KENTUCKY DATA PRIVACY

CHECKLIST

USERCENTRICS

THESE STEPS WILL HELP YOU ACHIEVE COMPLIANCE WITH THE KENTUCKY CONSUMER DATA PROTECTION ACT (KCDPA), WHICH APPLIES TO AND PROTECTS RESIDENTS OF KENTUCKY.

The checklist also includes recommended best practices for data privacy-related user experience.

1 Determine if your company is required to comply

If your for-profit organization:

- controls or processes personal data of at least 100,000 consumers or
- controls or processes personal data of more than 25,000 consumers and
- derives over 20% of gross revenue from the sale of personal data

Important to know:
The KCDPA is effective January 1, 2026. It does not apply retroactively.

2 Create a comprehensive Privacy Policy

Purpose: Inform consumers at or before the point of data collection:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data that 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 with regard to the consumer's request.

Language: Ensure the Privacy Policy is clear and easy to understand.

Implementation: As a best practice, implement a privacy notice with information about data use, consumers' rights and user options, like consent opt out. Enable consumers to exercise rights, like opting out, via a **banner or popup** when users visit your site, e.g. with a Consent Management Platform.

3 Inform users about their rights

Consumers' rights under the KCDPA:

- **Right to access:** request and receive a copy of their personal data
- **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
- **Right to nondiscrimination:** for exercising privacy rights
- **Right of minors:** consent must be obtained from a parent/guardian before children's (under age 13) personal data is collected
- **Right to restrict use of 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 or Notice every 12 months

Review your operations and potential changes in the law every 12 months. Updating your Privacy Policy information and the **effective date**. Effective date should be updated even if you don't make any other changes to the Policy.

Transparency: Ensure that the information that users must be notified about is clear, comprehensive and up to date. Ensure that the date of the last update is clearly visible.

Data sold: List all the categories of personal information that 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 the use of a Consent Management Platform (CMP).

6 Authenticate consent for collection of sensitive personal data or data from minors

Sensitive personal data: Consent is required for processing of 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 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.

8 Set up a system to verify Data Subject Access Requests (DSARs)

Enable consumers to **attach documentation** when submitting a request, to enable secure verification of their identity and residency.

Set up a system to enable submissions for verification requests.

If your business cannot reasonably verify the consumer's identity to the appropriate degree of certainty, it must **inform the consumer and explain** why the request could not reasonably be verified, and enable the consumer to rectify.

9 Keep track of Data Subject Access Requests (DSARs)

Set up a system to track all requests.

Time period: keep records of all requests and your business responses for **2 years** after the last consumer interaction.

10 Fulfill Data Subject Access Requests (DSARs)

Standard time period: **within 45 days**.

Extended time period: **up to 90 days**.

Usercentrics solutions enable your business to achieve and maintain KCDPA compliance. Do you have questions?

GET IN TOUCH