usually broadly defined to include categories such as identifiers (e.g., name, residence, email address, phone, driver's license number), biometric information, internet or other electronic network activity information, geolocation data, and audio, electronic, or visual information, among others. Collection and processing of "sensitive personal information," such as an individual's Social Security number, account login, or genetic information, requires additional safeguards (e.g., the VCDPA requires an informed, affirmative act indicating consent from consumers prior to collecting sensitive personal information). The CCPA extends protection to the personal information of households, business contacts, employees, contractors, and job applicants of regulated entities that reside in state, and personal information collected offline, such as in brick-and-mortar locations.

What do state data protection laws generally require?

While state data protection laws are not uniform in terms of the entities regulated, compliance requirements, enforcement strategies, or penalties, common themes emerge:

- Transparency regarding the collection of personal information and the purpose of processing
- Enhanced protections for sensitive personal information (e.g., opt-in consent required prior to collection; right to limit or opt out of processing altogether)
- Privacy notices that communicate clearly and concisely regarding data processing practices and activities
- Cybersecurity measures to secure personal information
- Consumers' right to control their own personal information (e.g., delete, correct, transfer), with easily accessible methods to exercise such rights
- Prohibition of discrimination or retaliation against consumers for exercising data privacy rights
- Opt-out rights that allow consumers to terminate processing of their personal information for specific purposes, such as targeted advertising, sale or sharing, or limit the processing sensitive personal information
- Contractual requirements for service providers and contractors that process personal information on behalf of regulated entities
- Direct liability of service providers/contractors for compliance with state data protection laws
- Accountability for compliance with applicable data protection laws by the regulated entity, including upstream (notifying data providers of restrictions on processing or the exercise of consumer rights) and downstream (notifying recipients of personal information of the same)

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com