DGPSI-AI vs. Draft Regulations for Use of AI in Courts, 2026

A side-by-side comparison

DGPSI-AI Framework (FDPPI / DPDPA compliance standard)	Draft Regulations for Use of AI in Courts, 2026 (Supreme Court of India)
Nature, scope and purpose	
A voluntary compliance framework for data fiduciaries and data processors under the DPDPA, 2023. Governs any deployer or developer of AI processing personal data, across all sectors. Built as 6 Principles + 9 Deployer Model Implementation Specifications (MIS) + 13 Developer MIS imposed through licensing contracts.	A sector-specific regulation for the judiciary, applying to the Supreme Court, High Courts, and all Courts, Tribunals and statutory Commissions performing adjudicatory functions (Reg. 2). Built as general principles (Ch. II), permitted/prohibited uses (Ch. III), institutional machinery (Ch. IV), oversight (Ch. V), procurement (Ch. VI) and remedies (Ch. IX).
Default risk posture	
Precautionary. Principle 1: "Unknown Risk is a Significant Risk." Deployers default to Significant Data Fiduciary obligations unless an "AI-Deviation Justification Document" records why the unknown risk is not significant (MIS-3).	Adoption-forward. Reg. 16 creates a presumption in favour of responsible AI adoption; Reg. 17 ("Innovation over Restraint") prefers active and responsible adoption over restraint, all other things being equal. Restrictions must be reasoned and recorded in writing.
Human accountability	
Principle 2: behind every AI algorithm there shall be one human for accountability. Deployer designates a human handler (default: DPO/Compliance Officer; alternatively the Process Owner) (MIS-4); the developer's human handler and contact details are recorded in the licensing contract (MIS-5; Dev. MIS-2).	Reg. 8: accountability for AI-assisted decisions rests exclusively on the officer; Black Box opacity or hallucination is no defence. A "Designated Officer" (Reg. 3(1)(u)) supervises, verifies and takes responsibility for each specified AI System; AI output is advisory and must be verified before use (Reg. 8(3)).
Explainability	
Principle 3: every privacy notice covering an AI process must be accompanied by an explainability disclosure. Deployer must collect an authenticated explainability document from the developer through the licensing contract (MIS-6; Dev. MIS-1).	Reg. 7: every AI System must meet high standards of transparency and explainability, understandable to judicial officers, parties and the public. Opaque systems face heightened scrutiny and are restricted in high-risk uses; Reg. 20(1)(e) absolutely prohibits undisclosed/unexplainable AI in processes materially affecting rights or liberty. Explainability documentation is a contract term for High-Risk tools (Reg. 46(4)(h)).
Pre-deployment assessment	
A documented Risk Assessment of the software, treated as the DPIA for the AI process, including vendor confirmation that the software qualifies as "AI" (autonomous learning / probabilistic behaviour test) (MIS-1). An "AI Justification Document" must justify the technical,	A comprehensive Technical and Ethical Impact Assessment before approval (Reg. 35), covering purpose and architecture, training-data quality, bias/error/hallucination risks, cyber security, explainability, HITL compliance and redressal.

DGPSI-AI Framework (FDPPI / DPDPA compliance standard)	Draft Regulations for Use of AI in Courts, 2026 (Supreme Court of India)
operational and economic need for AI (Principle 4; MIS-7).	Optional Controlled Environment Testing (sandbox) before full deployment (Reg. 36).
Audits	
External and independent. Annual evaluation by an external Data Auditor augments the DPIA (MIS-2); the AI model itself must be audited by an independent third-party auditor using an acceptable standard (Dev. MIS-11); vendor security testing preferably by a third party (MIS-8).	Internal only. Annual technical, legal and ethical audits (Reg. 38(1)), but conducted strictly 'in-house' — source code, algorithms and datasets may not be shared with any third party or taken outside Court premises (Reg. 38(2)). Cybersecurity audits at least annually (Reg. 48(5)).
Prohibited uses	
No enumerated prohibition list. Control is exercised through risk classification: cyborgs and sentient algorithms are "Critical Risks" requiring express approval at the highest management level (MIS-9(4)), and guardrails must address dark patterns, neurological manipulation and physical harm (Principle 5).	An absolute, non-derogable list (Reg. 20): no judicial outcome by algorithmic decision-making alone; no AI adjudication/sentencing without HITL; no risk scoring (bail, recidivism, credibility); no behavioural prediction or profiling; no surveillance of judges, advocates or litigants; no undisclosed AI-generated evidence; no use compromising judicial deliberations. Violations trigger remedial action by the AI Committee (Reg. 21).
Technical safeguards	
Engineering-level mandates: tamper-proof kill switch controlled separately from the device intelligence; self-destruct if the model attempts to access the kill switch (MIS-9(1)–(3); Dev. MIS-9–10); "fading memory" time-weighting of learning data (MIS-9(5)); emergency-handling instructions for hallucination or rogue behaviour (Dev. MIS-8); documented guardrails against dark patterns and manipulation (Principle 5).	Governance-level safeguards: emergency and fall-back protocols ensuring continuity through manual means, tested periodically, activated within 24 hours of failure (Reg. 42); continuous monitoring and incident reporting (Regs. 39–40); review of legacy systems within one year (Reg. 41). No kill-switch or hardware-isolation requirement.
Vendor / developer obligations	
13 Developer MIS imposed via the licensing contract: explainability document; human handler contact; training/testing documentation; model risk assessment; documented guardrails; default configuration; re-configuration/re-training instructions; emergency instructions; kill switch; independent audit; post-implementation behaviour monitoring for Critical Risk AI; disclosure of AI agents in the developer's workforce.	Reg. 46: prior written approval for any private entity; comprehensive pre-engagement evaluation; mandatory contract clauses on data ownership, purpose limitation, audit rights, source/model transparency with full technical documentation, explainability for High-Risk tools, indemnity protecting the Court, on-premise/sovereign-cloud deployment for sensitive judicial data, bar on retraining with Court data without approval, liability allocation; Court retains IP in tools built on Court data (Reg. 46(9)).
Indemnity and liability	

