KASOWITZ

# Data Privacy, AI Regulatory, and Compliance Update: July 2026

July 2026 continued the rapid development of global privacy, AI, and online safety regulation. In the United States, two significant Supreme Court decisions addressed the independence of the Federal Trade Commission and constitutional protections for location data. At the same time, the EU finalized amendments to the AI Act, issued final transparency guidance, and released new guidance addressing generative AI training data, anonymization, and video games. Regulators abroad also advanced new requirements and enforcement priorities concerning age assurance, AI transparency, and consumer protection.

For businesses, the common theme is that privacy and AI compliance continues to become more technical and operational. Companies should review cross-border transfer safeguards, update AI Act compliance timelines, assess how training data is collected and validated, and prepare for more detailed regulatory expectations concerning age assurance, AI agents, and sector-specific data practices.

## ***Trump v. Slaughter*** **Raises New Questions About the EU-U.S. Data Privacy Framework**

On June 29, 2026, the U.S. Supreme Court issued its decision in *Trump v. Slaughter*. The Court held that the statutory provision limiting the President's authority to remove FTC commissioners violated the constitutional separation of powers. Although the case did not directly concern privacy or international data transfers, the decision may affect an important part of the EU-U.S. Data Privacy Framework because the European Commission's adequacy decision relies on the FTC to supervise and enforce the DPF Principles against participating U.S. companies. The Supreme Court's conclusion that FTC commissioners must remain subject to presidential control has therefore raised questions about whether the FTC continues to provide the independent oversight contemplated by the adequacy decision.

With this rationale, on June 30, 2026, Max Schrems and noyb sent a letter asking the European Commission to prepare for withdrawal of the DPF adequacy decision. Noyb argues that the loss of statutory independence at the FTC undermines the commercial enforcement component of the DPF. It also argues that the Court's reasoning may call into question the independence of the Data Protection Review Court and other bodies involved in reviewing U.S. government access to personal data.

The DPF remains valid and available for data transfers. The Supreme Court did not invalidate the framework, and the adequacy decision will remain in effect unless it is suspended, repealed, or annulled by the European Commission or an EU court. The Danish Data Protection Authority has nevertheless advised companies to revisit the

country assessments supporting their transfer impact assessments and to review their exit strategies.

The potential effect on the Data Protection Review Court is also unclear. Some commentators distinguish the FTC's role in enforcing commitments made by participating companies from the national security safeguards created through Executive Order 14086 and Department of Justice regulations. Under this view, *Slaughter* creates a significant question regarding FTC oversight but does not, by itself, invalidate the Data Protection Review Court or the safeguards relevant to transfers conducted through Standard Contractual Clauses or Binding Corporate Rules.

Companies should not discontinue DPF-based transfers solely because of the decision. However, companies relying on the DPF should identify transfers that do not have an alternative legal mechanism, maintain or implement SCC fallback provisions where appropriate, update transfer impact assessments, and monitor further action by the European Commission, the EDPB, and EU courts.

## ***Chatrie v. United States*** **Addresses Government Access to Location Data**

The Supreme Court also issued its decision in *Chatrie v. United States* on June 29, 2026. The case involved a geofence warrant through which law enforcement obtained Google Location History data associated with devices located near the scene of a crime.

The Court held that law enforcement conducted a Fourth Amendment search when it obtained the location information. The Court concluded that individuals have a reasonable expectation of privacy in records concerning their cell-phone location, even where the government seeks information covering a limited period and obtains it from a third-party technology company. The Court left for the lower court the question of whether the warrant was sufficiently particularized and supported by probable cause.

The decision does not prohibit companies from collecting or retaining location information. It does, however, increase the legal significance of precise and historical location data held by mobile applications, platforms, advertising providers, and other technology companies.

Companies that collect location information should review their retention practices and law enforcement request procedures. They should also confirm whether requests for location data receive appropriate legal review, whether responsive information can be isolated without producing additional data, and whether compulsory disclosures are properly documented.

## **EU AI Omnibus Enters into Force**

The EU AI Omnibus entered into force on July 27, 2026, establishing a revised implementation schedule and making several other changes to the AI Act.

Under the revised schedule, requirements for high-risk AI systems listed in Annex III will apply beginning December 2, 2027. Requirements for high-risk AI systems embedded

in products covered by EU product safety legislation will apply beginning August 2, 2028.

The Omnibus also expands access to regulatory sandboxes, extends certain accommodations for small and medium-sized companies to qualifying small mid-cap companies, simplifies aspects of AI literacy and EU database registration, and provides additional enforcement authority to the AI Office. The amendments also permit certain processing of special categories of personal data for bias detection and correction and prohibit AI systems used to create nonconsensual intimate content.

The revised dates do not delay all AI Act obligations. Requirements addressing prohibited practices, general-purpose AI models, AI literacy, and certain transparency obligations follow separate implementation schedules. Companies should update their AI Act roadmaps to reflect the revised high-risk dates without treating the Omnibus as a general postponement of compliance.

## European Commission Finalizes Article 50 Transparency

On July 20, 2026, the Commission published the final Article 50 transparency guidance before the relevant obligations begin applying on August 2, 2026.

Article 50 applies to several different uses of AI. Providers of systems designed to interact directly with individuals generally must inform those individuals that they are interacting with AI. Providers of systems that generate or manipulate synthetic audio, image, video, or text content must also mark covered outputs in a machine-readable format.

