



SecComply • EBOOK

AI Regulation Outlook 2027

What changed in 2026, and how to get ready

OCTOBER 2026 EDITION

Covers the EU AI Omnibus, Colorado SB 26-189, India's synthetic content rules and California's 2026 AI package



PREPARED BY **SECCOMPLY** • AI SECURITY, GRC, CISO ADVISORY

✉ info@seccomply.net

🌐 seccomply.net



100+
customers across
four continents



4 regions
US, Europe, Middle
East, India



4 pillars
GRC, AI security,
cloud, CISO
advisory



Award 2026
Emerging Tech
Start-up of the Year

ABOUT THIS EDITION

A rulebook that kept moving

At the start of 2026 most compliance calendars had one date circled: 2 August 2026, when the EU's high-risk AI rules were due to bite. By October that date had moved, Colorado had rewritten its AI law before it ever took effect, India had brought deepfakes under platform rules with a three-hour takedown clock, and California had signed more than two dozen new AI laws.

This edition is written for the people who have to turn that churn into a plan: CISOs, CIOs, risk and compliance leads, product owners and boards. It is organised the way questions arrive in practice. First, which laws apply to the kind of AI you build or use. Second, what is actually enforceable today versus what is still on paper. Third, which single set of controls gets you furthest across all of them.

Everything here reflects publicly reported developments up to mid-October 2026. Laws in this area change quickly, so treat dates as a guide and confirm the current position before acting.

How to use this ebook

01

Find your use case

Sections 3 and 4 group laws by what the AI does: hiring, lending, chatbots, synthetic media, frontier models.

02

Check the clock

Section 6 is a single compliance calendar from today to 2029, with every date that moved this year.

03

Build once

Sections 7 and 8 map one control set across major laws and turn it into a 90-day plan.

WHO WE ARE



Want this mapped to your AI estate?

SecComply helps organisations across the United States, Europe, the Middle East and India assess AI risk, design governance that auditors recognise, and secure the AI they build and buy. Write to us and a specialist will set up a short readiness call.

✉ info@seccomply.net

📄 seccomply.net

Contents

00	The short version	04
	2026 in numbers	05
	Where the world stands	06
01	The 2026 reset: delay is not deregulation	07
	The United States: federal pressure, state persistence	08
02	Comprehensive AI laws	09
	EU AI Act after the Omnibus	09
	Asia-Pacific: Korea, Vietnam, Taiwan, Kazakhstan, Japan, China	11
	The Americas: Colorado, Texas, Brazil	12
	Side by side: horizontal laws compared	13
03	Rules by use case	14
	Employment and HR technology	14
	Financial services and insurance	15
	Chatbots, companions and AI disclosure	16
	Deepfakes, labelling and content provenance	17
	Frontier and general-purpose models	18
	Algorithmic pricing and the rise of AI assurance	19
04	India spotlight	20
	Synthetic content under the IT Rules	21
	Where the DPDP Act meets AI	22
05	International cooperation and standards	23
06	Compliance calendar 2026 to 2029	24
07	One control set, many laws	25
08	Your 90-day plan and maturity model	26
	Ten questions boards should ask, and our outlook for 2027	27
09	How SecComply can help	28
	Sources, further reading and disclaimer	29

The short version

Ten things a busy leader should take away from 2026.

1

Deadlines moved, obligations did not disappear

The EU pushed its high-risk rules back to December 2027 and August 2028, Colorado reset to January 2027, and Korea paused fines for a year. In every case the substance of what must be done survived. Use the extra time to build, not to wait.

2

Transparency is the first duty to bite

Chatbot disclosure, deepfake labelling and machine-readable marking of synthetic content are live or imminent in the EU, India, China, Korea, Vietnam and several US states. If your product talks to people or creates media, this is your current exposure.

3

Horizontal laws now exist on three continents

The EU, South Korea and Vietnam all have comprehensive AI statutes in force. Taiwan and Kazakhstan have passed their own. Brazil's bill remains stuck in its lower house.

4

The US is a state-by-state map, for now

A December 2025 executive order and a March 2026 White House framework push for federal preemption, but Congress has not acted. State laws stay in force as written until a court, Congress or the state itself says otherwise.

5

Employment AI is the most regulated use case

Bias audits, notices, human review before adverse action and limits on emotion inference keep recurring. California's "No Robo Bosses" law and Illinois' civil rights amendment add to New York City's audit regime.

6

Frontier model rules are converging on one template

California and New York now share a compute threshold, a published safety framework and fast incident reporting. EU general-purpose AI obligations have applied since August 2025.

7

India regulates AI through existing law

No standalone AI Act, but the IT Rules now cover synthetic media with two to three hour takedown windows, and the DPDP Act's main obligations land in May 2027 with direct consequences for training data and automated decisions.

8

Assurance is becoming a market

California created a framework for independent AI verification and a registry for AI auditors, and ISO/IEC 42001 certification is becoming a common buyer request.

9

One control set covers most of the ground

Inventory, risk classification, impact assessment, notice, human oversight, logging, testing and incident response appear in nearly every regime. Build them once, map them many times.

10

Start with what you cannot see

Most organisations cannot list every AI system, model and agent they run, including those inside SaaS tools. An inventory is the cheapest and most valuable first step.

2026 in numbers

The figures that defined the year, and why each one matters for your programme.

16

months added to the EU deadline for stand-alone high-risk AI, now 2 December 2027.

3 hrs

for Indian intermediaries to act on a court order or government notice about unlawful content, down from 36.

10²⁶

operations: the training compute line used by California, New York and Korea to flag the most capable models.

2 Dec

2026: end of the EU grace period for watermarking content from generative systems already on the market.

20+

AI-related bills signed in California in 2026, spanning workplaces, healthcare, provenance and audits.

₹250 cr

top penalty under India's DPDP Act, for failing to protect personal data. Core duties apply from 13 May 2027.

€35m

or 7% of global turnover: the top EU AI Act fine for prohibited practices, in force since August 2025.

1 yr

Korea's minimum grace period before AI Basic Act fines, starting from 22 January 2026.

What changed since January 2026

Development	When	Why it matters
Korea's AI Basic Act takes effect	22 Jan 2026	Second comprehensive AI law in force worldwide, with reach to foreign providers.
India notifies synthetic content rules	In force 20 Feb 2026	Mandatory labelling and sharply shorter takedown windows for platforms.
Vietnam's AI law in force	1 Mar 2026	Risk tiers, conformity checks for high-risk systems, machine-readable labels.
White House legislative framework	20 Mar 2026	Asks Congress to preempt "unduly burdensome" state AI laws.
New York RAISE Act finalised	27 Mar 2026	Frontier developer duties from 1 January 2027, aligned with California.
Colorado repeals and replaces its AI Act	14 May 2026	Narrower, notice-based rules from 1 January 2027.
EU AI Omnibus enters into force	27 Jul 2026	High-risk deadlines deferred, two new prohibitions added.
EU transparency duties apply	2 Aug 2026	Chatbot, deepfake and emotion recognition disclosures become enforceable.
California's 2026 AI package signed	Sep 2026	Auditor registry, workplace AI limits, companion chatbot safeguards.

