KASOWITZ

Data Privacy, AI Regulatory, and Compliance Update: 2026

Spring of 2026 will continue as an active period of privacy compliance and focus on global AI governance. There are several new U.S. and international laws and amendments taking effect mid-year for companies to be aware of. From seismic shifts in child privacy rules to the most comprehensive AI regulation we have seen thus far in the U.S., critical new AI, privacy, and technology compliance obligations will be going into effect over the next few months that companies should be prepared for. Now is the time to engage counsel to ensure your company can navigate these complex obligations.

COPPA Amended Rule Compliance Date

On April 22, 2026, the amended COPPA Rule will finally move from regulatory text to required compliance. The FTC's 2025 revisions, which are the first major overhaul in more than a decade, impose a fundamental shift in how operators will need to handle children's data. This will impact not only platforms squarely directed to children under thirteen, but also for the far broader universe of "mixed-audience" services whose users may include minors of various ages.

At the center of the new Rule is a more demanding standard for disclosures and parental consent. The familiar "support for internal operations" exception which has long been a safe harbor for analytics, performance measurement, and limited adtech, has been substantially narrowed. Operators may no longer rely on broad contractual language or generic parental notices to cover data sharing with SDKs or plug-ins. Instead, they must obtain specific, informed parental consent before disclosing a child's personal information to any third party that does not fall squarely within the internal-operations exception. This requirement shifts compliance from the legal team to the architectural level: engineers may need to reconfigure data flows so that consent signals literally gate which APIs or cookies/adtech are activated.

The rule also enshrines, for the first time, an explicit obligation to maintain documented data retention and deletion schedules tied to the stated purposes of collection. The FTC has long criticized "indefinite retention" as a backdoor risk to children's privacy, but 2026 will mark the first time operators must have a formal policy and system-enforced deletion processes. Privacy and governance leaders will need to align these schedules with broader record retention programs, especially since retention for COPPA purposes may be shorter than that permitted for other categories or data under comprehensive state privacy laws.

The compliance burden will fall not only on game studios, streaming platforms, and education tech providers, but also on advertisers, analytics vendors, and SDK developers whose data collection may now constitute "operation of a website or online service directed to children." Many of these entities will, for the first time, have to

implement verifiable parental consent workflows or contractual clauses that will require partners to do so.

UK Digital Verification Services (DVS) under the DUAA

The UK's DVS regime passed under the Data (Use and Access) Act of 2025. The heart of the DVS lies in certified identity and attribute providers, i.e., entities that can issue verifiable assertions about individuals (age, identity status, credentials). These assertions will support verified access to services and data, including government and regulated services. To participate, providers must embed themselves into the UK Digital Identity & Attributes Trust Framework, which has been an iterative process.

For organizations that rely on third-party identity providers (e.g., for age gating, attribute-based access, digital onboarding, verifiable credentials), DUAA resets the terms of trust. It is not good enough to accept a provider's assertion in good faith: under the DUAA, replying parties must verify that the provider is duly certified, monitor certificate validity, accept revocation signals, and incorporate proof-of-validity checks before granting access or relying on attributes. This likely introduces vendor compliance monitoring as a new, necessary privacy control.

Because identity attributes are often highly sensitive (for instance, DOB, identity number, age categorization), the DVS regime recases them as regulated signals. Privacy teams will need to treat them with elevated controls: minimize which attributes are retained, log provenance and usage, restrict access to verification results, and ensure that downstream processors or analytics tools do not re-use them in unanticipated ways.

Moreover, DUAA's tension with existing UK GDPR and DPA frameworks must be managed carefully. On one hand, DUAA enables stronger verified access to regulated services; on the other, reliance on verification must comport with data protection principles, and you cannot request or use more identity attributes than strictly necessary, nor process them without an adequate legal basis (e.g., explicit consent or statutory authorization).

From a program standpoint, preparatory steps should include auditing your identity/attribute providers, segregating which ones already hold certification, and embedding revocation monitoring in downstream flows. Contracts with providers should likely be amended (or created) to include re-certification requirements, audit data sharing, liability clauses, and immediate revocation obligations under DUAA standards. Internally, DPIA templates should also be updated to include DVS flows and revocation events among the triggers for impact assessments.

Colorado's Comprehensive AI Framework

Colorado remains the most ambitious U.S. jurisdiction in building an EU-style AI law. Senate Bill 205, the Colorado Artificial Intelligence Act, becomes fully effective on June 30, 2026 (after a five-month extension adopted in 2025). The statute focuses regulation on both developers and deployers of high-risk AI systems, defined as systems that make or materially contribute to decisions in high-impact contexts such as credit,

employment, housing, insurance, education, health care, and access to government services.

For developers, the law imposes a duty to exercise reasonable care to prevent algorithmic discrimination. Developers must prepare technical documentation describing system design, training data, risk-testing results, and known limitations, and they must furnish that documentation to both regulators and business customers.

Deployers (the organizations actually using high-risk AI) must conduct initial and annual impact assessments, establish written risk-management policies, and provide pre-use notices to consumers explaining that an automated system is involved. If a consumer experiences an adverse outcome, such as a loan denial or employment rejection, the deployer must issue an adverse-action notice and offer information about the logic and data sources influencing the decision. Deployers must also post a public statement describing how they use high-risk AI and the safeguards in place.

Colorado's framework is unusual in expressly recognizing compliance with the NIST AI Risk Management Framework or ISO/IEC 42001 as a rebuttable presumption of compliance. In practice, adopting those frameworks can serve as an affirmative defense if enforcement arises.

Only the Colorado Attorney General may enforce the statute; there is no private right of action.

* * *

Kasowitz's Data Strategy, Privacy, and Security team has deep knowledge in the data, privacy, and security sectors, and is familiar with the potentially existential risks faced by companies that rely on data as an engine of commerce and innovation. Global data, AI, privacy, and security threats are "bet the company" issues that Kasowitz is well equipped to handle. Our team consists of seasoned lawyers who have worked at or represented the largest and most innovative companies in the world, former regulators, and former government attorneys. We leverage our extensive subject matter knowledge to support companies through global privacy and technology counseling, regulatory support in the AI, privacy and security space, litigation, and incident preparedness and response.

For more information, please contact:

Brandy Worden
Partner
bworden@kasowitz.com

Frederick C. Bingham
Associate
fbingham@kasowitz.com

Cyrus Borhani
Associate
cborhani@kasowitz.com