



OKLAHOMA CONSUMER DATA PRIVACY ACT (OCDPA)

CHECKLIST



 **USERCENTRICS**

Oklahoma Consumer Data Privacy Act (OCDPA), gives Oklahoma residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	January 1, 2027
Retroactive	No

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

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

Oklahoma does not impose a standalone annual revenue threshold.

Entity-level exemptions:

- State agencies and political subdivisions
- Nonprofit organizations
- Higher education institutions
- [GLBA](#)-regulated financial institutions
- [HIPAA](#)-covered entities and business associates
- Individuals processing personal data solely in a personal or household context

Data-level exemptions:

- Protected health information under HIPAA
- Employee and job applicant data
- Emergency contact information
- FERPA-regulated student data
- [FCRA](#)-regulated data
- GLBA-regulated financial data

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers about:

- Categories of personal data processed, including sensitive data
- Purposes for processing
- Categories of third parties data is shared with, if any
- Whether the business sells personal data or uses it for targeted advertising

Rights: Explain how consumers can exercise their rights, including how to appeal a denied request.

Language: Keep the [privacy policy](#) reasonably accessible and clear.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a [Privacy Policy Generator](#) and a [CMP to manage opt-outs](#).

3 Inform Consumers About Their Rights

Consumers' rights under the OCDPA:

- **Right to access:** Confirm whether personal data is processed and access it
- **Right to correct:** Fix inaccuracies in personal data collected
- **Right to delete:** Request deletion of personal data provided by or obtained about them
- **Right to portability:** Obtain a copy of their data in a portable, readily usable format where processing is automated
- **Right to opt out:** Of targeted advertising, the sale of personal data, and profiling used in decisions with legal or similarly significant effects
- **Right to non-discrimination:** For exercising these rights

The OCDPA does not include a right to revoke consent, a right to limit use of sensitive data beyond the consent requirement itself, or authorized-agent provisions.

4 As a Best Practice, Review and Update Your Privacy Notice Periodically

Review operations and any changes in the law regularly, and keep the notice's effective date current and visible.

5 Obtain Affirmative Consent for Sensitive Personal Data

[Sensitive data](#) under the OCDPA includes:

- Racial or ethnic origin
- Religious beliefs
- Mental or physical health condition or diagnosis
- Sexual orientation
- Citizenship or immigration status
- Genetic or biometric data processed to identify an individual
- Personal data from a known child under 13
- Precise geolocation (within a 1,750-foot radius)

Passive signals do not count as valid consent. This includes accepting broad terms, hovering, or closing content.

6 Handle Children's Data in Line With COPPA

Personal data from a known child under 13 must be processed in accordance with [COPPA](#). The OCDPA does not extend additional protections to 13- to 16-year-olds beyond this.

7 Audit Consent Interfaces for Dark Patterns

The OCDPA explicitly prohibits [dark patterns](#). This includes interfaces designed to subvert or impair a consumer's autonomy or choice, and any practice the FTC designates as such. Review consent banners and opt-out flows accordingly.

8 Enable Consumers to Make Data Subject Access Requests (DSARs)

Provide at least two secure contact methods to submit a [DSAR](#). Consumers cannot be required to create a new account solely to submit a request.

9 Respond to and Verify DSARs

Standard time period: within 45 days. Extended time period: up to 90 days total, with notice to the consumer within the initial 45-day window. Responses must be free of charge, up to twice per year per consumer.

10 Establish an Appeal Process

Provide a way for consumers to appeal a denied request, with a written explanation within 60 days. If the appeal is denied, direct the consumer to the Oklahoma Attorney General's online complaint mechanism.

11 Maintain Written Processor Contracts

Govern all processor relationships (e.g., analytics or advertising vendors) with a written agreement covering processing instructions, data types, duration, and each party's obligations. This should include equivalent terms for any subprocessors.

12 Conduct Data Protection Assessments

Required for high-risk activities: targeted advertising, data sales, profiling with legal or significant effects, and sensitive data processing. These apply only to processing activities beginning on or after January 1, 2027, and are not retroactive.

**Falling thresholds, rising enforcement and litigation,
eroding ad revenue. Do you know your risk?**

GET IN TOUCH