Where the world stands

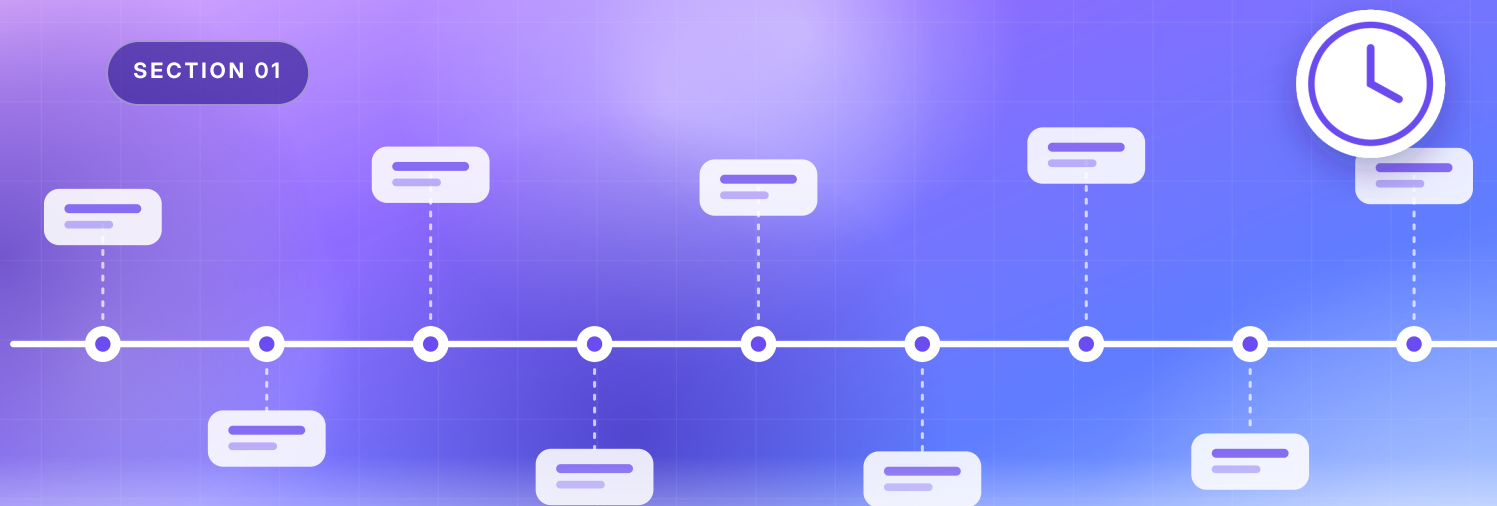
A status board, not a map. What matters for planning is not where a law was proposed but whether it can be enforced against you today.

In force now Obligations apply today	Enacted, duties ahead Law passed, compliance date pending	In the legislature Bills, drafts and stalled texts	Guidance-led Principles, plans and supervisors
EU EU AI Act Bans, AI literacy, GPAI duties and transparency rules KR South Korea AI Basic Act since 22 Jan 2026; fines paused for at least a year VN Vietnam AI Law since 1 Mar 2026, with grace for existing systems IT Italy National AI law (Law 132/2025) since Oct 2025 CN China AI content labelling rules and an AI clause in the Cybersecurity Law IN India IT Rules on synthetic content since 20 Feb 2026 US US states CA SB 53 and SB 243, TX TRAIGA, IL HB 3773, NYC LL 144	EU EU high-risk rules Annex III Dec 2027; product-embedded Aug 2028 CO Colorado SB 26-189 from 1 Jan 2027, subject to litigation NY New York RAISE Act for frontier developers from 1 Jan 2027 CA California No Robo Bosses Act Jul 2027; AI verification framework Jan 2027 IN India DPDP Core data duties from 13 May 2027 TW Taiwan AI Basic Act passed Dec 2025; rules to follow KZ Kazakhstan First AI law signed Nov 2025	BR Brazil PL 2338/2023 passed the Senate in Dec 2024; awaiting a committee opinion in the Chamber US US Congress Preemption proposals stalled; no federal AI statute UK United Kingdom No government AI bill; a private member's bill on superintelligence IN India Draft second amendment to the IT Rules awaiting finalisation US Other states Hundreds of AI bills introduced each year, few enacted	IN India AI Governance Guidelines (Nov 2025); RBI and SEBI expectations JP Japan AI Promotion Act and a national AI Basic Plan, without penalties SG Singapore Frameworks and proposed MAS guidelines for financial institutions UK United Kingdom Sector regulators, plus FCA AI Live Testing AS ASEAN Regional guide on AI governance, expanded for generative AI



Reading the board

A jurisdiction can appear in more than one column. India, for instance, has binding platform rules, data protection duties on the way and principle-based guidance for everything else. Map your exposure by obligation, not by country.



The 2026 reset: delay is not deregulation

2026 was the year regulators blinked on dates and held firm on substance. Four moves explain most of the headlines.

EU: more time for high-risk only

The AI Omnibus, published as Regulation (EU) 2026/1744 and in force from 27 July 2026, moved the stand-alone high-risk deadline from August 2026 to 2 December 2027 and the product-embedded deadline to 2 August 2028. Transparency rules for chatbots and deepfakes still applied on 2 August 2026, and two new bans were added.

Colorado: rewritten before it began

After a constitutional challenge and a federal court stay in April 2026, Colorado repealed its 2024 AI Act and replaced it with SB 26-189, signed on 14 May 2026. The new law is narrower and notice-based, and starts on 1 January 2027.

Korea: law live, fines later

Korea's AI Basic Act took effect on 22 January 2026. The science ministry committed to at least a year before administrative fines, but its investigation powers and the duties themselves applied from day one.

United States: preemption by pressure

Executive Order 14365 created a federal task force to challenge state AI laws, and a March 2026 White House framework asked Congress to preempt them. Congress has not passed a preemption statute, so state laws continue to apply.



What a "delay" really buys you

None of these moves removed the core expectations: know your AI systems, assess the risk they pose, tell people when AI is involved, keep humans able to intervene, and keep records. A deferral gives you time to build those capabilities properly. It does not change what auditors, customers and regulators will eventually ask to see.

The United States: federal pressure, state persistence

How the federal push unfolded

-  **JULY 2025**
 The Senate votes 99 to 1 to strip a ten-year moratorium on state AI laws from the budget reconciliation bill.
-  **11 DECEMBER 2025**
 Executive Order 14365 sets a national AI policy direction and orders action against state laws seen as burdensome.
-  **9 JANUARY 2026**
 The Department of Justice stands up an AI Litigation Task Force to challenge state AI laws in court.
-  **20 MARCH 2026**
 The White House publishes a National Policy Framework for AI asking Congress to preempt state laws, with carve-outs for child safety, fraud, consumer protection and states' own use of AI.
-  **APRIL 2026**
 A federal court stays enforcement of Colorado's original AI Act pending a constitutional challenge.
-  **SUMMER 2026**
 Preemption drafts circulate in Congress; more than 200 state lawmakers and labour groups publicly oppose them.
-  **OCTOBER 2026**
 No federal preemption statute has passed. Midterm elections narrow the legislative window further.

