

# Global compliance readiness guide

Rapid tech innovation and evolving security threats are forcing regulators at every government level to adopt new policies, standards, and oversight. In this era of constant change, timely and engaging ethics and compliance training is essential. Here's your guide to identifying the highest-urgency compliance gaps in 2026.



## AI GOVERNANCE

**Regulations in focus:** EU AI Act | US state AI laws | Singapore AI Governance Framework for Agentic AI

**Applies to:** Global — any organization using or deploying AI systems that affect EU residents or US consumers

### WHAT CHANGED IN 2025:

- **The EU AI Act's** prohibited practices, governance, and AI literacy obligations became applicable, general-purpose AI rules also took effect.
- Enforcement:
  - In the US, **EEOC ramped up enforcement** against AI hiring tools
  - In New York City, **AI Bias Audit Law** enforcement is intensifying
- Singapore introduced **draft frameworks for agentic AI governance**, signalling growing regulatory focus on autonomous systems and structured oversight in Asia.

### WHAT'S CHANGING IN 2026:

- The EU AI Act's penalties and monitoring take effect, and high-risk (hiring, credit, healthcare, law enforcement) system compliance starts.
- **New laws** are taking effect in early 2026 in California, Texas, Colorado, Illinois, and New York.
- Ongoing introduction of laws and regulations across the US.
- Singapore launched the world's first **Model AI Governance Framework for Agentic AI**, formalising expectations for human accountability and oversight — requiring approval checkpoints and controls for autonomous systems to mitigate automation bias.



## DATA PRIVACY, CONFIDENTIALITY, AND INFO SECURITY

**Regulations in focus:** EU GDPR | EU Data Act | US state privacy laws


**Applies to:** Global — any organization collecting or processing personal data


### WHAT CHANGED IN 2025:

- **Amendments to California's CCPA** expanded data broker oversight.
- Changes to data privacy rules in **Australia** and **Brazil**.
- GDPR enforcement:
  - **TikTok fined €530M** for illegal data transfers
  - **Meta fined €479M** for consent manipulation

### WHAT'S CHANGING IN 2026:

- Comprehensive privacy laws take effect in **Indiana, Kentucky, and Rhode Island**, now totaling 20 states.
- States (notably Texas and California) are moving from warnings for non-compliance to enforcement.
- **Additional rules** for cybersecurity audits, risk assessments, and automated decision-making technology (ADMT) in California's CCPA.
- Third-party service and cloud providers are raising security and KYC requirements.
- **Additional EU Data Act obligations** come into force.
- New data protection laws and changes in **Vietnam, India**, and **the UK**.

 Train employees and leadership on responsible AI use, bias risks, and regulatory obligations. [Learn more](#)

 Conduct annual cybersecurity awareness training and phishing simulations for all employees. [Learn more](#)

# Global compliance readiness guide

Rapid tech innovation and evolving security threats are forcing regulators at every government level to adopt new policies, standards, and oversight. In this era of constant change, timely and engaging ethics and compliance training is essential. Here's your guide to identifying the highest-urgency compliance gaps in 2026.



## ANTI-MONEY LAUNDERING

**Regulations in focus:** FATF | EU AMLA | FinCEN (US)

**Applies to:** Financial services, real estate, luxury goods, and other industries

### WHAT CHANGED IN 2025:

- The EU's authority for anti-money laundering and countering the financing of terrorism (**AMLA**) became fully operational.
- FATF revised its **recommendations** to ensure stricter payment transparency.
- China amended its **AML Law**.
- Notable penalties:
  - **Germany fined JPMorgan** a record €45M for systemic failures in AML controls
  - **The Central bank of Ireland fined Coinbase** €22M for AML breaches

### WHAT'S CHANGING IN 2026:

- The EU AMLA will develop regulations and implementations for technical standards to harmonize AML rules across member states.
- The EU's sixth anti-money laundering directive (**6AMLD**) sanctions standards and penalties will be finalized, they will require more robust KYC technology and enhanced training.



Ensure staff is trained on money laundering red flags and suspicious activity reports (SARs) filing procedures.

[Learn more](#)



## ANTI-HARASSMENT, DISCRIMINATION, AND DEI

**Regulations in focus:** EU Pay Transparency Directive | Title VII (US) | UK Equality Act | US State mandatory training laws

**Applies to:** All employers globally — especially those operating in the EU or with US multi-state workforces

### WHAT CHANGED IN 2025:

- In the US, there's a **new compliance landscape** for federal contractors.
- Notable lawsuits:
  - **Apple is facing a class-action lawsuit** over alleged gender pay bias and sexual harassment.
  - The family of **Stephanie Cosme**, a 32-year-old Air Force contractor, filed a lawsuit alleging that racial and gender discrimination contributed to her death.

### WHAT'S CHANGING IN 2026:

- EU member states have to transpose into national law the **EU Pay Transparency Directive**. Companies have to conduct pay gap analysis and prepare for mandatory reporting.

### US STATE PATCHWORK:

- Six states (California, Connecticut, Delaware, Illinois, Maine, and New York) mandate **harassment training** for ALL private employers, each with different frequency, duration, content, and audience requirements.
- Several states (Florida, Nevada, New Jersey, and Texas) mandate training for government employees only.
- Washington state expanded the private-sector mandate on January 1, 2026.



Train employees (including remote and hybrid workers) and managers on their role in preventing harassment, handling complaints, and non-retaliation. [Learn more](#)