Insights, News & Events

OKLAHOMA'S NEW CONSUMER PRIVACY LAW AND DATA BREACH UPDATES: WHAT BUSINESSES NEED TO KNOW

Insights
Apr 2, 2026

Oklahoma's New Consumer Privacy Law and Data Breach Updates: What Businesses Need to Know

Oklahoma will soon join 19 other states and add to the patchwork of consumer privacy laws that multistate employers have to navigate beginning January 1, 2027. Governor Kevin Stitt signed the Oklahoma Consumer Data Privacy Act (OCDPA) into law on March 20, a system that generally follows the model of other consumer privacy laws across the country. This Insight will point out key takeaways for businesses, and also cover the Oklahoma data breach updates that went into effect in January.

Scope and Applicability

The law applies to a controller or processor that conducts business in Oklahoma or produces a product or service targeted at Oklahoma and during a calendar year either:

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

These thresholds align with most other consumer privacy laws that have been enacted. Importantly, Oklahoma's law

Related People

Kate Dedenbach, CIPP/US
Of Counsel

248.901.0301

Jillian Seifrit, CIPP/US
Associate

610.230.6129

does not apply in the employer-employee or business-to-business context.

Consumer Rights

The law provides Oklahoma residents with the following rights which align with the standard rights across consumer privacy laws:

- Right to confirm whether the controller is processing consumer's personal data and access such data
- Right to correct
- Right to delete
- Right to access and obtain copies of personal data in a portable format
- Right opt out of the processing of data for targeting advertising, sale, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer
- Right to appeal

Exemptions

Like most other consumer privacy laws, there are certain entities that the law does not apply to.

- State agencies or political subdivisions of Oklahoma
- Financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA)
- A covered entity or business associate governed by HIPAA
- Nonprofit organizations
- Institutions of higher education meaning public institutions that are a member of The Oklahoma State System of Higher Education or a technology center school district or a private institution of higher education
- Processing of personal data by a person in the course of a purely personal or household activity

Service Focus

Consumer Privacy Team

Data Protection and Cybersecurity

Privacy and Cyber

- Personal data collected and used for purposes of the Controlled Substances Act

Additional Business Obligations

The law also creates some fairly standard obligations for covered entities in the state. If covered, businesses must:

- Limit the collection of personal data
- Establish, implement, and maintain reasonable administrative, technical, and physical security practices
- Obtain consumer consent before processing any "sensitive data" (which includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, genetic or biometric data that is processed for the purpose of uniquely identifying an individual, personal data collected from a known child, or precise geolocation data)
- Provide consumers with a clear privacy notice
- Conduct a data protection assessment for the following activities:
  - Processing of personal data for targeted advertising
  - Sale of personal data
  - Processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact on a consumer, financial, physical, or reputational injury to a consumer, a physical or other intrusion on solitude or seclusion of the private affairs or concerns of a consumer if the intrusion would be offensive to a reasonable person or other substantial injury to a consumer
  - Processing sensitive data
  - Processing activities that present a heighted risk of harm to consumers

Enforcement

There is no private right of action for the new law, but the Attorney General can bring an action against entities in

violation. The AG must notify the business and provide a 30-day cure period before they can bring an action. If the business does not cure the violation, the AG can levy a fine of up to $7,500 per violation.

Data Breach Law Updates

As of January of this year, Oklahoma now requires businesses to provide notice to the Oklahoma Attorney General when 500+ Oklahoma residents are impacted by a breach. The regulatory notice is due within 60 days of providing individual notice. The individual notice timing is unchanged (without unreasonable delay).

Also, the definition of "personal information" now includes biometric data and unique electronic identifiers or routing codes in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Another new addition to the data breach law is that an entity that uses "reasonable safeguards" and provides notice in accordance with the statute are not subject to civil penalties. They may also use such compliance as an affirmative defense in a civil action filed under the law. However, an entity that fails to use reasonable safeguards but provides notice is still subject to actual damages and a civil penalty of $75,000.

"Reasonable safeguards" means policies and practices that ensure personal information is secure. These safeguards can include, but are not limited to, conducting risk assessments, implementing technical and physical layered defenses, employee training on handling personal information, and establishing an incident response plan.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber team or our Data Protection and Cybersecurity team.