Meanwhile, the states kept legislating



California VERY ACTIVE

Frontier transparency (SB 53) and companion chatbot rules (SB 243) apply from January 2026. A further package signed in September 2026 covers AI audits, workplaces, healthcare and provenance.



New York ENACTED

RAISE Act for frontier developers from January 2027, alongside rules for AI companions and algorithmic pricing disclosure.



Texas IN FORCE

The Responsible AI Governance Act (TRAIGA) took effect on 1 January 2026, banning certain harmful uses and creating a regulatory sandbox.



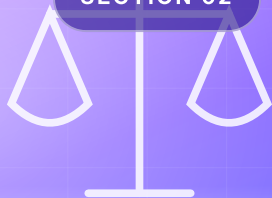
Illinois IN FORCE

Human Rights Act amendment treats discriminatory AI in employment as a civil rights violation from 1 January 2026.



Practical stance for 2027

Plan to comply with state laws as written. Build controls that satisfy the strictest state you operate in, track the Colorado litigation, and keep federal developments on a watch list rather than in your compliance baseline.



Comprehensive AI laws

Horizontal laws regulate AI across sectors by sorting systems into risk tiers. The EU AI Act remains the reference point, and most newer statutes borrow its vocabulary even when they soften its demands.

The EU AI Act after the Omnibus

The Act entered into force on 1 August 2024 and applies in stages. The AI Omnibus changed several of those stages in July 2026. Green marks what already applies; violet marks what is still ahead.



Who carries the load

Providers that develop or place AI on the EU market hold most obligations. **Deployers** that use high-risk AI must follow instructions, assign human oversight, keep logs and, in some cases, assess impact on fundamental rights.

Reach beyond Europe

The Act applies to non-EU companies whose AI systems, or their outputs, are used in the EU. An Indian SaaS firm with EU customers can be in scope.

Penalties

Up to €35m or 7% of global turnover for prohibited practices, and up to €15m or 3% for most other breaches, with lower caps for SMEs.

What the Omnibus actually changed

Topic	Original AI Act	After the Omnibus (in force 27 July 2026)
Stand-alone high-risk (Annex III)	2 August 2026	2 December 2027: hiring, education, credit, essential services, law enforcement and similar uses
High-risk in regulated products (Annex I)	2 August 2027	2 August 2028: for example medical devices, machinery and toys with AI components
Transparency (Article 50)	2 August 2026	Unchanged for chatbot, deepfake and emotion recognition disclosure. Machine-readable marking gets a grace period to 2 December 2026, only for systems already on the market
Prohibited practices	Eight banned categories	Two additions from 2 December 2026: systems built to create non-consensual intimate imagery, and systems generating child sexual abuse material
AI literacy	Ensure a sufficient level of literacy among staff	Softened to supporting the development of literacy, with the Commission and Member States expected to help
Bias testing data	Legal uncertainty under GDPR	Express permission to process special category data where needed to detect and correct bias in high-risk systems
Smaller companies	Simplifications for SMEs	Simplifications extended to small mid-cap companies
Supervision	Mostly national authorities	EU AI Office gains a stronger role over AI built on general-purpose models and AI inside very large online platforms

The high-risk toolkit, in plain terms

When the high-risk rules apply, a provider will need to show eight capabilities. Deployers will rely on these to meet their own duties, so expect them to appear in procurement questionnaires well before 2027.

ART. 9

Risk management

A living process to find, assess and reduce risks across the system's life.

ART. 10

Data governance

Training, validation and test data that is relevant, representative and checked for bias.

ART. 11

Technical file

Documentation detailed enough for an authority to assess compliance.

ART. 12

Logging

Automatic event records that allow outcomes to be traced.

ART. 13

Instructions for use

Clear information on capabilities, limits and intended purpose.

ART. 14

Human oversight

Design that lets trained people understand, override or stop the system.

ART. 15

Accuracy and security

Declared performance, resilience to errors and protection against attacks.

ART. 17 & 72

Quality and monitoring

A quality management system and post-market monitoring of real-world performance.



Italy: the first national AI law in the EU

IN FORCE

Law 132/2025 took effect on 10 October 2025. It names AgID and the cybersecurity agency ACN as AI authorities, sets sector rules for healthcare, employment and public administration, adds AI-related offences and requires parental consent for children under 14. National regulators like these will enforce most of the Act.

Asia-Pacific: from promotion to obligation

Asian lawmakers have mostly paired AI rules with industrial policy: funding, sandboxes and national AI bodies sit alongside duties on transparency and high-impact systems.



South Korea: AI Basic Act IN FORCE 22 JAN 2026

Korea's framework act covers "high-impact" AI in sectors such as energy, drinking water, healthcare and medical devices, nuclear materials, biometrics, hiring, loan screening, transport and public services, plus generative AI and very large models trained above 10^{26} operations. Operators must tell users when they face AI or AI-generated output, label realistic synthetic content, run risk management for high-impact systems, explain outputs where feasible and keep safety documentation. Foreign providers above set revenue or user thresholds must appoint a domestic representative.

Penalties: administrative fines up to KRW 30 million. The ministry has committed to at least one year before fines are imposed, but investigation powers apply now.



Vietnam: Law on Artificial Intelligence IN FORCE 1 MAR 2026

Passed in December 2025, the law sorts systems into high, medium and low risk. High-risk systems on a government list face conformity certification, impact assessments, transparency about data and logic, human override and incident reporting. AI-generated audio, images and video must carry machine-readable labels. Existing systems have until 1 March 2027 to comply, or 1 September 2027 in health, education and finance. Implementing decrees are being issued in phases.



Taiwan PASSED DEC 2025

The AI Basic Act, passed on 23 December 2025, sets principles on privacy, safety, fairness, transparency and accountability, adopts risk classification, and asks ministries to issue implementing rules and promote AI literacy.



Kazakhstan SIGNED NOV 2025

The country's first AI law introduces risk classification and an autonomy scale, places responsibility on developers, and bans manipulative practices and exploitation of vulnerable groups.



Japan PROMOTION-FIRST

The 2025 AI Promotion Act sets up a national AI strategy headquarters and a basic plan rather than penalties. The government relies on guidance, voluntary cooperation and the power to publicise misuse.



China IN FORCE

Measures requiring visible and embedded labels on AI-generated content apply from 1 September 2025. Amendments to the Cybersecurity Law, effective 1 January 2026, add AI governance, ethics and risk assessment to the statute for the first time.



The common thread in Asia

Labelling of synthetic content is the one obligation that appears in Korea, Vietnam, China and India alike. If you build or embed generative AI for Asian markets, a single provenance and labelling capability, with visible labels and machine-readable metadata, will serve all four.

