onetrust

Governing AI in 2026:

A global regulatory guide

2026

Table of Contents

onetrust

The pace of AI regulation has accelerated sharply. In 2025 alone, more than 3,200 regulatory updates were issued worldwide, with 875 directly related to AI laws and regulations. By the end of the year, 51 AI laws were already in force, 15 had been passed, and 97 more were in progress. In the United States, over 40 states introduced or considered close to 700 AI-related bills[1].

This shift is no longer theoretical. Enforcement activity across privacy and AI is intensifying, with over €2 billion in GDPR enforcement actions in 2025, including some of the largest fines on record. Regulators are now applying similar expectations to AI systems that influence individuals' rights, access, and opportunities.

This whitepaper examines how global AI regulation applies through 2026, with a focus on what privacy and compliance teams must operationalize today. It translates binding legal obligations into governance actions, using Europe and the United States as anchors, while addressing APAC and Latin America as rapidly maturing enforcement regions.

[1] OneTrust 2026 Predictions Report: Into the Age of AI – Lessons from the Future

1. The role of privacy and compliance teams in AI Governance

Artificial intelligence now shapes hiring decisions, credit assessments, healthcare access, pricing, content moderation, and public services. As these systems move from experimentation into production, regulators are assessing whether organizations can control risk, explain outcomes, and demonstrate accountability.

AI regulation does not replace privacy law. It extends privacy governance into automated and algorithmic systems that affect individuals at scale. Across jurisdictions, regulators expect organizations to:

- Identify where AI is used in decision-making
- Assess risks to individuals and fundamental rights
- Provide clear notice when AI influences outcomes
- Maintain documentation that demonstrates accountability
- Monitor systems after deployment and respond to incidents

These expectations closely mirror established privacy program responsibilities. As a result, privacy and compliance teams are increasingly responsible for making AI governance work in practice, even when AI development sits elsewhere in the organization.

Core regulatory patterns shaping AI governance

Across jurisdictions, and despite regional differences, binding AI laws follow a common structure:

- **Risk-based classification:** Most laws distinguish AI systems by impact, not technology. Systems used in employment, credit, healthcare, education, public services, or biometric identification consistently fall into higher-risk categories and trigger additional obligations.
- **Role-based accountability:** Regulators assign responsibilities across the AI lifecycle. Developers, deployers, distributors, and providers each carry distinct duties. This mirrors controller–processor models under privacy law and requires clear internal role definition.
- **Accountability through evidence:** Documentation, logging, assessments, and monitoring are treated as proof that governance exists in practice. Regulators increasingly view the absence of documentation as evidence of noncompliance.

For privacy teams, these requirements are not unfamiliar. They extend existing governance practices into AI-driven decision-making and automated systems.

