

EU AI ACT (2024) vs India DPDP Act (2023) vs NIST AI RMF (2023)

ASPECT	EU AI ACT	INDIA DPDP	NIST AI RMF
Scope	Regulates AI systems placed on the EU market or affecting EU citizens. Extraterritorial.	Regulates digital personal data processing in India or abroad if targeting Indians.	Voluntary framework for AI risk management globally.
Core Approach	Risk-based classification: Unacceptable, High-risk, Limited, Minimal.	Consent-based: processing only with user consent or lawful grounds. Extra duties for Significant Data Fiduciaries.	Process-based: Govern, Map, Measure, Manage functions.
High-Risk Obligations	Conformity assessments, human oversight, logging, documentation, transparency, cybersecurity.	Significant Data Fiduciaries must appoint DPO, do DPIAs, audits, grievance redressal.	Organizations set governance, identify risks, develop metrics, manage and monitor.
Individual Rights	Transparency: users informed when interacting with AI, limited explanation rights.	Rights to access, correct, erase, withdraw consent for personal data.	No enforceable rights; principles of fairness, transparency encouraged.
Enforcement Body	EU AI Office + national regulators.	Data Protection Board of India (DPBI).	None (voluntary guidance).
Penalties	Up to €35M or 7% global annual turnover.	Up to 250 crore (~€27M) per violation.	No penalties, non-binding.
Cross-Border Impact	Applies extraterritorially to any company impacting EU citizens.	Allows cross-border transfers except to restricted jurisdictions.	Global applicability; voluntary use anywhere.
Focus	AI governance, safety, accountability.	Data privacy, consent, user rights.	Risk management, trustworthiness, fairness.