The Americas: narrower laws, longer runways



Colorado SB 26-189

FROM 1 JAN 2027

REPLACES SB 24-205

Colorado's 2024 law would have imposed EU-style governance duties on developers and deployers of high-risk AI. It never took effect. Its start date slipped from February to June 2026, a federal court stayed enforcement in April 2026, and on 14 May 2026 the governor signed SB 26-189 to repeal and replace it.

The new law targets **automated decision-making technology that processes personal data and materially influences consequential decisions** in areas such as employment, housing, lending, insurance, healthcare, education and essential government services. Instead of a full governance programme, deployers owe consumers targeted disclosure, an explanation of adverse outcomes, a chance to correct data and a way to request human review, and must keep records for three years. There is no private right of action, the Attorney General must offer a 60-day cure period, and financial institutions are now in scope, with exemptions for anti-money laundering, sanctions, fraud and identity checks.

Watch: challenges to the new law are expected, and Attorney General rulemaking must be finished by the start date.



Texas TRAIGA

IN FORCE 1 JAN 2026

The Texas Responsible AI Governance Act prohibits developing or deploying AI with intent to manipulate people into self-harm or crime, to unlawfully discriminate, or to produce child sexual abuse material and certain deepfakes. Government agencies must disclose AI use to the public. The Attorney General enforces with a cure period, and a state sandbox lets companies test AI under relaxed rules.



Brazil PL 2338/2023

PENDING

The Senate approved Brazil's EU-style AI bill in December 2024. It reached the Chamber of Deputies in March 2025, where a special committee was formed but had not issued its opinion as of September 2026. With the October 2026 general election, passage before 2027 looks unlikely. If enacted in its Senate form, it would ban excessive-risk systems, impose impact assessments and governance duties for high-risk uses and allow fines up to R\$50 million or 2% of revenue. Until then, Brazil's data protection and consumer laws already apply to AI.



The design lesson from Colorado

Colorado's journey shows where legislators land after pushback: away from abstract "reasonable care" duties and towards concrete consumer rights at the moment of decision, namely notice, explanation, correction and human review. Building those four rights into any AI-assisted decision process is a sound bet in every market.

Horizontal laws side by side

Same goal, different levers. The table compares the status and design of the main horizontal AI laws as of October 2026.

Law	Status	Model	Bans	Key dates	Top penalty
EU AI Act	IN FORCE phased	Four tiers: prohibited, high-risk, transparency, minimal	Yes, 10 categories from Dec 2026	High-risk Dec 2027 and Aug 2028	€35m or 7% of turnover
Korea AI Basic Act	IN FORCE	High-impact and generative AI duties	No	Fines no earlier than 2027	KRW 30m
Vietnam AI Law	IN FORCE	High, medium, low risk	Restrictions by decree	Existing systems Mar or Sep 2027	Set by decree
Italy Law 132/2025	IN FORCE	National layer on the EU Act	Via EU Act	Since Oct 2025	EU Act plus new offences
Colorado SB 26-189	ENACTED	Consumer rights on automated decisions	No	1 Jan 2027	Attorney General enforcement; no private right of action
Texas TRAIGA	IN FORCE	Intent-based prohibitions	Yes, narrow	Since 1 Jan 2026	Civil penalties, higher for uncured breaches
Taiwan AI Basic Act	ENACTED	Principles plus risk classes	To be set	Implementing rules pending	To be set
Brazil PL 2338	BILL	EU-style tiers	Yes	None until enacted	R\$50m or 2% of revenue
Japan AI Promotion Act	IN FORCE	Promotion and guidance	No	Basic plan adopted	None; public naming

Where they converge



Same hot spots

Employment, credit, insurance, education, healthcare and essential services appear on almost every high-risk list.



Same first duty

Telling people they are dealing with AI is the most common obligation and usually the first to apply.



Same evidence

Risk assessments, technical documentation and logs are what every regulator asks to see.

Employment and HR technology

Hiring and workforce tools were among the first AI uses to attract specific laws, and they remain the most heavily regulated. Rules now reach beyond hiring to discipline, dismissal, monitoring and layoffs.



New York City Local Law 144

SINCE JUL 2023

Annual independent bias audits of automated employment decision tools, a public summary of results and advance notice to candidates.



California SB 947, "No Robo Bosses"

NEW · JUL 2027

Human review and corroboration before discipline or termination driven mainly by an automated system, plus notice and data access rights for workers.



Illinois HB 3773

SINCE JAN 2026

Discriminatory use of AI in employment decisions is a civil rights violation, using zip codes as a proxy for protected traits is barred, and employers must give notice of AI use.



California AB 1883 and SB 951

NEW

Workplace surveillance tools may not infer emotions or collect neural data, and mass layoff notices must disclose when AI or automation is the cause.



California anti-discrimination rules

SINCE OCT 2025

Employment regulations explicitly cover automated decision systems; evidence of anti-bias testing can support an employer's defence.



EU and Korea

HIGH-RISK

Recruitment and worker management are high-risk under the EU Act from December 2027; emotion recognition at work has been banned since February 2025. Hiring is high-impact in Korea.



Five duties that keep recurring in HR AI laws

Notify candidates and staff before AI is used. **Test** for disparate impact at least yearly. **Review** adverse outcomes with a human. **Record** inputs, outputs and decisions. **Offer** a route to appeal or an alternative process. Bills in New York, New Jersey, Massachusetts and other states follow the same pattern.

Financial services and insurance

Banks, lenders and insurers already answer to model risk, fair lending, conduct and consumer protection rules that apply whether or not AI is involved. Supervisors have therefore leaned on guidance and testing environments, while legislators target specific harms such as automated claim denials.

Supervisory expectations

- **EU:** AI for creditworthiness and for life and health insurance pricing is high-risk from December 2027. The European Parliament has asked the Commission for guidance on how existing financial law applies to AI.
- **United Kingdom:** the FCA's AI Live Testing service gives firms regulatory and technical support while they deploy AI; its first cohort started in October 2025.
- **Singapore:** MAS consulted in late 2025 on guidelines asking financial institutions to inventory AI, rate its risk and apply lifecycle controls with board oversight.
- **India:** the RBI's FREE-AI framework (August 2025) sets principles and recommendations for regulated entities, and SEBI rules make regulated firms answerable for the AI tools they use.
- **Colorado:** SB 26-189 brings lending and insurance decisions into scope from 2027, with carve-outs for fraud and AML tools.

Insurance-specific rules



US model bulletin

The national insurance commissioners' bulletin, adopted by many states, expects a written AI governance programme and reminds insurers that unfair discrimination rules apply to algorithms.



Colorado insurance rules

Life, auto and health insurers must govern their use of external consumer data and predictive models, under regulations made under a 2021 law.



Health claim decisions

Texas bars automated systems from making adverse healthcare determinations, and similar bills in other states require a qualified human to decide denials.



