NEW JERSEY DATA PRIVACY ACT (NJDPA)

CHECKLIST

USERCENTRICS

New Jersey Data Privacy Act (NJDPA), gives New Jersey 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, 2025
Retroactive	No
Cure period	Sunset July 15, 2026, now at Attorney General's discretion

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 consumers, excluding data processed solely to complete a payment transaction, or
- Controls or processes the personal data of at least 25,000 consumers, and derives revenue or a discount on goods or services from the sale of personal data

Entity-level exemptions:

- State agencies and political subdivisions
- GLBA-regulated financial institutions and affiliates
- Secondary market institutions
- Certain insurance institutions and insurance support organizations
- National securities associations
- HIPAA-covered entities and business associates, but only for non-PHI data handled in accordance with HIPAA's privacy and security rules

Data-level exemptions:

- Protected health information under HIPAA
- GLBA-regulated financial data
- FCRA-regulated consumer report data
- Driver's Privacy Protection Act data
- Data processed in connection with certain human-subjects research

Notably absent are nonprofit organizations, higher education institutions, FERPA, and pseudonymous.

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
- Whether a third party may collect personal data about a consumer's online activity over time and across different commercial websites or services, using third-party cookies or trackers

Rights: Inform website visitors of their privacy rights and how to exercise them, including how to review and request changes to their personal data, or 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 Universal Opt-Out Signals

Recognize a consumer's opt-out preference signal, such as Global Privacy Control (GPC), as a valid method of opting out of the sale of personal data and targeted advertising.

4 Inform Consumers About Their Rights

Consumers' rights under the NJDPA:

- **Right to access:** Request and receive a copy of their personal data
- **Right to disclosure:** 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 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
- **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, or directly from individuals between the ages of 13 and 17
- **Right to restrict sensitive personal information:** Limit or refuse the collection or use of personal data the law classifies as sensitive

5 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.

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. Financial account information combined with a security code, access code, or password is classified as sensitive data under the NJDPA. This is a broader definition than most peer states.

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger, or directly from the individual if they are between 13 and 17, for processing their data for targeted advertising, sale, or profiling.

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.

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.