Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

December 22, 2025

Effective Jan. 1: California Regulatory Updates, New State Privacy Laws, and Opt-Out Signal Requirements

By Amy S. Mushahwar, Tricia Y. Wagner CIPP/US, CISSP, CISA, and Chloe Rippe

A significant set of U.S. state privacy law developments, all effective Jan. 1, will expand compliance obligations for companies operating nationwide. These developments fall into three principal categories: (1) new regulatory requirements adopted by the California Privacy Protection Agency (CPPA) under California's Consumer Privacy Act of 2018 (CCPA), which includes enforcement of privacy and security risk assessment requirements; (2) new comprehensive consumer privacy statutes in Indiana, Kentucky, and Rhode Island; and (3) statutory requirements in Delaware and Oregon mandating recognition of universal opt-out preference signals.

Together, these changes reflect the continued maturation of state privacy regimes and reinforce the need for scalable, multi-jurisdictional privacy compliance programs, including clear risk assessment protocols. We start first with the CCPA Amendments and Regulatory Updates, given that many companies benchmark their compliance programs as a differential of the CCPA (and European Union's General Data Protection Regulation ("GDPR"), if they purposefully direct activities to the EU market).

1. California: CCPA Amendments and Regulatory Updates

California continues to shape U.S. privacy regulation through ongoing amendments to the CCPA, codified at California Civil Code § 1798.100 et seq., and its implementing regulations administered by the CPPA.

The CPPA regulations adopted in 2025–addressing risk assessments, automated decision-making technology (ADMT), cybersecurity audits, and related updates to existing compliance requirements–take effect beginning Jan. 1 and introduce new and revised requirements affecting transparency, consumer rights, sensitive personal information, and organizational governance.

California's New Mandatory Risk Assessment Framework

One of the most significant changes effective Jan. 1 is California's new mandatory risk-assessment framework for certain high-risk processing activities, which requires businesses to conduct a risk assessment before initiating covered processing on or after Jan. 1 and to complete assessments for certain covered processing already underway by Dec. 31, 2027.

The regulations require a risk assessment when personal information is processed in ways that could materially impact consumer privacy, including (but not limited to):

- Using ADMT for decisions that produce legal or similarly significant effects on consumers (e.g., eligibility determinations, financial or housing decisions).
- Processing sensitive personal information, particularly if it could limit a consumer's rights, opportunities, or access to essential services.
- Selling or sharing personal information in a manner that may expose consumers to increased privacy risks.

- Profiling individuals, especially when used for behavioral advertising, workplace monitoring, or other activities that may impact consumers in meaningful ways.
- Processing that could create a reasonably foreseeable risk of harm, including risks related to discrimination, loss of confidentiality, or economic injury.

Given the complexity of these assessments and the potential exposure to regulatory enforcement, companies should consider conducting preliminary risk assessments under attorney-client privilege to protect the analysis from disclosure, especially if California's regulations create newly risk-assessed infrastructure. The final risk assessment can then be completed after a period of remediation.

Additional California Regulatory Updates

Beyond risk assessments, the regulations also implement a range of additional updates that materially affect day-to-day CCPA compliance, particularly in the following areas:

- Transparency and Notice Requirements: The regulations update the rules governing notices at collection and the presentation of opt-out and limitation rights, including enhanced requirements for clarity, placement, and accessibility across interfaces such as mobile apps, connected devices, and other nontraditional user interfaces (Cal. Civ. Code §§ 1798.100(a), 1798.120(b), 1798.135; CPPA Regulations).
- Sensitive Personal Information: The regulations expand and clarify requirements governing the use and disclosure of sensitive personal information, including refinements to how businesses must present and honor the right to limit use and disclosure of such information, as well as additional protections for personal information relating to consumers under the age of 16 (Cal. Civ. Code §§ 1798.120(c)-(d), 1798.121, 1798.140(ae); CPPA Regulations).
- Consumer Rights Requests: The regulations impose more prescriptive requirements for receiving, verifying, responding to, and documenting consumer rights requests, including affirmative confirmation that requests to opt out of sale or sharing and requests to limit use have been honored, and include expanded recordkeeping obligations (Cal. Civ. Code §§ 1798.130, 1798.135; CPPA Regulations).

2. New Comprehensive Privacy Statutes: Indiana, Kentucky, and Rhode Island

Three new comprehensive state privacy laws take effect on Jan. 1, extending privacy rights to residents of Indiana, Kentucky, and Rhode Island:

- Indiana Consumer Data Protection Act (INCDPA)
- Kentucky Consumer Data Protection Act (KCDPA)
- Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)

Each statute follows the now-familiar controller-processor framework and grants consumers rights to access, correct, delete, and obtain copies of their personal data, in alignment with most company privacy programs that are often optimized to the European Union's GDPR and California's privacy laws, as discussed above, and most companies provide state differential practices as new privacy statutes deviate from this model and even more come online. Similar to past practices in other states, the laws also provide consumers with the right to opt out of targeted advertising, the sale of personal data, and certain profiling activities and impose heightened requirements for the processing of sensitive data, generally requiring affirmative consumer consent.

