



LOUISIANA DATA PRIVACY ACT (LDPA)

CHECKLIST



USERCENTRICS

Louisiana Data Privacy Act (LDPA) gives Louisiana 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 organization conducts business in Louisiana or its products or services are consumed by Louisiana residents, and meets at least one of the following:

- Annual gross revenue exceeding USD 25 million
- Buys, receives, sells, or shares the personal data of 75,000 or more consumers or households annually for commercial purposes
- Derives 50 percent or more of annual revenue from selling personal data

Entity-level exemptions:

- State agencies and political subdivisions
- Nonprofit organizations
- Higher education institutions
- [GLBA](#)-regulated financial institutions
- [HIPAA](#)-covered entities and business associates
- Electric public utilities
- Organizations registered with the Secretary of State to conduct public opinion polls

Data-level exemptions:

- Protected health information under HIPAA
- Employee and job applicant data
- [FCRA](#)-regulated data
- Driver's Privacy Protection Act-regulated data
- FERPA-regulated student data

2 Create a Comprehensive Privacy Policy

Businesses are required to disclose:

- 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 processes it for targeted advertising

Rights: Explain how consumers can exercise their rights, including the appeal process.

Implementation: Provide a consumer request submission mechanism accessible from your website. If you sell sensitive or biometric data, post a separate, conspicuous disclosure.

A [Privacy Policy Generator](#) and a [CMP](#) can help. Also make sure to keep the [privacy policy](#) up to date. Update it every 12 months at least, even if only the last updated date needs to be changed. Otherwise, update it any time business operations, technologies in use, or regulatory requirements change.

3 Inform Consumers About Their Rights

Consumers' rights under the LDPA:

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

Consumers may designate an authorized agent to submit opt-out requests on their behalf. This can include a technology-based opt-out signal.

4 Honor Authorized-Agent Opt-Out Signals

Confirm your consent infrastructure can detect and process opt-out requests submitted via browser settings, extensions, or global device settings (e.g., [Global Privacy Control](#)). Only signals activated by an affirmative consumer choice, not a default setting, need to be treated as valid; confirm your implementation meets this standard.

5 Obtain Affirmative Consent for Sensitive Personal Data

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

- Racial or ethnic origin
- Religious beliefs
- Mental or physical health condition or diagnosis
- Sexual orientation or gender identity
- Citizenship or immigration status
- Genetic or biometric data processed to identify an individual
- Personal data from a known child under 13
- Precise geolocation

6 Handle Children's Data in Line With COPPA

Processing of personal data from a known child under 13 must comply with [COPPA](#), and requires affirmative parental or guardian consent.

7 Audit Consent Interfaces for Dark Patterns

The LDPA prohibits [dark patterns](#), including any practice the FTC designates as such.

8 Review Data-Sharing Arrangements Against the LDPA's "Sale" Definition

Louisiana's definition of "sale" covers both monetary and other valuable consideration. This is broader than some comparable state laws, which limit "sale" to money changing hands. Reassess arrangements that were excluded elsewhere.

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

Provide at least two secure contact methods. Consumers cannot be required to create a new account solely to submit a request.

10 Respond to DSARs

Respond to [DSARs](#) within 45 days, extendable by a further 45 days with notice to the consumer. Provide responses free of charge once per 12-month period per consumer. Manifestly unfounded, excessive, or repetitive requests may be charged a fee or declined. The burden of demonstrating this falls on the business. Responses must be free of charge, up to twice per year per consumer.

11 Establish an Appeal Process

Resolve appeals within 60 days. If denied, direct the consumer to the Louisiana Attorney General's complaint mechanism.

There is a cure period available from January 1 to July 31, 2027. However, after that the opportunity to cure is at the AG's discretion..

12 Maintain Written Processor Contracts and Conduct Data Protection Assessments

Govern processor relationships with a written agreement covering instructions, data types, duration, and obligations, including subprocessor terms. Conduct [data protection assessments](#) for targeted advertising, data sales, profiling, and sensitive data processing. These cover activities already underway before January 1, 2027 that continue past that date, as well as new activities.

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

GET IN TOUCH