Deployers are subject to separate requirements for emotion recognition, biometric categorization, deepfakes, and certain AI-generated or manipulated text published to inform the public about matters of public interest. The applicable disclosure depends on the type of system, the content involved, and whether the company is acting as a provider or deployer.

The Commission also approved a voluntary Code of Practice concerning transparency of AI-generated content. Companies may comply through other measures, but non-signatories should be prepared to demonstrate that their technical marking and disclosure practices satisfy Article 50.

Companies should conduct a system-by-system assessment rather than use one general AI disclosure. The assessment should address the company's role, the type of content generated, whether the system interacts directly with individuals, and whether required technical marking is controlled by the company or a third-party provider.

## EDPB Issues Guidance on Anonymization and Web Scraping

On July 8, 2026, the European Data Protection Board adopted draft guidelines on anonymization and separate draft guidelines on web scraping in the context of generative AI. Both sets of guidelines are open for public consultation/comment through October 30, 2026.

The anonymization guidance addresses when information may fall outside the GDPR because individuals are no longer identifiable. The EDPB focuses on whether individuals can be isolated within a dataset, whether records can be linked, and whether information about an individual can be inferred. The guidance also recognizes that whether information is anonymous may depend on the circumstances and capabilities of the organization receiving or using the data.

The web-scraping guidance confirms that the GDPR applies when scraping involves the collection, storage, organization, or other processing of personal data. Among other things, companies must address legal basis, transparency, purpose limitation, data minimization, accuracy, and special category data. The EDPB also recommends that companies use reliable sources, document when information was collected, and validate scraped data before using it to develop or train AI systems.

For companies developing or purchasing AI systems, the guidance reinforces the importance of training-data diligence. Companies should understand where training data originated, when it was collected, whether it contains personal or sensitive information, what legal basis supports the processing, and what controls are available to correct or remove information.

## Spanish and Belgian Regulators Publish Video Game Privacy Guidance

On June 18, the Spanish and Belgian data protection authorities jointly published "Recommendations and Best Practices for Data Protection in Video Games." The authorities describe the document as the first guidance produced by European data protection regulators specifically to promote GDPR compliance in the design, development, and distribution of video games.

The guidance is directed to participants throughout the video game lifecycle, including developers, designers, studios, publishers, cloud providers, analytics vendors, anti-cheat providers, and AI technology providers. It addresses how GDPR roles may be allocated across the video game ecosystem and identifies common processing activities, threats, and risks.

The guidance also addresses telemetry, player profiling, behavioral predictions, automated decision-making, differentiated treatment, SDKs, launchers, cloud gaming, AI tools, and children's data. The regulators developed the recommendations through review of privacy notices, contracts, service-level agreements, and other documentation, together with analysis of games and supporting technologies in operation.

The document does not create new statutory obligations. However, it provides a detailed indication of how European regulators may apply existing GDPR requirements to video game products and supporting services.

Video game companies should review actual data flows across the product lifecycle, identify controller and processor roles, assess SDKs and third-party technologies, and confirm that contracts and privacy notices accurately describe how player information is

collected and used. Companies should also pay particular attention to profiling, anti-cheat tools, behavioral data, and processing involving children.

## UK Regulator Focuses on Age Assurance

On July 15, 2026, UK's Ofcom published its first statutory report on how online services are using age assurance to comply with the UK Online Safety Act. Ofcom found that age checks are being deployed more regularly but identified several areas in which services must improve their practices.

Ofcom stated that services using age inference should move to methods identified in its guidance as highly effective unless they can provide reliable and compelling evidence that their existing method meets the required standard. The regulator also emphasized that services remain responsible for age-assurance systems implemented by third-party vendors.

On July 16, 2026, Ofcom opened an investigation into whether TikTok has complied with its duty under Section 12 of the Online Safety Act to protect children from harmful content. The investigation will examine, among other issues, whether TikTok's age-assurance approach is highly effective at determining whether a user is a child. The opening of the investigation does not establish that TikTok violated the Act.

Companies subject to the Online Safety Act should maintain evidence supporting their age-assurance methods, test whether those methods correctly identify children, and document vendor diligence. Companies should also ensure that data collected for age assurance is limited, appropriately secured, and retained only as long as necessary.

## Japan Enacts Amendments to the APPI

Japan enacted amendments to the Act on the Protection of Personal Information on July 10, 2026, and promulgated the amendments on July 17, 2026. Most provisions will take effect on a date established by implementing order within two years. Japan's Personal Information Protection Commission is expected to issue implementing regulations and guidance before the amendments become operative.

The amendments expand individual rights to request that certain processing involving information derived from physical characteristics cease. They also introduce an administrative monetary surcharge where unlawful personal data processing produces an economic benefit. The final scope of these exceptions will depend on implementing rules, including conditions concerning purpose restrictions, public disclosures, contractual controls, and onward use.

Companies operating in Japan should monitor the implementing process and determine whether the amendments will require changes to rights-request procedures, data inventories, AI development practices, or enforcement-risk assessments.

## Moving Forward

Companies should use the remainder of 2026 to review the systems, transfers, and business practices affected by these developments. Priority areas should include identifying transfers that rely solely on the EU-U.S. Data Privacy Framework, updating EU AI Act implementation timelines, reviewing the sources and legal basis for AI training data, assessing age-assurance and children's safety, and video game data practices, as applicable.

Companies should also ensure that AI inventories cover systems that interact directly with individuals, generate synthetic content, act through external tools, or create persistent human-like interactions. Privacy, AI, product, and cybersecurity teams should coordinate these workstreams so that public disclosures, contracts, technical controls, and internal documentation remain consistent.

* * *

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