While Indiana and Kentucky impose baseline transparency obligations requiring controllers to describe categories of personal data processed, purposes of processing, and categories of third parties with whom data is shared through generally applicable privacy notice requirements and consumer opt-out rights, Rhode Island's notice framework diverges from the general model adopted by most states. Rather than impose an omnibus privacy notice obligation applicable to all covered controllers, the RIDTPPA's notice requirements apply specifically to commercial websites and internet service providers that collect, store, and sell personally identifiable information (PII) and require disclosure of the categories of personal data collected, the identities of all third parties to whom PII has been or may be sold, and an active contact

mechanism, along with a clear and conspicuous statement if personal data is sold or used for targeted advertising. Unlike corresponding laws in many states, the RIDTPPA does not explicitly require the disclosure of processing purposes in these notice provisions.

3. Delaware and Oregon: Mandatory Recognition of Universal Opt-Out Preference Signals

Effective Jan. 1, both Delaware and Oregon require covered businesses to recognize and honor universal opt-out preference signals as a valid method for consumers to exercise their opt-out rights:

- Delaware Personal Data Privacy Act § 12D-105
- Oregon Consumer Privacy Act, ORS § 646A.576

Under both statutes, businesses that engage in targeted advertising or the sale of personal data must treat a valid opt-out preference signal, sent with the consumer's consent and transmitted through a consumer's browser or device settings, as a binding opt-out request, to the extent the signal can be reasonably recognized and processed, without requiring the consumer to submit a separate request or take additional steps.

Because these requirements are substantively aligned, businesses can generally address Delaware and Oregon through a unified technical and operational approach. Implementation, however, raises practical considerations, including:

- Ensuring systems can detect and process recognized opt-out signals
- Aligning signal-based opt-outs with existing consent and preference-management tools
- Communicating opt-out status to processors and downstream third parties
- Avoiding user-interface designs that could be viewed as frustrating or undermining consumer choice

As more states adopt similar requirements, honoring universal opt-out signals is quickly becoming a baseline component of U.S. privacy compliance.

What Companies Must Do Now

In light of these Jan. 1 developments, companies should take immediate action in the following areas:

- Conducting Applicability Assessments: Reassess whether the INCDPA, KCDPA, and RIDTPPA apply based on data processing thresholds and business activities. Companies processing significant volumes of consumer data may now fall under multiple state regimes.
- Updating Privacy Notices: Privacy notices must be updated to reflect newly effective state-specific rights and disclosures, including the specific disclosure requirements under Rhode Island's framework for commercial websites.
- Implementing Opt-Out Signal Recognition: Technical systems must be capable of recognizing and honoring universal opt-out preference signals in Delaware and Oregon. This requires coordination between legal, privacy, and engineering teams to ensure proper technical implementation.
- Reviewing and Updating Vendor Agreements: Vendor and processor agreements must be reviewed to confirm alignment with updated controller-processor obligations and downstream opt-out requirements across all applicable jurisdictions.
- Conducting California Risk Assessments: For companies subject to the CCPA, implement processes for meeting the new risk assessment obligations, determine which processing activities trigger the risk assessment requirement, and engage counsel to conduct pre-assessments under attorney-client privilege. This is particularly critical for companies that have not previously conducted comprehensive privacy risk assessments across their California-subject data environment, as the assessments may reveal compliance gaps that should be protected from disclosure. Companies must also understand when cybersecurity audits are required under the new regulations.

The risk assessment requirement presents both a compliance obligation and an opportunity to strengthen privacy governance. Companies that approach these assessments strategically–under privilege and with experienced privacy counsel in a pre-assessment phase–can identify and address vulnerabilities before they result in the final reporting that may be requested for regulatory review.

Looking Ahead

With additional state privacy laws scheduled to take effect in 2026 and beyond, and with regulators increasingly focused on enforcement and accountability, the Jan. 1 changes reflect a broader evolution toward more mature and enforceable state privacy regimes.

Lowenstein Sandler's Data360 team continues to advise clients on these developments and on building scalable, risk-based privacy compliance programs. Please contact us if you would like assistance evaluating how these changes affect your organization.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data Privacy, Security, Safety & Risk Management
T: 202.753.3825
amushahwar@lowenstein.com

TRICIA Y. WAGNER CIPP/US, CISSP, CISA
Counsel
T: 202.753.3658
twagner@lowenstein.com

CHLOE RIPPE
Associate
T: 212.419.5895
crippe@lowenstein.com