For regulated entities in India

Expect AI questions in RBI and SEBI inspections to follow the same lines as supervisors elsewhere: a board-approved AI policy, an inventory, model validation, explainability for customer-facing decisions, vendor accountability and incident reporting. Building to that list now will also cover most of what Colorado and the EU will ask of global lenders.

Chatbots, companions and AI disclosure

If a person can mistake your AI for a human, or its output for something real, a disclosure duty probably applies somewhere you operate. The EU's four transparency duties are the most complete set and became enforceable on 2 August 2026.

50(1)

PROVIDERS

Design systems that interact with people so users know they are dealing with AI, unless it is obvious.

Applies since 2 Aug 2026

50(2)

PROVIDERS

Mark synthetic audio, images, video and text in a machine-readable, detectable way.

Legacy systems: 2 Dec 2026

50(3)

DEPLOYERS

Inform people exposed to emotion recognition or biometric categorisation.

Applies since 2 Aug 2026

50(4)

DEPLOYERS

Disclose deepfakes, and AI-written text published to inform the public on matters of public interest.

Applies since 2 Aug 2026

Companion and mental health chatbots in the US



California SB 243 SINCE JAN 2026

Companion chatbot operators must disclose that users face AI, remind known minors every three hours, maintain and publish self-harm protocols that refer users to crisis services, and report referral data annually from July 2027. A further child-safety bill, SB 1119, was signed in 2026.



New York AI companion law SINCE NOV 2025

Operators must detect expressions of self-harm, point users to crisis support and remind users at the start of a session and every three hours that they are not talking to a person.



Utah HB 452 SINCE MAY 2025

Mental health chatbots must disclose they are not human, may not sell health data or use it for targeted ads without consent, and gain a defence if they keep documented safety policies.



Maine and others IN FORCE

Maine bars businesses from leading consumers to believe a chatbot is human. California's AB 1979 brings certain healthcare chatbot providers under medical confidentiality rules.



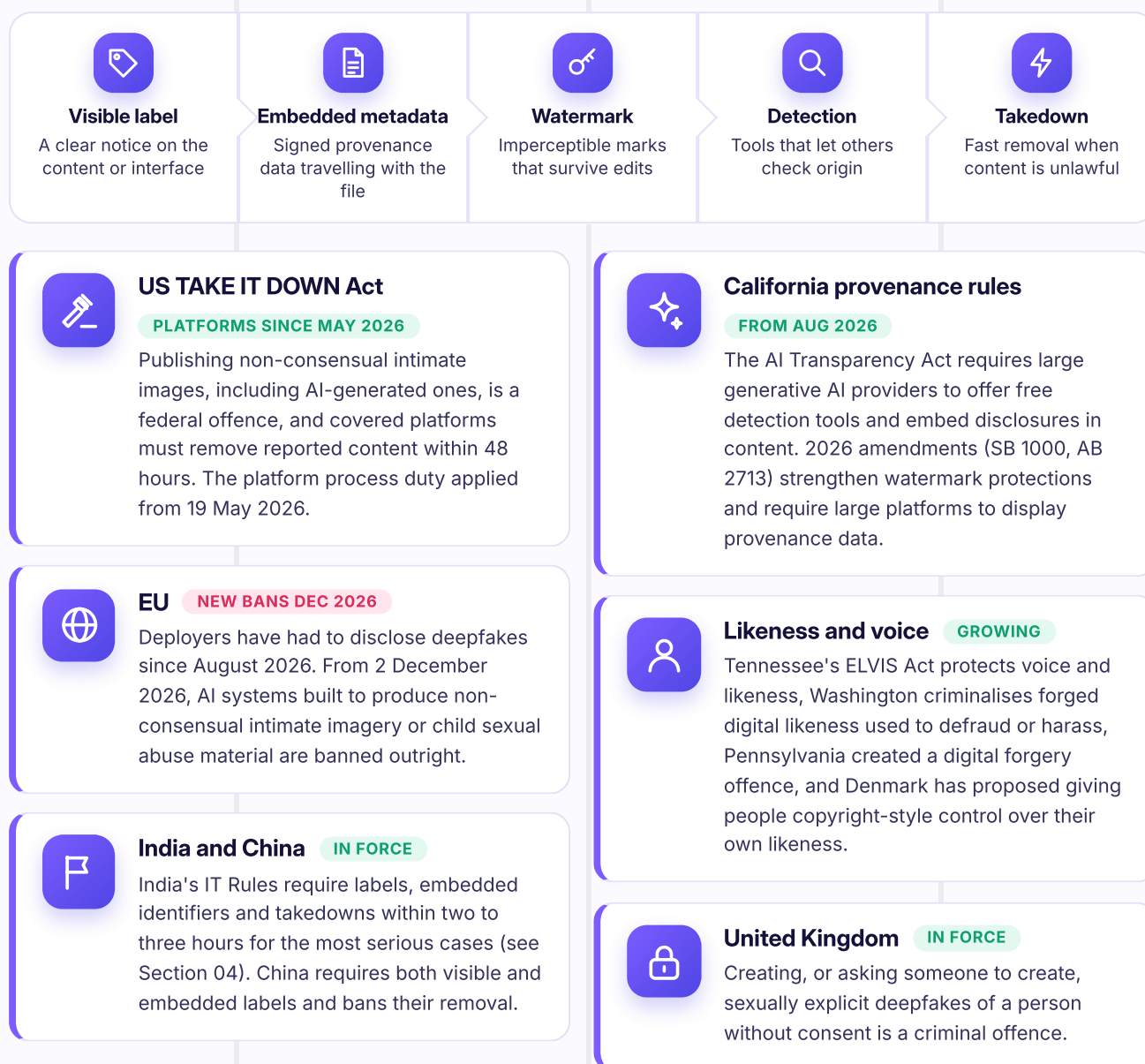
A disclosure pattern that travels

Show an AI notice before the first message, repeat it at intervals in long sessions, answer truthfully when asked "am I talking to a bot?", and route any self-harm signal to a human or crisis resource. That covers the core of the EU, Korean, Californian and New York rules.

Deepfakes, labelling and content provenance

Laws on synthetic media now attack the problem from two ends: criminal and takedown rules for harmful content, and labelling rules that make all synthetic content identifiable.

The provenance stack regulators are converging on



The fraud angle for CISOs

The fastest-growing deepfake harm for businesses is impersonation: cloned executive voices and video used to authorise payments. Out-of-band verification for payment and credential changes, and staff awareness, matter as much as any labelling obligation.

Frontier and general-purpose models

Only a handful of companies train the largest models, but their obligations shape the documentation, safety reports and incident data that flow down to every business that builds on them.