2. Europe: Enforcement-ready AI governance

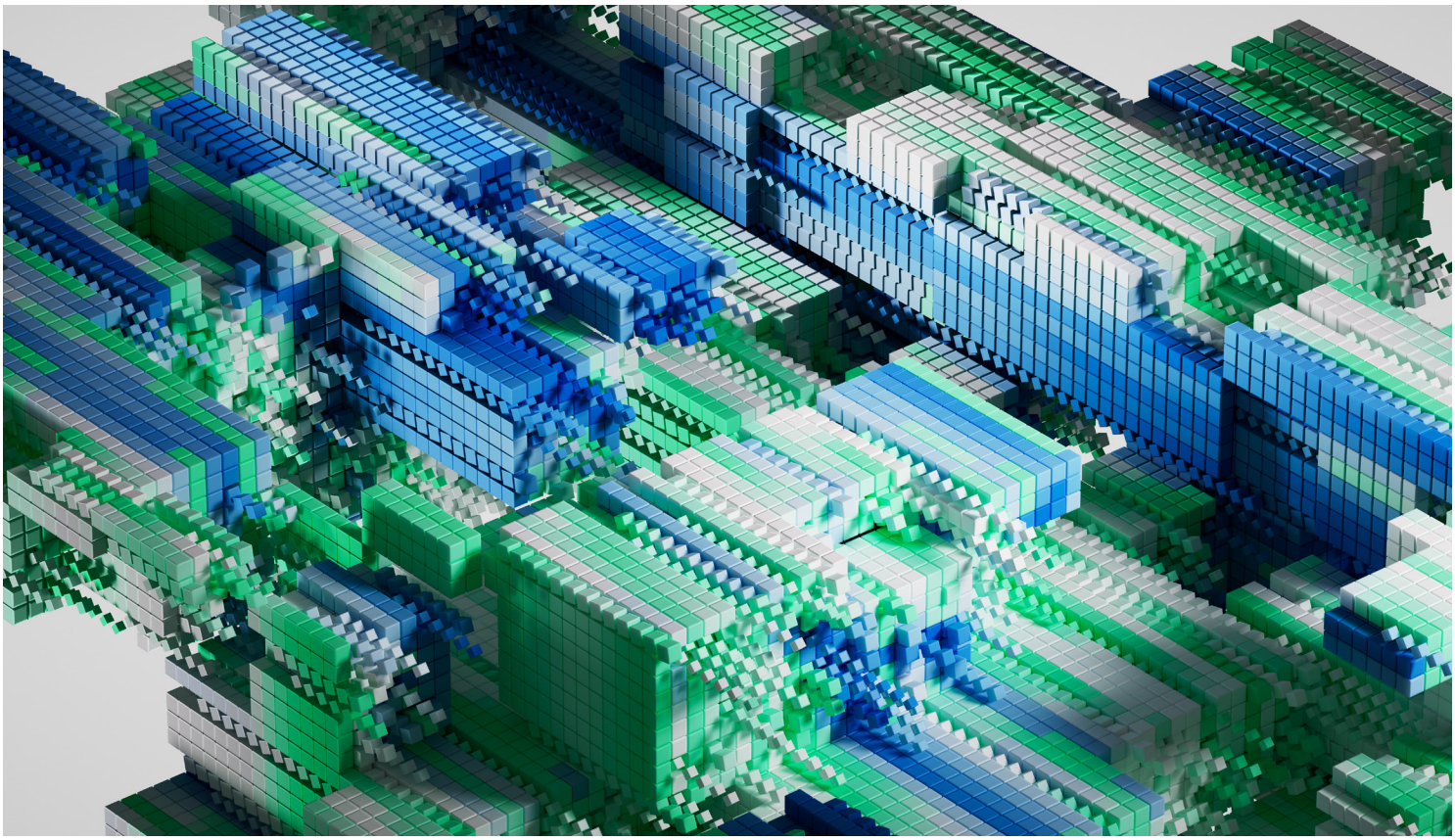
Regulatory overview

The EU Artificial Intelligence Act is the most comprehensive AI regulation currently in force. Its risk-based model classifies systems as unacceptable risk, high risk, specific transparency risk, and limited risk, with obligations scaling accordingly.

It entered into force in August 2024, with obligations phasing in through 2027. By 2026, organizations will already be expected to comply with:

- Prohibitions on certain AI practices
- Transparency obligations for AI interactions
- Governance requirements for general-purpose AI models
- Penalty provisions enforced by national authorities and the EU AI Office

High-risk AI systems must undergo pre-deployment assessments, maintain technical documentation, log system activity, and support post-market monitoring. Deployers must assess impacts on fundamental rights, reinforcing existing DPIA practices under GDPR.



Key obligations by actor

Actor	Core obligations
Providers	Technical documentation, conformity assessments, post-market monitoring, incident reporting
Deployers	Fundamental rights impact assessments, usage controls, monitoring
Distributors	Verification of conformity and documentation

Operational implications for privacy teams

Privacy teams are often responsible for:

- Integrating AI risk assessments with DPIA workflows
- Supporting fundamental rights impact assessments
- Maintaining documentation repositories
- Coordinating responses to regulator inquiries

The role of the EU Digital Omnibus

The Digital Omnibus proposal introduced in late 2025 seeks to align the GDPR, the AI Act, and ePrivacy obligations. It proposes adjustments to definitions of personal data, data subject rights, and legitimate interest, including broader flexibility for AI training.

While still under debate, the Omnibus reflects a shift in regulatory posture. European regulators are looking to simplify compliance mechanics without stepping back from oversight. For privacy teams, this suggests continued scrutiny of automated decision-making, profiling, and transparency, even as operational details evolve.

3. United States: State-led AI enforcement

In the absence of a federal AI statute, US states are defining enforceable standards through consumer protection and civil rights frameworks.

California, Colorado, and Texas are setting expectations around:

- Disclosure when individuals interact with AI
- Documentation of AI system purpose and limitations
- Controls to prevent discriminatory outcomes
- Oversight tied to existing enforcement authorities

Key laws effective in 2026

State	Law	Effective date	Focus
California	AI Transparency Act	Jan 1, 2026	Disclosure, content labeling
California	Gen AI Training Data Transparency Act	Jan 1, 2026	Dataset transparency
Colorado	AI Act	Jun 30, 2026	Algorithmic discrimination
Texas	Responsible AI Governance Act	Jan 1, 2026	Prohibited practices

These laws emphasize disclosure when individuals interact with AI, documentation of system purpose and limitations, and safeguards against discriminatory outcomes. Legislation also heavily focuses on specific use cases of AI, such as consumer transactions, healthcare, and deepfakes. Enforcement relies on existing authorities such as state attorneys general, with penalties tied to ongoing violations.

Operational implications for privacy teams

Privacy teams must ensure AI notices align with consumer privacy disclosures, rights request workflows accommodate AI-driven decisions, and documentation supports reasonable care defenses under state enforcement models.

4. Asia-Pacific: Binding rules and early enforcement

Several APAC jurisdictions have already moved beyond voluntary guidance and operate under binding AI frameworks.

