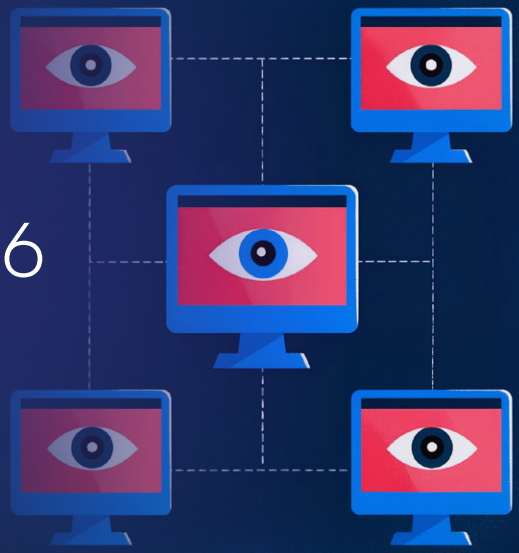
1touch.io
Data Aware Security

Preparing for January 2026 State Privacy Changes

What Privacy, Legal, and Security Leaders Need to Know (US)



Executive Summary

January 2026 marks a turning point in US privacy enforcement. This shift is not driven by a single law, but by a convergence of new state statutes, amendments, and enforcement mechanisms that materially change how privacy programs are expected to operate.

Regulators are raising expectations in three areas:

- Broader and more consistent consumer rights
- Evidence-based governance and risk reporting
- Operational accountability across data, vendors, mobile apps, and automated systems

Organizations that rely primarily on policies, spreadsheets, and manual workflows will struggle to keep pace. Those that invest in visibility, automation, and defensible evidence will be better positioned to meet regulatory scrutiny and executive expectations.

1. Why January 2026 Matters

By January 2026, the US privacy landscape becomes significantly more complex due to:

- Three new state privacy laws taking effect
  Rhode Island, Kentucky, and Indiana
- California's Delete Act entering an active enforcement phase for data brokers
- Amendments across multiple states focused on children's privacy, geolocation data, mobile applications, automated decision making, and risk assessments

At the same time, roughly 30 percent of Americans are now covered by comprehensive state privacy laws. The historical approach of managing privacy requirements strictly on a state-by-state basis is breaking down.

Privacy teams are increasingly expected to grant core consumer rights more broadly, prove governance and cybersecurity controls with defensible evidence, and address specific edge cases regulators now prioritize, including children's data, SDK behavior, and broker-style data sharing.

For many organizations, this translates into more audits, more executive scrutiny, and increased operational pressure.

2. Key Regulatory Developments

New State Privacy Laws

Rhode Island, Kentucky, Indiana

All three states introduce familiar consumer rights such as access, correction, deletion, portability, and opt out. However, their differences have meaningful operational implications.

Rhode Island includes high penalties with no cure period, a low revenue threshold that pulls in smaller and mid-size organizations, expanded notice requirements for commercial websites and ISPs, and disclosure obligations for current and potential third-party data sharing, including "may sell" relationships.

Kentucky includes a permanent cure period that makes enforcement more business-friendly, aligns closely with Virginia-style privacy frameworks, and applies a narrow, literal definition of "sale".

Indiana has no revenue threshold but broad exemptions, allows access requests to be fulfilled with representative summaries, and includes an unusual provision limiting revocation of consent once given.

Many organizations are shifting toward granting baseline rights to all US users, applying state-specific controls only where required, scaling DSAR, correction, and opt-out workflows, and centralizing consent, preference, and third-party tracking.

B California Delete Act

The California Delete Act applies to data brokers, but California defines this category broadly.

An organization may be considered a data broker if it sells or shares personal data, or uses pixels, SDKs, or tracking technologies that enable secondary data use.

Key milestones include annual registration with California, centralized deletion requests through the DROP mechanism beginning in January 2026, expectations for processing bulk deletion and opt-out requests at scale by August 2026, and formal audit requirements beginning in 2028.

Organizations must be able to determine whether they qualify as a data broker based on actual data flows, delete and suppress data across multiple systems from a single request, accurately match identities and prevent re-ingestion, and log actions for audit and enforcement defense.

Regulators have signaled that organizations operating in gray areas will likely be treated as data brokers.

C Expanding Regulatory Focus Areas

Children's privacy requirements are tightening across states, including restrictions on selling data or targeted advertising, age assurance and content controls, and treating children's data as sensitive by default.

Complexity arises from different age thresholds across states, enforcement based on context and behavior rather than stated age, and increased scrutiny of services that appear child-focused. Organizations cannot rely solely on statements such as "we do not market to children" to avoid obligations.

Some states prohibit the sale of precise geolocation data outright, even with consent. This directly affects mobile applications and services that rely on location-based monetization.

Regulators are increasingly focused on mobile applications and SDKs, particularly SDK-driven data sharing, secondary uses and profiling, and alignment between app store disclosures and internal practices. Many organizations underestimate the privacy risk introduced by mobile SDKs and embedded third-party services.

California CCPA Amendments

California is adding several material obligations that significantly raise the bar for privacy governance.

Risk assessments must be ongoing with annual reporting and executive attestation under penalty of perjury. Regulators expect evidence-backed analysis rather than policy summaries.

Cybersecurity audits formally link privacy obligations with security controls.

Organizations must accept authorized agent requests while still verifying identity and preventing abuse.

California is also adding explicit opt-out rights for certain automated decision making, aligning with broader AI transparency and governance trends.

These changes increase personal accountability for executives and elevate the importance of defensible reporting.

3. How Privacy Programs Are Evolving

Organizations are moving away from a single national baseline with state-specific exceptions and toward broad rights granted by default with targeted controls for age, region, or prohibited uses.

Effective privacy programs increasingly start with understanding real data flows across cloud, SaaS, mobile apps, and vendors, cataloging trackers, SDKs, APIs, and broker relationships, and identifying technical controls that can be enforced consistently.

Many teams are planning for future expansion by building reusable age and regional controls, preparing for broker-style suppression obligations, and creating scalable pipelines for risk and audit evidence.

4. Readiness Questions for 2026

Organizations preparing for January 2026 should be able to answer whether they can process access, deletion, correction, and opt-out requests consistently across jurisdictions, whether they understand if tracking technologies or partners classify them as a data broker, whether they can suppress and delete identities across all systems from a single request, and whether they have visibility into mobile SDK data flows and secondary uses.

They should also be able to explain what evidence executives will rely on when signing risk assessments and how authorized agent requests are handled without increasing fraud risk.

If these answers rely heavily on spreadsheets, manual coordination, or point-in-time snapshots, gaps are likely to surface under regulatory scrutiny.

5. What “Good” Looks Like in 2026

Organizations best positioned for 2026 typically have unified visibility into sensitive and personal data across environments, evidence-grade governance that supports audits and executive attestations, scalable rights management capable of handling centralized and bulk requests, age-aware and region-aware policy enforcement, and clear executive reporting grounded in actual data risk.

Final Thought

January 2026 is less about checking new compliance boxes and more about operational credibility.

Privacy programs that can clearly demonstrate where data lives, how it flows, and how controls are enforced will move faster and with less risk. Those that cannot will face increasing regulatory and executive pressure.