AI Vocabulary Reference • Tier 4: Architecture & Vendor

The language of procurement and infrastructure • Aurorae Group, LLC

This reference is designed for those involved in selecting, contracting, or managing AI vendors and infrastructure — including procurement, legal, IT, finance, and senior HR leaders. It assumes familiarity with foundational concepts (Tier 1) and governance vocabulary (Tier 3). Note: This document addresses concepts, not legal advice. All vendor contracts should be reviewed by qualified legal counsel.

Infrastructure & Deployment

The terms that govern how AI systems are built, hosted, and integrated — and what that means for data, security, and organizational control.

API (Application Programming Interface)	A defined set of protocols that allows one software system to communicate with another. AI vendors typically offer APIs that allow organizations to integrate AI capabilities directly into their own applications and workflows. **Why it matters for procurement:** Understanding whether a vendor offers API access — and at what cost — determines how deeply an AI tool can be embedded into existing systems. It is also a signal of the vendor's intended market: consumer tools rarely expose APIs; enterprise tools typically do.
Cloud vs. On-Premise	Cloud AI tools run on the vendor's servers and transmit data over the internet. On-premise solutions run on the organization's own infrastructure, keeping data within its control. Hybrid models combine both approaches. **Why it matters for procurement:** For organizations handling sensitive data — employee records, compensation, health accommodations — the cloud vs. on-premise question is a data governance question before it is a technology question. The answer shapes what vendors are even eligible for consideration.
Data Residency	The geographic location where data is stored and processed. Many countries and regulated industries require that certain data remain within specific jurisdictions. Cloud AI vendors may store data in multiple regions by default. **Why it matters for procurement:** Nonprofits and foundations operating across jurisdictions, or handling data subject to state-level privacy laws, need to know where their data lives. Vendors who cannot specify data residency or offer jurisdictional controls are a compliance risk.
Model Hosting	The infrastructure environment in which an AI model runs — which may be the AI developer's own servers, a third-party cloud provider (AWS, Azure, Google Cloud), or the customer's own infrastructure. **Why it matters for procurement:** Model hosting determines who has physical access to the data processed by the model. A vendor may have strong contractual data protections but host on infrastructure controlled by a third party with its own data practices. Both layers require review.
Inference vs. Training	Inference is the process of using an AI model to generate outputs from new inputs. Training is the process of building or updating a model using data. These are distinct operations with different data implications. **Why it matters for procurement:** Most vendor agreements cover inference — using the model — but organizations should clarify whether their data is also used

	for training. Many enterprise agreements explicitly prohibit training on customer data. This distinction should be confirmed in contract, not assumed.
Fine-Tuning	The process of further training a pre-built AI model on an organization's own data to improve its performance on specific tasks or to align its outputs with organizational voice, terminology, and standards. **Why it matters for procurement:** Fine-tuning can significantly improve AI performance for specialized use cases but requires careful data governance. The data used to fine-tune a model becomes part of the model — understanding what that means for data ownership, confidentiality, and vendor rights is essential before proceeding.

Vendor Evaluation

The vocabulary of due diligence — what to ask, what to verify, and what the answers actually mean for your organization.

Service Level Agreement (SLA)	A contractual commitment from a vendor specifying the performance standards they guarantee — including uptime, response time, support availability, and remedies for failures to meet those standards. **Why it matters for procurement:** SLAs define the floor of vendor accountability. Organizations that rely on AI tools for operational continuity — HR platforms, applicant tracking, benefits administration — need SLAs that reflect that dependency, including clear escalation paths and financial remedies.
Data Processing Agreement (DPA)	A legally binding contract between an organization and a vendor that governs how personal data is collected, stored, processed, and protected — required under GDPR and similar privacy regulations. **Why it matters for procurement:** Any AI vendor that processes personal data on your behalf requires a DPA. This is not optional and should be reviewed by legal before any data is shared. Vendors who resist or delay DPA execution are a signal worth taking seriously.
Data Ownership	The legal rights governing who controls, can access, can use, and can transfer data — including data inputted into an AI system, data generated by the system, and derivative data created through use. **Why it matters for procurement:** Vendor contracts frequently include provisions that grant the vendor broad rights to data submitted through their platform. Understanding and negotiating data ownership clauses before signing protects organizational IP, employee data, and competitive information.
Zero Data Retention	A vendor policy or contractual provision specifying that data submitted to the AI system is not stored, logged, or retained beyond the immediate interaction — providing a stronger privacy guarantee than standard data handling. **Why it matters for procurement:** Zero data retention is available from some enterprise AI vendors and is worth requesting for use cases involving sensitive HR data. It should be confirmed contractually, not assumed based on marketing materials.
SOC 2 Certification	A third-party audit certification confirming that a vendor's systems and controls meet defined standards for security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type II covers an extended period of operational compliance.