	California SB 53	New York RAISE Act	EU GPAI rules	Korea AI Basic Act
Status	SINCE 1 JAN 2026	FROM 1 JAN 2027	SINCE 2 AUG 2025	SINCE 22 JAN 2026
Who	Frontier developers; heavier duties above \$500m revenue	Frontier developers; heavier duties above \$500m revenue	All GPAI providers; extra duties for systemic-risk models	Developers of high-performance AI
Compute line	Above 10^{26} operations	Above 10^{26} operations	Systemic risk presumed above 10^{25} FLOPs	10^{26} FLOPs or more
Core duties	Publish a frontier AI framework and transparency reports; whistleblower protections	Publish a framework, transparency reports, quarterly risk summaries to a new state office	Technical documentation, copyright policy, training data summary; evaluations and security for systemic-risk models	Identify, assess and mitigate risks; monitor and respond to safety incidents
Incidents	Report critical safety incidents within 15 days, 24 hours if imminent harm	Report within 72 hours, 24 hours to authorities if imminent harm	Report serious incidents to the AI Office	Report results to the science ministry
Penalty	Up to \$1m per violation	Up to \$1m first, \$3m later	Up to €15m or 3% of turnover	Up to KRW 30m

🕒 EU timing to note

The Commission's power to enforce GPAI obligations began on 2 August 2026. Models placed on the market before August 2025 must comply by 2 August 2027. Signing the voluntary Code of Practice is the main route to showing compliance.

🏢 If you build on these models

Ask your model providers for their published safety frameworks, model cards and EU documentation. These are now legal deliverables, and they are the evidence you need for your own risk assessments and customer questionnaires.



One template, three jurisdictions

California wrote the template, New York amended its law in March 2026 to align with it, and Korea uses the same compute line. Expect other US states to copy the same structure rather than invent new ones.

Algorithmic pricing and the rise of AI assurance

Pricing algorithms under scrutiny

US lawmakers increasingly treat pricing software as a competition and fairness issue. New York requires businesses to tell consumers when a price was set by an algorithm using their personal data, and separately restricts rent-setting software that pools data from competing landlords. California's AB 325 extends its antitrust law to shared pricing algorithms that use competitor data, including for wages. Bills on "surveillance pricing" in groceries, retail and ticketing are moving in several other states.

From self-declaration to independent checks

The bigger story of 2026 is assurance. Buyers, insurers and regulators increasingly want evidence that has been checked by someone independent, and new laws are building the infrastructure for it.





India: governing AI through the laws it already has

India has chosen not to pass a standalone AI Act. The AI Governance Guidelines released by MeitY in November 2025 say so plainly: use existing legislation wherever possible, add targeted rules where harm is visible, and rely on voluntary measures and techno-legal tools for the rest. For businesses, that means AI obligations arrive through four layers that are easy to miss if you only search for "AI law".

Data protection

DPDP Act 2023 and Rules 2025

Consent, notice, purpose limits, children's data, breach reporting and extra duties for significant data fiduciaries, including checks on algorithmic software.

CORE DUTIES MAY 2027

Platforms and content

IT Act and IT Rules 2021, as amended

Labelling of synthetic media, user declarations, embedded identifiers and two to three hour takedown windows.

IN FORCE FEB 2026

Sector supervisors

RBI, SEBI, CERT-In, IRDAI and others

Expectations on AI governance, accountability for vendor tools, model risk and cyber incident reporting.

GUIDANCE AND RULES

National guidance

India AI Governance Guidelines, Nov 2025

Seven principles, six pillars and an action plan, designed as a reference rather than a binding code.

VOLUNTARY

7

principles ("sutras") in the national guidelines, including trust, people first, fairness, accountability and understandable-by-design.

50 lakh

registered users: the line above which social media platforms face the strictest synthetic content duties.

13 May 2027

the date most DPDP obligations apply to every business processing digital personal data.

Synthetic content under the IT Rules

MeitY notified amendments to the IT Rules on 10 February 2026, and they took effect ten days later on 20 February. For the first time, Indian law defines "synthetically generated information" and attaches specific duties to it.

What counts

Audio, visual or audio-visual content created or altered by a computer so that it looks real and could be taken for a real person or event. Routine edits, accessibility improvements and good-faith document work are excluded, and plain AI-generated text is outside this definition, although existing rules on unlawful content still apply to it.

What platforms must do

- **Prevent:** services that let users create synthetic media must take reasonable technical steps to block unlawful outputs, such as child sexual abuse material, non-consensual intimate imagery, forged documents and deceptive depictions of real people.
- **Label:** lawful synthetic content must carry a prominent visual or audio label and, where feasible, permanent metadata or identifiers that users cannot strip.
- **Verify:** large social media platforms must ask users to declare synthetic uploads and use technical tools to check those declarations.
- **Remind:** users must be told every three months, rather than once a year, about the consequences of breaking platform rules.

The new takedown clock

Court order or government notice

Before: 36 hours

Now: 3 hours

Intimate imagery, impersonation, morphed images

Before: 24 hours

Now: 2 hours

Complaints about content concerning an individual

Before: 72 hours

Now: 36 hours

General user grievances

Before: 15 days

Now: 7 days

Bars are scaled within each row to show the relative cut.

What is at stake

Platforms that knowingly allow unlabelled or unlawful synthetic content, or miss these deadlines, risk losing safe harbour protection for third-party content under Section 79 of the IT Act.



Next: a second amendment DRAFT

Draft rules published in March 2026 and revised in April would make compliance with MeitY advisories part of platforms' due diligence, tying them to safe harbour. Consultation closed in May 2026 and the final text is awaited.



Not only for social media

"Intermediary" is broad in Indian law. SaaS products, marketplaces, hosting providers and AI apps that let users generate images, voice or video should check whether they fall within these duties, and test whether they could meet a two-hour takedown at 2 a.m.

Where the DPDP Act meets AI

The Digital Personal Data Protection Rules were notified on 13 November 2025 and phase in over 18 months. The government has signalled it may shorten that runway, so plan for the earlier end of the range.



Six places the DPDP Act touches your AI

1 · Training data

Personal data used to train or fine-tune models needs a lawful basis, usually consent given for a specific purpose. Reusing customer data for model training is a new purpose.

2 · Notices

Notices must say in plain language what data is collected and why. Vague references to "improving our services" will not cover AI training or profiling.

3 · Children

Processing data of anyone under 18 needs verifiable parental consent, and tracking, behavioural monitoring and targeted advertising aimed at children are barred.

4 · Algorithmic due diligence

Significant data fiduciaries must check that the algorithmic software they deploy does not put data principals' rights at risk, alongside an annual impact assessment and audit.

5 · Breaches

Personal data breaches go to the Board and affected people without delay, with a detailed report to the Board within 72 hours. Leaks through AI tools count.

6 · Rights and erasure

People can ask to access, correct and erase their data. Plan how you will honour erasure when data sits inside embeddings, logs or fine-tuned models.

Sector supervisors to watch

Body	What it has said about AI
RBI	FREE-AI framework (August 2025): principles and recommendations on governance, model risk, consumer protection and AI incident reporting for regulated entities.
SEBI	Regulated entities are fully responsible for AI tools they build or buy, including outputs and data privacy; further guidance on AI in trading has been signalled.
CERT-In	An April 2026 advisory on AI-driven cyber threats and a May 2026 blueprint for reducing exposure to AI-assisted exploitation, on top of the six-hour incident reporting rule.
Supreme Court	Draft rules (June 2026) on AI use in courts keep AI assistive, subject to human judgment, and rule out AI-based sentencing.