DGPSI-AI Framework (FDPPI / DPDPA compliance standard)	Draft Regulations for Use of AI in Courts, 2026 (Supreme Court of India)
Principle 4: unconditional indemnity to the data principal — protection runs to the affected individual.	Reg. 46(4)(i): mandatory indemnity protecting the Court from vendor-caused harm; Reg. 46(4)(l) allocates liability between Court and vendor. Affected persons pursue grievance redressal before the Court (Reg. 52) or general legal remedies (Reg. 53).
Data protection	
Anchored directly in the DPDPA: applies to data fiduciaries/processors; explainability tied to the privacy notice; indemnity to the data principal; risk assessments double as DPIAs.	Applies DPDPA and IT Act to all Court AI Systems (Reg. 47); defines and elevates "sensitive judicial data" — no transfer to external systems without written authorisation, data minimisation, anonymisation before training use, least-privilege access protocols (Reg. 48).
Institutional machinery	
None of its own — relies on existing DPDPA roles: DPO/Compliance Officer, Process Owner, external Data Auditor, and top management approval for Critical Risk systems.	Extensive: a permanent Apex Body with five standing committees (Judicial, Technical, Infrastructure & Finance, Case & Data Management, Cyber Security); CoRE-AI research centre; AI Committees in the Supreme Court and every High Court; AI Secretariats; AI Register; AI Incident Database; AI Content Verification Authority; Annual Transparency Reports (Ch. IV–V).
Disclosure to affected persons	
Explainability disclosure accompanies the privacy notice to data principals whose personal data is processed by the AI (Principle 3); sufficient disclosure of AI risk to data principals (MIS-9(6)).	Parties must be informed when AI materially assists Court processes (Reg. 43(1)–(2)); parties/counsel must declare AI-assisted submissions in prescribed Annexure formats; synthetic data use must be disclosed; GenAI content requires origin disclosure and centralised verification (Reg. 3(1)(y), Reg. 43–44).
Autonomous / agentic AI	
Addressed at developer level: disclosure of AI agents used in the developer's workforce and their impact on the model (Dev. MIS-13); post-implementation behaviour monitoring for Critical Risk AI (Dev. MIS-12); sentient algorithms classified as Critical Risk (MIS-9(4)).	Mentioned once: the Apex Body must ensure no AI system, "whether autonomous AI agent or static predictive model", violates the law (Reg. 23(a)). No definition of "AI agent" and no dedicated agentic-AI standards.
Overall character	
Risk-first compliance standard governing the deployer–vendor relationship through documentation, contract and independent assurance; strong on engineering safeguards, silent on institutional design.	Institution-first regulation governing one sector through committees, registers, approvals and absolute prohibitions; strong on governance architecture and red lines, lighter on engineering-level and independent-assurance requirements.

Note: The two instruments are complementary rather than competing. DGPSI-AI governs the vendor/deployer side of the same AI Service Providers the Courts would engage under Chapter VI of the draft Regulations; a vendor compliant with the DGPSI-AI developer specifications would already satisfy most of the contractual requirements of Regulation 46(4). The principal points of tension are the audit philosophy (independent third-party vs. in-house only) and the default risk posture (precautionary vs. adoption-forward).