



MONTANA CONSUMER DATA PRIVACY ACT (MTCDDPA)

CHECKLIST



 **USERCENTRICS**

Montana Consumer Data Privacy Act (MTCDDPA) gives Montana 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.



i Important to know:

Action	Date
Effective date	January 1, 2025
SB 297 amendment	Effective October 1, 2025, lowered applicability thresholds, added minors' protections, and eliminated the right to cure
Retroactive	No

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Conducts business in Montana or targets products or services to Montana residents, and
- Controls or processes the personal data of at least 25,000 Montana consumers annually, excluding data processed solely to complete a payment transaction, or
- Controls or processes the personal data of at least 15,000 Montana consumers, and derives more than 25 percent of gross revenue from the sale of personal data

Minors' privacy provisions apply to any entity conducting business in Montana, regardless of these thresholds.

Entity-level exemptions:

- State government entities, boards, commissions, and political subdivisions
- National securities associations
- [HIPAA](#)-covered entities and business associates

- Banks, credit unions, insurers, and insurance producers (replacing the broader GLBA “financial institution” exemption SB 297 removed)
- Nonprofit organizations established to detect and prevent insurance-related fraud (narrowed by SB 297 from a general nonprofit exemption)
- Institutions of higher education

Data-level exemptions:

- HIPAA
- Health Information Technology for Economic and Clinical Health Act
- Patient Safety and Quality Improvement Act
- [FCRA](#)
- [COPPA](#)
- FERPA
- Driver’s Privacy Protection Act
- Farm Credit Act
- Airline Deregulation Act
- [GLBA](#) (data-level exemption retained even though the entity-level one was removed)
- HR/employment data, health records, human-subjects research data

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection about:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any

Rights: Inform website visitors of their privacy rights and how to exercise them, including how a consumer may appeal a controller’s decision.

Language: Keep the privacy policy clear and easy to understand, and available in the language the controller uses to provide the product or service.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a banner or popup when visitors visit your site, [powered by a CMP](#).

3 Inform Consumers About Their Rights

Consumers’ rights under the MTCDDPA:

- **Right to access:** Request and receive a copy of their personal data (certain highly sensitive categories, such as Social Security numbers, are excluded from what must be disclosed)
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected

- **Right to deletion:** Personal data that has been collected about them (with exceptions)
- **Right to data portability:** Copy of personal data must be provided in a portable and readily useable format
- **Right to opt out:** Of processing of personal data for the purposes of sale, targeted advertising, or profiling in furtherance of automated decisions that produce legal or similarly significant effects
- **Right to nondiscrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent or guardian before children's (under age 13) personal data is collected
- **Right to restrict sensitive personal information:** Limit or refuse the collection or use of personal data the law classifies as sensitive

4 As a Best Practice, Review and Update Your Privacy Policy Every 12 Months

Review your operations and any changes in the law every 12 months. Update the [privacy policy](#) and its effective date, even if no other changes are made. For example, use a [Privacy Policy Generator](#).

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible.

Data sold: List all categories of personal information your business has sold in the past 12 months.

5 Enable Clear Options When Consent Is Required

When: If the personal data collected is sensitive, or that of a child.

Availability: Easily accessible on your website.

Method: Via a CMP.

6 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Consent is required for processing [sensitive personal data](#).

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger.

7 Apply Heightened Minors' Protections

Since October 1, 2025, controllers owe a duty of care to consumers under 18 and must design products and services accordingly. This applies regardless of whether the applicability thresholds in Step 1 are met.

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

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission of [DSARs](#).

Note: Opt-out requests do not require identity verification, though a request may be denied on a good-faith, reasonable, and documented belief that it is fraudulent.

9 Set Up a System to Verify Data Subject Access Requests (DSARs)

As a best practice, enable consumers to attach documentation to help verify their identity and residency. If your business cannot reasonably verify a consumer's identity, inform them and explain why, and enable them to rectify.

10 Keep Track of Data Subject Access Requests (DSARs)

Set up a system to track all requests. Keep records of requests and responses for two years after the last consumer interaction.

11 Fulfill Data Subject Access Requests (DSARs)

Respond within 45 days from the date the request is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window.

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

GET IN TOUCH