



DELAWARE PERSONAL DATA PRIVACY ACT (DPDPA)

CHECKLIST



 **USERCENTRICS**

Delaware Personal Data Privacy Act (DPDPA) gives Delaware 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
Original effective date	January 1, 2025
Retroactive	No
Pending amendment (HB 380)	Passed the legislature June 16, 2026; not yet signed into law as of this review

HB 380 would, if signed, lower the applicability thresholds, expand the sensitive-data definition, and add new third-party contracting requirements, effective January 1, 2027. Industry groups have formally urged a veto.

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Controls or processes personal data of at least 35,000 Delaware residents, excluding data controlled or processed solely to complete a payment transaction, or
- Controls or processes personal data of at least 10,000 Delaware residents, and derives more than 20 percent of gross revenue from the sale of personal data

Entity-level exemptions:

- State governmental entities, including regulatory, administrative, legislative, or judicial bodies
- [GLBA](#)-regulated financial institutions and their affiliates
- Nonprofit organizations dedicated exclusively to preventing and addressing insurance crime
- Nonprofits providing services to victims or witnesses of child abuse, domestic violence, human trafficking, sexual assault, a violent felony, or stalking, specifically for the data collected in that service context

Data/regulatory-level exemptions:

- [HIPAA](#)
- GLBA
- [FCRA](#)
- Driver's Privacy Protection Act
- FERPA
- Farm Credit Act
- Airline Deregulation Act

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.

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 Honor Opt-Out Preference Signals

Since January 1, 2026, controllers must recognize a consumer's opt-out preference signal (e.g., [Global Privacy Control \(GPC\)](#)) as a valid method of opting out of data sales or targeted advertising. Confirm your consent infrastructure detects and processes these signals.

4 Inform Consumers About Their Rights

Consumers' rights under the DPDPA:

- **Right to know:** Whether personal data is processed, with confirmation and access to it
- **Right to access:** Request and receive a copy of their personal data
- **Right to disclosure:** Request and receive a list of the categories of third parties to which the controller has disclosed the consumer's personal data

- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data collected about them (with exceptions)
- **Right to data portability:** A copy of personal data in a portable, readily usable format
- **Right to opt out:** Of processing for the purposes of sale, targeted advertising, or profiling for decisions with legal or similarly significant effects
- **Right to nondiscrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent/guardian before a known child's (under 13) personal data is collected
- **Right to restrict use of sensitive personal information:** Limit or refuse collection or use of personal data the law classifies as sensitive

Note: When responding to access requests, do not disclose certain higher-risk identifiers directly (e.g., Social Security numbers, biometric data). Instead, notify the consumer that the data is held, without revealing it.

5 Review and Update Your Privacy Policy or Notice Every 12 Months

Review operations and potential legal changes every 12 months. Update the privacy policy and its effective date, even if no other changes are made. A [Privacy Policy Generator](#) can help.

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.

6 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.

7 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.

8 Conduct Data Protection Assessments Where Required

Since July 1, 2025, controllers processing the data of 100,000+ consumers must conduct [data protection assessments](#) where processing activities present heightened consumer risk (e.g., targeted advertising, data sales, certain profiling, sensitive data processing).

9 Enable and Respond to 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, verification, and tracking of [DSARs](#). If identity cannot reasonably be verified, inform the consumer and explain why, and enable them to rectify. Keep records of all requests and responses for 2 years after the last consumer interaction.

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