



DATA PRIVACY | TECHNOLOGY & INNOVATION

Global AI Governance Frameworks in a Diverging World

27 March 2026 6 min read

by Ahmore Burger-Smidt, Director and Head of Regulatory

"The biggest lesson learned is we have to take the unintended consequences of any new technology along with all the benefits, and think about them simultaneously – as opposed to waiting for the unintended consequences to show up and then address them,"

Satya Nadella *Microsoft CEO 2024*

Artificial intelligence governance has moved from theory to the board agenda. Organisations building or deploying AI across borders now face a mix of voluntary guidance and hard law. The practical question is no longer whether to adopt a framework, but which combination will withstand regulatory scrutiny, match the organisation's risk profile, and work in day to day operations. There is no single winner.

When considering guidance and hard law when aiming to adopt an AI framework organisations ought to adopt a practical approach. For most, the defensible answer is layered: comply where the law is strict, and use one or more voluntary frameworks to structure governance, evidence good practice, and adapt as the landscape shifts.

The current touchstones are well known. The OECD AI Principles, refreshed in 2024, provide high-level, government-endorsed norms that cross borders. NIST's AI Risk Management Framework offers operational scaffolding that integrates with enterprise risk programmes. IEEE's Ethically Aligned Design provides engineers with granular guidance. Singapore's Model AI Governance Framework is praised for its practical, proportionate implementation and sector-specific playbooks. ISO/IEC 42001 introduces the first certifiable AI management system standard. The G7 Hiroshima Process Code of Conduct points frontier developers towards safety testing and transparency.

Alongside these sits the outlier in legal effect: the EU AI Act, now in force with staged obligations through 2027 and backed by serious penalties.

Despite different origins, these instruments all speak to the same five principles: fairness, accountability, transparency, human oversight and safety.

Where they deviate is depth and enforceability. The OECD sets the tone, articulating non discrimination, respect for rights, transparency and robustness as shared values, while deliberately stopping short of prescribing how to implement them. NIST translates principles into processes through govern, map, measure, and manage functions, and tackles bias, explainability, and human judgement with concrete practices. IEEE dives into the technical detail, from dataset audits to fail safe design patterns. Singapore keeps the focus on outcomes, insisting on context-appropriate metrics, proportionate explanations, and the right-sized human involvement. ISO/IEC 42001 turns governance into an auditable discipline, requiring documented roles, risk treatment, oversight mechanisms and continual improvement. The G7 Code sets expectations for advanced models: pre-deployment testing, red-teaming, transparency reporting, and post-market monitoring.

Two frameworks, however, play a distinctive role in keeping governance human centred and proportionate. The OECD Principles begin with people, not systems. By anchoring AI to human rights, democratic values and the rule of law, they make human agency and dignity the standard for design choices, deployment contexts and routes to redress. They call for inclusive growth and non-discrimination, pushing organisations to ask who benefits, who is burdened, and whether affected communities can understand, contest, and influence AI-enabled decisions. Their take on transparency and explainability is purposeful: disclosure should be meaningful to users and those impacted, not a tick box. Because the OECD speaks in norms rather than checklists, it invites stakeholder engagement and reasoned judgement, keeping AI grounded in lived experience and social outcomes as technology evolves.

Singapore's Model AI Governance Framework operationalises the same ethos through the principle of proportionality. It assumes that risk is contextual and that fairness, transparency and oversight must be calibrated to the impact of a given use case. It promotes explanations that are meaningful to their audience rather than generic templates, and it links the degree of human involvement in the loop to the stakes of the decision. Its sector guides, notably in financial services and healthcare, translate principles into practical steps that fit real operational environments. By encouraging continuous monitoring, targeted testing, and structured user feedback, it steers teams towards the right-sized controls that protect individuals while leaving room for innovation. For organisations at different stages of maturity, this approach avoids gold plating and reduces the risk that governance becomes paperwork detached from outcomes.

The EU AI Act differs from every other instrument here in both scope and enforceability. It is a binding law with extra territorial reach, applying to providers, deployers, importers and distributors that place AI systems on the EU market or whose systems affect people in the EU. It classifies AI uses by risk, prohibits certain practices outright, and imposes detailed, legally enforceable obligations on high-risk systems, including risk management, data governance, technical documentation, logging, human oversight, post-market monitoring, and incident reporting. It brings general-purpose AI into scope, layering transparency requirements and additional measures when models present systemic risks. Compliance is policed through conformity assessment, with meaningful fines for breaches. Much of the practical detail will be elaborated through harmonised standards and secondary measures over the next two years, but the direction is fixed: unlike voluntary frameworks, the Act creates duties, assigns liability and sets penalties. By contrast, the OECD Principles, NIST, IEEE, Singapore's framework and the G7 Code are non binding; they shape expectations and practice but do not carry legal sanctions. Even ISO/IEC 42001, while certifiable and powerful in procurement and assurance, is not law and does not create any statutory defences on its own.

Choosing among frameworks, therefore, becomes a question of balance and fit. The OECD Principles provide legitimacy, a common language for boards and stakeholders, and a north star that keeps programmes human centred. Singapore supplies the day to day discipline of proportionality, helping teams define the use case, assess the risks, calibrate the controls, explain decisions in ways people can act on, and adjust as evidence accumulates. NIST offers the most detailed operational practices to make those choices repeatable across the lifecycle. ISO/IEC 42001 turns them into a verifiable management system that regulators, customers and investors can trust. IEEE hardens the engineering spine. The EU AI Act sets the hard floor where it applies; its obligations should be built in from the outset, not layered on at the end.

For cross border organisations, interoperability is the key to defensibility. An ISO-style management system can serve as the backbone, integrating NIST processes and Singapore's proportional controls while remaining anchored to the OECD's human-centred norms and mapped to the EU AI Act where relevant.

What does this mean for organisations adopting AI tools, engaging in big data analytics and creating value? The destination is not perfection but defensibility. In a world of regulatory divergence, the strongest posture is a coherent, documented and adaptable governance architecture that shows your work: why you chose the frameworks you did, how they map to your risks and markets, and how you are improving over time.

Principle and prescription are not alternatives; they are the twin rails that keep AI governance both human centred and proportionate, and, where the EU AI Act applies, lawful.

Be proactive. Identify unintended consequences and reap the benefits of AI adoption.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)