KASOWITZ

Data Privacy, AI Regulatory, and Compliance Update: 2026

New U.S. and international laws related to privacy compliance and global AI governance continue to take effect throughout the year. From app store accountability requirements in Utah, to the EU's GPAI Code of Practice, to U.S. profiling rules, organizations are facing a more operational and interconnected compliance landscape. These developments, outlined below, underscore the need for coordinated compliance counseling.

Utah App Store Requirements

Utah's App Store Accountability Act will reach full compliance on May 6, 2026. The statute shifts responsibility for age verification and parental consent from app developers to the app-store layer itself: App stores must determine a user's age when an account is created, classify minors, and link them to a parent or guardian account that can grant consent before any downloads or in-app purchases can occur. App stores would be required to inform each developer if the parent or guardian revokes consent. In addition, private right of action provisions kick in on December 31, 2026. However, Utah recently passed an amendment bill, HB 498, which may materially change timing and enforcement if it becomes law.

EU GPAI Code of Practice

In July 2025, the European Commission published a voluntary Code of Practice for General-Purpose AI, offering a pre-regulatory path for GPAI providers to align with Articles 53–55 before the Act's enforcement date. The Code broadly covers transparency, copyright compliance, and safety/security. It requires documentation sheets describing model architecture, training data provenance, compute and energy use, and risk-mitigation processes; adoption of written copyright-compliance policies; and serious-incident reporting within 15 days (or 2 days for imminent danger).

Providers adhering to the Code gain an evidentiary presumption of compliance under Article 53(4). The Commission's enforcement powers take effect in August 2026.

U.S. State Privacy Laws and Profiling Controls

This year, nearly twenty U.S. states will have comprehensive privacy statutes in force. Although framed as consumer-privacy laws, many include AI-related profiling provisions functionally regulating automated decision-making. For example, Virginia's CDPA and Colorado's CPA both grant individuals the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects; language which is mirrored in Connecticut, Oregon, and Indiana statutes. These laws also require data-protection assessments for such processing.

For businesses, this means profiling activities including credit scoring, hiring algorithms, insurance risk models must be inventoried, subject to risk assessments, and paired with opt-out mechanisms. Attorneys General in California, Colorado, and Connecticut have already issued investigative demands on profiling practices, signaling active enforcement in 2026. Companies should therefore unify their privacy and AI compliance teams to ensure consistent documentation and consumer-rights handling.

* * *

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

Cyrus Borhani
Associate
cborhani@kasowitz.com

Frederick C. Bingham
Associate
fbingham@kasowitz.com