



SaaS Contract Checklist for 2025

A Checklist for Negotiating SaaS Agreements in the Age of AI



Reviewing SaaS Contracts in 2025

As SaaS offerings increasingly incorporate and rely on AI — from large language models to machine learning and expanded use of APIs — contracts also continue to adapt to keep pace with evolving business models and regulatory scrutiny. In many ways, this metamorphosis is similar to the transition from on-premise software to cloud-based SaaS products, but with even greater levels of complexity relating to data ownership, privacy, IP rights, security, accuracy/bias, and equitable allocation of risk.

For in-house counsel, the stakes are higher than ever: regulators and customers (both public and private sector) often expect transparency and safeguards, while providers are shifting to pricing models to account for the costs and complexity of implementing and running new AI functionality, and trying to mitigate potential liability from use of third-party AI models. These changes can create new risks as well as opportunities to better align contracts with business priorities.

This checklist highlights some of the key issues to consider so you're equipped to ask informed questions (whether you're a provider or a customer), engage with stakeholders across your organization and on the other side of the table, and/or create a framework to evaluate whether your SaaS agreements are positioned to be future-ready, equitable, and aligned with organizational risk tolerance and business goals.

With this in mind, it may be useful to focus on the following concepts when reviewing, negotiating, or developing SaaS agreements.

SaaS Contract Checklist

01.

Data Ownership & Usage Rights

- Clearly define ownership of customer data, usage data, embeddings, fine-tuning, derivative data, and AI-generated outputs.
- Specify limits on provider use of customer data for training AI models — distinguish between public/shared models vs. private instances.
- Ensure data portability and deletion rights are explicit, including timelines and format requirements.
- Require clear procedures for data return upon termination and audit rights to confirm deletion.

02.

Privacy & Security

- Confirm compliance with applicable AI/data regulations, such as GDPR, CPRA, and HIPAA, and monitor for changes and newly implemented laws and regulations.
- Require third-party certifications (SOC 2, ISO 27001, FedRAMP for GovTech), as applicable.
- Assess the process for managing sub processors and downstream vendors, including addressing notice, approval rights, and/or rights of termination.
- Address incident response timelines, notification requirements, and cooperation on breach investigations.
- Identify approaches for AI-specific risks, such as prompt injection, data leakage, and retrieval automated generation.
- Consider controls covering data segregation, encryption, AI testing, content filtering, and prompt retention periods.

03.

AI-Specific Warranties & Disclaimers

- Evaluate the scope of warranties for accuracy, explainability, reliability, and bias mitigation.
- Negotiate remedies for AI performance failures, including reperformance, remediation, credits, and termination rights.
- Address disclaimers that exclude high-risk uses (medical, legal, safety-critical) and ensure carve-outs are appropriately tailored to the specific use case.
- Ensure appropriate transparency, including updates, retraining cycles, tech stack, and major AI model changes.

04.**Intellectual Property (IP) Rights**

- Clarify ownership of trained models, outputs, prompts, fine tuning, embeddings, and customer-specific data sets.
- Address copyright and infringement risks tied to AI training data and generated outputs.
- Incorporate tailored indemnities relating to third-party IP infringement claims — including those arising from AI-generated content.
- Appropriately scope mutual licenses (to client content and use of the platform, etc.) with relevant rights and limitations, including suspension and termination where appropriate, to mitigate risk.
- Consider use of curated data sets, use of content filters, originality checks, watermarking, and similarity thresholds as mitigations.

05.**Service Levels & Transparency**

- Compare traditional uptime SLAs to new AI performance metrics, such as accuracy thresholds/rates, response latency, retraining rates, throughput limitations.
- Push for algorithmic transparency — model lineage, audit rights, access to documentation, and disclosures of training data sources.
- Define remedies for breaches, including model drift, retraining failures, or systemic inaccuracy.
- Consider claw backs or service credits for material failures tied to AI components.

06.**Liability & Insurance**

- Review liability caps and carve-outs in light of AI risks, including data misuse, discriminatory, harmful or inaccurate outputs, prohibited use cases, unauthorized training on customer data and regulatory fines.
- Consider “super caps” or uncapped liability for privacy breaches, confidentiality violations, and certain AI risks.
- Assess appropriate insurance coverage, specifically covering cyber risk, AI risks, and professional liability, and ensure limits align with exposure.

07.**Regulatory Trends**

- Monitor for newly enacted AI laws and regulation.
- Assess applicability of the EU AI Act, U.S. Executive Orders, NIST AI Risk Framework, and state-level AI laws.
- Include a change-in-law clause to ensure the contract can adapt to comply with new regulations.
- For GovTech SaaS in particular, expect audit rights, transparency mandates, Red-teaming (pre-testing) and impact assessments in line with procurement requirements.
- Comply with regulatory inquiries.

Negotiation Best Practices for AI-Enabled SaaS Deals

If You're the Provider:

- Use visual diagrams to explain your AI/tech stack and build client trust.
- Propose remediation processes for inaccurate or biased outputs.
- Carve out AI liability where possible; push back on uncapped liability for third-party LLMs.
- Disclaim liability for high-risk use cases; consider acceptable use policies to ensure responsible use of AI tools.
- Offer structured audit trails to reassure clients on model decisions.

If You're the Client:

- Ask for disclosures about model training, refresh cycles, data location and retention, subprocessors, and AI data usage, including prohibitions and limitations on training/fine-tuning.
- Push for tailored SLAs with claw backs and clear remediation steps.
- Require “human-in-the-loop” safeguards for high-risk outputs.
- Negotiate termination rights, data portability, and deletion guarantees.
- Insist on reasonable privacy and security protective measures, even where liability caps exist.



Key Takeaway

SaaS contracts are no longer just about uptime and liability caps. They must address AI-specific risks, rapidly evolving regulations, and shifting business models. By proactively updating your negotiation approach, you can protect your organization and ensure scalable, future-ready partnerships.

