

Checkpoint	What to Ask the Vendor	Why It Matters
Transparency artifacts	Share the latest Model Card, Data Sheet, and bias metrics for this release.	Confirms the vendor measures subgroup error and documents lineage as required for high-risk systems under EU AI Act Art. 10 on data governance. https://artificialintelligenceact.eu/article/10
Regulatory alignment map	Map your controls to NIST SP 1270, EU AI Act risk requirements, and ISO/IEC 42001 clauses.	Harmonizes their lifecycle controls with the frameworks most auditors use, reducing integration gaps. https://artificialintelligenceact.eu/article/14
Explainability Interface	Provide an API or dashboard exposing feature-influence (e.g., SHAP) and slice-level metrics on demand.	Let's your risk team interrogate bias drivers and contest individual predictions—an implicit requirement of EU AI Act human-oversight rules (Art. 14) https://artificialintelligenceact.eu/article/14 Artificial Intelligence Act EU
Independent assurance	Provide a recent SOC 2 report with an AI fairness annex or a TÜV/AIQCP certificate.	External attestation reduces reliance on vendor self-reporting and meets board-level assurance norms. https://www.schellman.com/blog/soc-examinations/how-to-incorporate-ai-into-your-soc-2-examination
Human override & appeal	End-users must be able to disable automated decisions or request human review	Satisfies ‘meaningful human oversight’ obligations in EU AI Act Art. 14 and many consumer-protection statutes.
Bias-incident SLA	Report any discovered fairness or drift issue within 24 h; root-cause analysis in 7 days.	Aligns bias events with security-incident playbooks, limiting liability and reputational damage.
Training-data lineage & usage	Grant right to inspect training-data sources; forbid reuse of our data for unrelated models; list all sub-processors.	Prevents hidden proxy bias, IP leakage, and supply-chain surprises—aligns with EU AI Act Art. 10(2)(b) on data origin. https://artificialintelligenceact.eu/article/10/
Data-residency & deletion	Process data only in approved jurisdictions; certify deletion or anonymization within 30 days of contract end.	Meets sectoral sovereignty laws and eases exit without legal ([Article 10: Data and Data Governance
Ongoing drift & fairness monitoring	Provide monthly fairness reports or API hooks so we can pull real-time disparity metrics.	Bias can re-emerge post-deployment; continuous monitoring is mandated by ISO/IEC 42001 internal-audit clause 9.2. https://cyberzoni.com/standards/iso-42001/clause-9-2
Exit & portability	“On termination, deliver decision logs and model artefacts in a portable format.”	Enables forensic bias review and prevents lock-in if you must switch vendors.