South Korea's Basic AI Act enters into force on January 22, 2026. It applies extraterritorially where systems affect Korean users and introduces requirements for transparency, risk assessment, human oversight, and documentation, particularly for high-impact and large-scale AI systems. A draft enforcement decree published in September 2025 clarifies watermarking, disclosure, and oversight obligations.

China enforces multiple AI regulations, including the Generative AI Services Management Measures and Measures for the Identification of Synthetic Content Generated by AI effective September 1, 2025.

These laws impose obligations around consent, data quality, content labeling, user rights, and complaint handling.

Japan relies on a principles-based AI Act emphasizing cooperation and transparency rather than penalties. Vietnam's Law on Digital Technology introduces binding AI provisions effective in 2026, with a comprehensive AI Law entering into force on March 1, 2026, which includes labeling, transparency, and prohibitions tied to human rights and public order.

Across the region, AI governance is increasingly linked to data protection, security, and rights-based oversight.

Comparative overview

Jurisdiction	Law	Status	Key focus
China	Gen AI Services Measures	In force	Consent, labeling, user rights
China	Synthetic Content Measures	Sep 1, 2025	Content identification
South Korea	Basic AI Act	Jan 22, 2026	High-impact AI governance
Vietnam	Law on AI	March 1, 2026	Transparency, prohibitions
Japan	AI Act	In force	Principles-based governance

Operational implications for privacy teams

Privacy teams operating in APAC must manage overlapping AI, data protection, and content obligations, maintain localized documentation, and support user rights and complaint mechanisms embedded in AI regulations.

Operational implications for privacy teams

Brazil's framework places privacy teams at the center of AI governance by embedding rights-based protections, assessment requirements, and accountability mechanisms directly into AI regulation.

5. Latin America: Brazil's AI framework takes shape

Brazil is positioning itself as a leading AI regulator in Latin America. Bill No. 2338, approved by the Senate in December 2024 and awaiting final approval, introduces a comprehensive, risk-based AI framework aligned with the EU AI Act.

If enacted, organizations would need to support impact assessments, incident reporting, transparency obligations, and individual rights to contest AI-driven decisions, request human review, and seek correction of discriminatory outcomes.

6. How to operationalize AI-readiness

Effective AI-readiness requires extending privacy operations, not rebuilding them from scratch. Organizations need the ability to inventory AI systems, connect risk assessments to product changes, manage disclosures consistently, and maintain evidence across jurisdictions.

In practice, this means replacing fragmented spreadsheets and ad hoc reviews with workflows that embed assessment, documentation, monitoring, and response into day-to-day operations. Privacy teams benefit from centralized visibility into AI use cases, integrated assessment processes aligned with

DPIAs, automated tracking of regulatory changes, and scalable handling of rights and incident requests tied to AI-driven outcomes.

When governance is operationalized, teams spend less time chasing information and more time managing risk proactively. This reduces regulatory exposure while enabling responsible AI deployment at speed.

Governance as an enabler through 2026

Key AI regulatory milestones through 2026 include the phased application of the EU AI Act, the entry into force of multiple US state AI laws on January 1 and June 30, 2026, South Korea's Basic AI Act on January 22, 2026, and binding AI provisions across APAC and Latin America.

Organizations that reach these milestones with mature privacy programs in place will be better positioned to adapt. A well-run privacy function provides the structure AI governance now demands: clear ownership, documented assessments, transparent communication, and continuous monitoring.

As AI regulation moves deeper into enforcement, privacy becomes more than a compliance requirement. It becomes an enabler for innovation, allowing organizations to deploy AI responsibly, earn trust, and scale with confidence across global markets.

Assess your AI governance readiness for 2026.

Exolore our integrated privacy solutions to evaluate current privacy and AI controls against emerging regulatory expectations and identify operational gaps.

Learn more

Appendix - Regional regulatory comparison table

Region	Law	Effective timeline	Scope	Key focus areas	Enforcement
European Union	EU Artificial Intelligence Act	In force August 2024, phased application through 2027	Extraterritorial. Applies to AI systems used or affecting individuals in the EU	Risk classification, high-risk system obligations, GPAI governance, prohibited practices	National authorities and EU AI Office. Fines up to 7 percent of global turnover
United States	Colorado AI Act	June 30, 2026	Developers and deployers of high-risk AI systems operating in Colorado	Algorithmic discrimination, consumer transparency, documentation	Colorado Attorney General. Unfair trade practice model
United States	California AI Transparency Act and Gen AI Training Data Transparency Act	January 1, 2026	Large generative AI providers and developers of publicly available Gen AI systems	AI-generated content disclosure, dataset transparency, provenance controls	California Attorney General and local authorities
United States	Texas Responsible Artificial Intelligence Governance Act	January 1, 2026	Broad, with primary obligations on governmental agencies	Prohibited AI practices, biometric protections, transparency	Texas Attorney General with cure periods
Asia-Pacific	South Korea Basic AI Act	January 22, 2026	Extraterritorial. Applies where AI systems affect Korean users	High-impact AI, risk assessment, human oversight, documentation	Ministry of Science and ICT. Administrative and criminal penalties

onetrust