Selling from India to the world?

Indian SaaS and IT services firms are often "providers" under the EU AI Act and may need a domestic representative in Korea. Customers in both markets are already sending AI questionnaires. Align DPDP work with ISO/IEC 42001 and EU transparency duties so one evidence pack serves every buyer.



International cooperation and standards

No single treaty governs AI, but a thin international layer is forming, and standards bodies are doing much of the practical work of turning legal principles into auditable controls.

Intergovernmental initiatives



United Nations

A 2025 General Assembly resolution created an Independent International Scientific Panel on AI, with 40 experts reporting on risks and impacts, and a Global Dialogue on AI Governance that meets alongside existing UN events.



Council of Europe

The Framework Convention on AI, open for signature since September 2024, is the first binding international treaty on AI, covering human rights, democracy and the rule of law across the AI lifecycle.



ASEAN, OECD and G7

ASEAN expanded its AI governance guide for generative AI in January 2025. The G7 Hiroshima process now has an OECD-run reporting framework where developers publish how they manage risk.



UNESCO

Guidance on generative AI in education and research, and guidelines for AI in courts and tribunals published in December 2025.

Standards that auditors use

Standard	Use it for
ISO/IEC 42001	A certifiable AI management system: policy, roles, risk, impact assessment, lifecycle controls
ISO/IEC 23894	AI-specific risk management guidance
ISO/IEC 42005	Structuring AI system impact assessments
ISO/IEC 42006	Requirements for bodies certifying AI management systems
NIST AI RMF and GenAI profile	US-style risk framework: Govern, Map, Measure, Manage
EU harmonised standards	Presumption of conformity with the AI Act once published; work is running late, which drove the high-risk delay



Why standards matter more in 2027

With laws diverging on detail, a recognised management system standard is the only artefact most regulators, customers and auditors will accept across borders. ISO/IEC 42001 also sits naturally alongside an existing ISO 27001 programme.

Compliance calendar: 2026 to 2029

Already live: EU AI Act bans, literacy, GPAI and transparency duties · Korea AI Basic Act · Vietnam AI Law · Italy Law 132/2025 · China labelling rules and Cybersecurity Law AI clause · India synthetic content rules · California SB 53 and SB 243 · Texas TRAIGA · Illinois HB 3773 · NYC Local Law 144 · US TAKE IT DOWN Act platform duties.

2026

NOV
2026

INDIA **DPDP consent manager framework** begins, one year after the Rules were notified.

2 DEC
2026

EU **Watermarking grace ends** for generative systems already on the market, and the **two new bans** on intimate imagery and abuse material generators apply.

2027

1 JAN
2027

US **Colorado SB 26-189, New York RAISE Act, California SB 813** verification framework and workplace emotion and neural data limits, plus California's privacy rules on automated decision-making technology.

EARLY
2027

KOREA The committed **one-year pause on fines** under the AI Basic Act runs out; check for any extension.

1 MAR
2027

VIETNAM **Existing AI systems** must comply in most sectors.

13 MAY
2027

INDIA **DPDP core obligations** apply: notice, consent, security, breach reporting, rights and SDF duties.

1 JUL
2027

US **California SB 947** (No Robo Bosses) applies; annual companion chatbot reporting under SB 243 begins.

2 AUG
2027

EU **GPAI models** placed on the market before August 2025 must comply; Member States must have **national sandboxes** running.

1 SEP
2027

VIETNAM Existing systems in **health, education and finance** must comply.

2 DEC
2027

EU **Stand-alone high-risk AI** (Annex III): hiring, education, credit, essential services and more.

2028 and beyond

2 AUG
2028

EU **High-risk AI in regulated products** (Annex I).

1 JAN
2029

US **California AB 1405** AI auditor registry.

Watch list, no date yet

Brazil PL 2338 · US federal preemption · Colorado litigation · India IT Rules second amendment · Taiwan implementing rules · Vietnam decrees · a UK AI bill

One control set, many laws

The fastest way through fragmented regulation is to stop treating each law as a project. Build one set of controls, then map it. The matrix shows how eleven core controls line up with major laws and frameworks.

Control	EU AI Act	Korea AI Basic Act	Colorado SB 26-189	NYC LL 144	India DPDP and IT Rules	ISO/IEC 42001	NIST AI RMF
AI inventory and classification Know every system, model and agent	●	●	○	○	○	●	●
Risk management process Identify, assess, treat, review	●	●	○		○	●	●
Impact and bias assessment Effects on people and groups	●	○	○	●	●	●	●
Data governance Lawful, relevant, quality data	●	○	○	○	●	●	●
Transparency and notice Tell people when AI is involved	●	●	●	●	●	○	○
Human oversight and review Ability to intervene and appeal	●	●	●	○	○	○	●
Logging and record retention Trace decisions after the fact	●	○	●	○	●	●	○
Testing for accuracy and security Evaluation, red teaming, robustness	●	○			○	●	●
Incident reporting Detect, escalate, notify	●	○			●	○	○
Third-party oversight Vendors, models and APIs	●	○	○	○	●	●	●
AI literacy and training People who understand the tools	○	○			○	●	●

● Explicit requirement or core expectation ○ Supports or is needed indirectly · Not a focus

Indicative mapping for planning. Scope and exact duties depend on your role, sector and the systems involved.

Your 90-day plan

Most of the value comes from the first three months. This plan assumes an existing security or privacy programme you can build on.

Days 1 to 30

See what you have

- Name an accountable executive and a working group across security, legal, data and product.
- Build an AI inventory: in-house models, embedded vendor AI, copilots, agents and shadow tools.
- Record for each system its purpose, data, users, markets and the decisions it influences.
- Approve an interim acceptable-use policy for generative AI.

Days 31 to 60

Classify and prioritise

- Map each system against the laws that reach it, using the calendar in Section 06.
- Flag high-risk and consequential-decision uses first: hiring, credit, insurance, health, children.
- Run impact and bias assessments on the top five.
- Check that chatbot and synthetic content disclosures are live wherever they are already required.

Days 61 to 90

Build the backbone

- Adopt a management system structure, ideally ISO/IEC 42001, aligned with ISO 27001.
- Add AI clauses to vendor contracts: documentation, incidents, data use, audit rights.
- Extend incident response to AI failures, misuse and deepfake fraud.
- Report status, gaps and budget to the board.

Where are you today?

1

Unaware

No inventory; AI adopted ad hoc by teams.

2

Reactive

Policies exist; reviews happen after issues or customer questions.

3

Defined

Inventory, risk tiers and assessments for key systems.

4

Managed

Controls monitored, vendors governed, metrics reported to the board.

5

Assured

Independent audit or certification; governance built into delivery.

