



May 06, 2026

**Categories:**

[Publications](#)

**Authors:**

[Caleb S. Long](#)

[Ravipal Singh](#)

[John T. Wolak](#)

# Oklahoma's Data Privacy Act: What You Need to Know

---

By enacting [Senate Bill \(SB\) 546](#), Oklahoma has become the 20th state to adopt comprehensive consumer privacy legislation. This new law continues the trend among states toward heightened transparency, consumer choice, and accountability required of businesses that collect, process, use, and store the personal data of resident consumers. SB 546 goes into effect **January 1, 2027**.

## Who Is Impacted

Oklahoma's data privacy law applies to any individual or entity who conducts business in Oklahoma or produces a product or service targeted to Oklahoma residents and that, during a calendar year, either:

- Controls or processes personal data of at least 100,000 consumers; or
- Controls or processes personal data of at least 25,000 consumers and derives more than 50% of gross revenue from the sale of personal data.

SB 546 distinguishes between "controllers" (i.e., person or entity who determine the purposes and means of processing personal data) and "processors" (i.e., person or entity who process personal data on behalf of a controller), while imposing obligations on each based on their role.

## A Few Key Exceptions

Like many other state omnibus privacy laws, SB 546 contains both entity-level exemptions and data-level exemptions.

## Entity-Level Exemptions

Oklahoma's privacy law does not apply to the following entities or persons:

- An Oklahoma state agency or a political subdivision of Oklahoma, or service providers processing personal data on behalf of such entities;
- Financial institutions or data subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);
- Covered entities and business associates governed by the Health Insurance Portability and Accountability Act of 1996 and related regulations;
- Nonprofit organizations;
- Institutions of higher education; and
- Individuals processing personal data in the course of a purely personal or household activity.

## Data Level Exemptions

Even where an entity is otherwise subject to Oklahoma's privacy law, certain categories of data are expressly excluded. Notable exclusions include:

- Protected health information, health records, and certain other specifically regulated health data;
- Personal data regulated by the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Driver's Privacy Protection Act;
- Personal data processed in compliance with the Controlled Substances Act provision governing the regulation of listed chemicals (21 U.S.C. § 830).
- Personal data processed or maintained in the context of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent such data is collected and used within that role; and
- Emergency contact information and benefits administration data related to individuals described above, when used solely for those purposes.

## What to Know if You Are Covered by the Act

## Consumer Rights

Like other state omnibus privacy statutes, Oklahoma's SB 546 grants consumers the following rights:

- Right to Confirm whether a controller is processing their personal data and access that data;
- Right to Correct inaccuracies in personal data;
- Right to Delete personal data provided by or obtained about the consumer;
- Right to Obtain a portable copy of personal data previously provided to the controller; and
- Right to Opt out of:
  - Targeted advertising,
  - The sale of personal data, and
  - Certain automated profiling that produces legal or similarly significant effects concerning the consumer.

Under SB 546, controllers typically must provide two or more secure and reliable ways for consumers to submit a rights request, and they are required to provide the requested information free of charge and up to two times annually. Controllers generally must respond to a consumer request within 45 days, with a one-time extension of 45 days permitted when reasonably necessary. Controllers must also provide an internal appeal process for instances when the controller declines to take action on a consumer's rights request.

Unlike several other state privacy statutes, SB 546 does not include a requirement to implement a universal opt-out mechanism (often browser-based) that automatically signals a consumer's choice to opt out of the processing, sale, or sharing of personal data for targeted advertising.

## Data Minimization and Purpose Limitation

Controllers are required to limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the

purposes disclosed to the consumer. Processing personal data for purposes that are incompatible with those disclosures generally requires consumer consent.

## Sensitive Data and Consent

Oklahoma's data privacy law imposes heightened obligations for the processing of sensitive data, including precise geolocation data, biometric data used for identification, genetic data, and personal data collected from known children (individuals under the age of 13). As a general rule, controllers must obtain affirmative consent before processing sensitive data.

## Data Security

Controllers must implement and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue, while processors are required to assist controllers with security and breach notification compliance.

## Privacy Notices

Controllers must provide consumers with a reasonably accessible and clear privacy notice describing, among other things:

- Categories of personal data processed;
- Purposes of processing;
- Methods for exercising consumer rights and appealing decisions;
- Categories of data shared with third parties; and
- Categories of third parties that may receive shared data.

## Controller/Processor Contracting Requirements

A contract is required between a controller and a processor with various required terms, including:

- Clear processing instructions;

- The nature, purpose and duration of processing;
- The specific data subject to processing; and
- Any subcontracting must be pursuant to a written contract that extends the same processing requirements to the subcontractor.

## Data Protection Assessments

Controllers are required to conduct and document data protection assessments for certain higher risk processing activities, including:

- Targeted advertising;
- Sale of personal data;
- Certain profiling activities;
- Processing of sensitive data; and
- Processing that presents a heightened risk of harm to consumers.

These assessments must be made available to the Oklahoma Attorney General's Office upon written request but are otherwise confidential and exempt from public-records disclosure.

## Enforcement

### Attorney General Authority

SB 546 expressly provides that there is no private right of action; instead, the Oklahoma Attorney General's Office has exclusive enforcement authority for violations of SB 546.

### Cure Period and Penalties

Before initiating an enforcement action, the Attorney General's Office must provide a 30-day notice and cure period, during which the business alleged to be in violation of SB 546 may cure its violative activity and provide written proof of such cure. If a violation is not cured — or if a written assurance of compliance is breached — the Attorney General's Office may seek:

- Civil penalties of up to **\$7,500 per violation**;
- Injunctive relief; and
- Recovery of reasonable attorney fees and investigative costs.

## What to Do Now

Although Oklahoma's privacy law does not take effect until January 1, 2027, businesses that may be subject to its requirements should begin preparing by:

- Assessing whether they meet the Act's applicability thresholds;
- Mapping personal data collection and processing activities;
- Reviewing and updating privacy notices and consent mechanisms;
- Evaluating vendor and processor agreements; and
- Developing procedures for consumer rights requests and data protection assessments.

Early planning will help reduce compliance risk and position organizations to respond efficiently once enforcement begins. For more information or assistance, please contact the authors or any attorney with FBT Gibbons' [Data Security and Privacy](#) team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.