State Privacy Laws That May Impact Your Business

State privacy laws in the U.S. generally apply to businesses if they interact with residents of that state, regardless of where the business is located.

A brief overview

Applicability: Many state privacy laws apply to businesses outside the state if they collect personal information from residents of that state. This means that a business must comply with the privacy law of the state where it does business, or where its customers reside, even if it is based in another state or country.

Threshold Criteria: State consumer privacy laws include specific thresholds, such as minimum revenue amounts, data processing volume, and/or number of state residents affected.

Compliance Requirements: Businesses need to adapt their handling of personal information practices to comply with the privacy laws of the states in which they operate. Most state consumer privacy laws afford rights to consumers to access their data, to correct data, and to data portability and deletion, as well as rights to limit processing and to opt out of the sale of their data, profiling, and targeted advertising. This might involve updating policies and implementing procedures for responding to consumers exercising these new rights.

Enforcement: States can enforce their privacy laws through state agencies or through consumer complaints. Only California allows for a consumer to bring a private right of action under its consumer privacy law. However, there are many other privacy related claims that individuals can make against businesses. Failing to comply with state privacy laws could lead to legal action or regulatory penalties.

Important Definitions: When it comes to privacy laws, terminology can be confusing, as there are many overlapping terms and words that have specific meaning in the field. There are a few

fundamental terms that are defined here. However, these are for conceptual purposes and general understanding. They should not be considered a statutory definition applicable to a particular legal concern.

- **Personal Information** – Any information that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
- **Sensitive Personal Information** – This definition can vary from state to state but generally involves a consumer's government-issued identifier, such as a social security number, passport number, state identification card, or driver's license number.
- **Data Controller** – A person or business that decides how and why personal information is processed. They are responsible for the lawfulness of the processing, the protection of the data, and complying with the rights of the consumer under the statute.
- **Data Processor** – A person or business who processes personal information on behalf of the Data Controller.
- **Sale of Personal Data** – The exchange of a consumer's personal data by the controller to a third party for monetary or other valuable consideration or otherwise for a commercial purpose.
- **Targeted Advertising** – The targeting of an advertisement to a consumer based on the consumer's activity with one or more businesses, distinctly branded websites, applications, or services, with which the consumer has interacted.

U.S. Privacy Hub

View our U.S. Consumer Privacy Map