	Why it matters for procurement: SOC 2 Type II is a reasonable baseline security requirement for AI vendors handling organizational data. Its absence does not necessarily disqualify a vendor, but it shifts the burden of due diligence and should prompt deeper scrutiny of security practices.
Vendor Lock-In	The degree to which an organization becomes dependent on a specific vendor's technology, making it difficult or costly to switch to an alternative. AI tools that store proprietary data formats, custom models, or workflow integrations create higher lock-in risk. **Why it matters for procurement:** Lock-in risk is a strategic consideration as much as a technical one. Organizations investing significantly in AI tool configuration, custom prompts, or vendor-specific integrations should evaluate exit costs as part of procurement — not after the contract is signed.

Contract & Compliance

The terms buried in vendor agreements that determine who bears risk, who owns what, and what happens when things go wrong.

Indemnification	A contractual provision in which one party agrees to compensate the other for losses or damages arising from specified circumstances — in AI contracts, commonly covering IP infringement claims arising from AI-generated content. **Why it matters for procurement:** AI-generated content carries copyright uncertainty. Some vendors indemnify customers against IP infringement claims; others explicitly disclaim liability. Understanding who bears this risk before deployment — especially for externally published content — is essential.
Acceptable Use Policy (Vendor)	The vendor's own terms governing how their AI tool may be used — typically prohibiting harmful, illegal, or high-risk applications. Violations can result in account termination and may create organizational liability. **Why it matters for procurement:** Vendor AUPs are contractual obligations, not suggestions. Organizations should review them as part of procurement and ensure internal usage policies are aligned. Gaps between what employees are doing and what the vendor permits create legal exposure.
AI-Generated Content Rights	The question of who owns content produced by an AI system — the user, the vendor, or neither. This is an evolving area of intellectual property law with significant variation across jurisdictions and vendor agreements. **Why it matters for procurement:** For organizations producing client-facing, published, or commercially valuable content using AI, understanding the ownership status of AI-generated outputs is not optional. Some jurisdictions do not recognize AI-generated content as copyrightable, which affects how it can be protected.
Model Versioning	The practice of tracking and managing changes to an AI model over time, including updates to its training data, architecture, or behavior. Vendors may update models without notice, changing the outputs organizations have built workflows around. **Why it matters for procurement:** Organizations that depend on consistent AI behavior — for compliance, quality control, or brand voice — need contractual clarity on how and when models are updated, whether prior versions remain available, and how output changes will be communicated.

Breach Notification	The contractual and legal obligation for a vendor to notify an organization within a specified timeframe if a data breach occurs that may have exposed organizational or employee data. **Why it matters for procurement:** Breach notification timelines vary by jurisdiction and contract. GDPR requires notification within 72 hours of discovery. Vendor contracts should specify notification timelines, the information that must be included, and the remediation process — before a breach occurs.
Exit Provisions	Contractual terms governing what happens at the end of a vendor relationship — including data return, data deletion timelines, transition support, and any continuing obligations on either party. **Why it matters for procurement:** Exit provisions are frequently negotiated last and given the least attention. They matter most when a relationship ends badly or urgently. Organizations should ensure they can retrieve their data in a usable format, within a reasonable timeframe, and that deletion is confirmed and auditable.