Ten questions boards should ask

- 1 Do we have a complete list of the AI systems, models and agents we build, buy and use, including inside SaaS tools?
- 2 Which of them influence decisions about customers or employees, and in which countries?
- 3 Who is the named executive accountable for AI risk, and how often do they report to us?
- 4 Where are we already subject to live duties, such as EU transparency, India's IT Rules or US state laws?
- 5 How do we test our AI for bias, accuracy and security before and after release?
- 6 Can a customer or employee get an explanation and a human review of an AI-assisted decision?
- 7 What do our contracts require from AI vendors on data use, incidents and documentation?
- 8 Would we detect, and how fast would we respond to, an AI failure or a deepfake fraud attempt?
- 9 What personal data trains or feeds our models, and on what legal basis?
- 10 Could we show an auditor or major customer our AI governance evidence within a week?

Our outlook for 2027

SecComply's view, based on developments up to October 2026.

1 · Transparency enforcement comes first

Early EU and Korean cases are more likely to involve undisclosed chatbots and unlabelled synthetic media than high-risk systems.

2 · Procurement outruns regulation

Large buyers will ask for AI governance evidence, often ISO/IEC 42001, before any regulator does.

3 · US states keep going

Without a federal statute, more states will copy California's frontier template and Colorado's narrower decision rights.

4 · Agents become the new frontier

Autonomous agents acting with real credentials will push identity, access and logging to the top of AI risk agendas.

5 · India stays sector-led

Expect more MeitY advisories, sector rules from RBI and SEBI, and DPDP enforcement shaping AI practice, rather than an AI Act.

6 · Assurance professionalises

Auditor registries, certification bodies and insurance requirements will make independent AI assurance routine for higher-risk uses.



Could you answer all ten today?

If three or more answers are "not yet", a short AI governance readiness review will show where to start. SecComply can help you run one and turn the results into a board-ready roadmap.

✉ info@seccomply.net



How SecComply can help

SecComply is an AI-enabled security, compliance and CISO advisory firm. We help organisations turn the requirements in this ebook into a programme they can run, evidence and defend.



STEP 1

Discover

Map the AI you build, buy and use, including embedded vendor AI and AI agents, and the identities they act through.



STEP 2

Assess

Gap and risk assessments against the EU AI Act, ISO/IEC 42001, NIST AI RMF, DPDP and the US state laws that reach you.



STEP 3

Design

Governance structure, policies, impact assessment templates and a roadmap your teams can implement, with our guidance.



STEP 4

Secure

Test AI applications and model endpoints for issues such as prompt injection and excessive access, alongside VAPT.



STEP 5

Sustain

vCISO and CISO Office as a Service to keep controls, evidence and board reporting current as laws change.

100+

customers, from global enterprises and fast-scaling unicorns to governments

4

regions served: United States, Europe, Middle East and India

1 programme

DPDP, ISO 27001, SOC 2 and ISO/IEC 42001 run on shared controls and evidence

2026

Emerging Tech Start-up of the Year, ETNOW.in Business Conclave & Awards, West Edition



Platform

AI-powered tooling that automates evidence collection and monitors risk, so audit readiness is continuous.



Process

Proven frameworks accelerated by AI agents, with experts keeping approval and accountability.



People

Experienced security and compliance specialists, with leadership that includes a former Fortune 500 CISO.

Start with an AI governance readiness call

Tell us where you operate and what AI you use. We will tell you which rules reach you and what to do first.

✉ info@seccomply.net

Sources and further reading

This ebook was written by SecComply from primary legislative texts, regulator publications and reputable legal commentary available up to mid-October 2026. The main sources are listed below by section.

European Union

Regulation (EU) 2024/1689 (AI Act), Official Journal of the EU
 Regulation (EU) 2026/1744 amending the AI Act ("AI Omnibus"), published 24 July 2026
 European Commission guidelines on AI Act transparency obligations and the General-Purpose AI Code of Practice
 Italy, Law No. 132 of 23 September 2025 on artificial intelligence

United States

Executive Order 14365 (11 December 2025) and the White House National Policy Framework for AI (20 March 2026)
 Colorado SB 24-205, SB 25B-004 and SB 26-189
 California SB 53, SB 243, SB 813, AB 1405, SB 947, SB 951, AB 1883, SB 1000, AB 2713 and AB 325; California Civil Rights Council regulations on automated decision systems
 New York RAISE Act and 2026 chapter amendment; New York City Local Law 144; Illinois HB 3773; Texas HB 149 (TRAIGA); Utah HB 452; Texas SB 815
 TAKE IT DOWN Act (Public Law, May 2025); NIST AI Risk Management Framework and Generative AI Profile

Asia-Pacific

Republic of Korea, Framework Act on the Development of AI and Establishment of Trust, and its Enforcement Decree
 Vietnam, Law on Artificial Intelligence (Law No. 134/2025/QH15)
 Taiwan, Artificial Intelligence Basic Act; Kazakhstan, Law on Artificial Intelligence; Japan, AI Promotion Act

China, Measures for Labelling AI-Generated Synthetic Content; amended Cybersecurity Law (effective 1 January 2026)

India

Digital Personal Data Protection Act 2023 and DPDP Rules 2025 (MeitY, 13 November 2025)
 IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, notified 10 February 2026; draft second amendment (March and April 2026)
 India AI Governance Guidelines (MeitY, November 2025); RBI FREE-AI Committee report (August 2025); SEBI circulars and consultations on AI and ML; CERT-In advisories (2026)

International and standards

UN General Assembly resolution on the Scientific Panel and Global Dialogue on AI Governance (2025); Council of Europe Framework Convention on AI
 ASEAN Guide on AI Governance and Ethics and its generative AI expansion; OECD reporting framework for the G7 Hiroshima Code of Conduct
 ISO/IEC 42001, 23894, 42005 and 42006

Other

Brazil, PL 2338/2023 (Federal Senate and Chamber of Deputies records); UK Financial Conduct Authority, AI Live Testing; Monetary Authority of Singapore consultation on AI risk management (November 2025)

Important notice. This ebook is general information for awareness and planning. It is not legal advice, and it does not create any advisory or client relationship. AI laws and their interpretation change frequently; some measures described here are drafts, bills or subject to litigation, and dates may move. Before acting on anything in this document, confirm the current position with qualified legal counsel in the relevant jurisdiction. SecComply accepts no liability for decisions taken on the basis of this content. All product, company and law names belong to their respective owners. © 2026 SecComply. All rights reserved.



SecComply

Make AI regulation your trust advantage

From AI inventory to ISO/IEC 42001 readiness, AI security testing and DPDP compliance, SecComply is one accountable partner across every layer of security and compliance.



GRC & Compliance

DPDP, ISO 27001, SOC 2,
GDPR, ISO/IEC 42001



AI Security & Identity

Secure the AI you build
and use



App, Cloud & Supply Chain

AppSec, cloud and vendor
risk



CISO Advisory

vCISO and CISO Office as
a Service

 info@seccomply.net

 seccomply.net

 linkedin.com/company/sec-comply