INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

AI SAAS CONTRACTS: DATA RIGHTS, LIABILITY, AND VENDOR RISK

AUTHORED BY – SAMUDRANIL CHAKRABARTI
Student
Amity University Kolkata

Abstract

The commercialisation of artificial intelligence within cloud-based enterprise software has shattered the deterministic framework of traditional SaaS procurement. Unlike legacy software architectures, probabilistic AI systems yield dynamic and unpredictable results, necessitating a structural transition in intellectual property, liability allocation, and data rights management. This research paper evaluates the legal friction inherent in B2B AI contracting, specifically addressing the ownership of customer inputs and generated outputs alongside the risks of broad model-improvement covenants. By analysing the judicial enforceability of point-of-use liability disclaimers and mapping statutory mandates under the GDPR and EU AI Act, this study illustrates how fragmented, multi-tiered supply chains impose cascading risks upon developers and deployers alike. Ultimately, this analysis proposes an operational roadmap comprising tiered liability architectures, covenanted Data Processing Addenda, and performance-aligned pricing models to mitigate the regulatory vulnerabilities of unsanctioned "shadow AI" within the modern corporate landscape.

Keywords: *AI SaaS contracts, data rights, liability allocation, vendor risk, EU AI Act*

I. INTRODUCTION

The commercialisation of artificial intelligence within cloud-based enterprise software has shattered the deterministic framework of traditional SaaS procurement. For over two decades, the acquisition of software-as-a-service has functioned under a paradigm where predefined inputs yield predictable, repeatable, and easily verifiable results. Consequently, legacy Master Services Agreements (MSAs) and Data Processing Addenda (DPAs) are structured around this static architecture, treating the vendor as a passive host of customer information. Within this legacy environment, operational risks are restricted to service interruptions, standard

ISSN: 2582-6433

cybersecurity breaches, and basic non-performance, typically mitigated through linear Service Level Agreements (SLAs) and historical liability caps.

However, the integration of generative AI and autonomous agentic workflows has rendered these traditional frameworks obsolete. AI SaaS platforms operate on a probabilistic model, where proprietary corporate datasets and prompts are processed through neural networks characterised by non-deterministic behaviour. These systems yield dynamic and unpredictable outputs, introducing severe legal friction across six critical contractual pillars: limitation of liability, indemnification, the DPA, AI usage rights, SLA performance, and pricing architectures. This shift necessitates a structural transition in how financial and operational exposures are managed within the modern corporate landscape.

This legal friction stems from the mismatch between standard SaaS boilerplate and the realities of the AI data lifecycle. Vendor templates routinely seek broad model-improvement covenants, permitting the ingestion of confidential customer inputs to fine-tune commercial algorithms. Such practices compromise trade secret protections and threaten intellectual property exclusivity while triggering significant data privacy vulnerabilities. Concurrently, generic liability disclaimers fail to protect enterprise buyers from the non-linear failure modes inherent in probabilistic systems, including factual hallucinations, algorithmic bias, and third-party copyright infringement arising from unlicensed training datasets.

These risks are further compounded by a fragmented regulatory environment that imposes cascading, non-transferable compliance burdens upon the deployer. Under the EU AI Act and relevant GDPR provisions, organisations must satisfy rigorous mandates regarding human oversight, data quality management, and automated log retention. Traditional procurement frameworks are incapable of mitigating these exposures, leading to a dangerous rise in unsanctioned "shadow AI" and severe regulatory vulnerabilities across the multi-tiered supply chain.

II. RESEARCH OBJECTIVES

This study investigates the legal friction and operational exposures inherent in the commercialisation of AI within cloud ecosystems by pursuing these core research objectives:

1. To dissect the doctrinal allocation of intellectual property rights, specifically addressing the ownership of customer inputs and the ingestion of proprietary data for model

ISSN: 2582-6433

fine-tuning.

2. To examine the judicial enforceability of non-deterministic system disclaimers under the UCC conspicuousness mandate and the emerging Point-of-Use In-Product Placement Principle.
3. To evaluate how cascading deployer mandates under Article 26 of the EU AI Act and GDPR necessitate a structural transition in Master Services Agreements and DPAs.
4. To formulate a multi-dimensional risk-classification taxonomy and operational remediation pathway to manage fragmented supply chain exposures and the proliferation of shadow AI.

III. RESEARCH QUESTIONS

To investigate the doctrinal legal friction and operational vulnerabilities identified, this study addresses the following research questions:

- **Research Question 1:** By what contractual mechanisms can procurement teams enforce "no-training" covenants to prevent the ingestion of proprietary corporate datasets while securing exclusivity over generated outputs?
- **Research Question 2:** What thresholds of conspicuousness and point-of-use placement must be satisfied for probabilistic system disclaimers to maintain judicial enforceability under emerging technology litigation standards?
- **Research Question 3:** To what extent do non-transferable deployer mandates under the EU AI Act and GDPR necessitate a structural transition in the architecture of legacy Master Services Agreements and DPAs?
- **Research Question 4:** How should multi-dimensional risk-classification taxonomies and performance-aligned pricing models be structured to mitigate the cascading exposures of fragmented supply chains and shadow AI?

IV. HYPOTHESES

To provide a doctrinal foundation for the legal friction evaluated throughout this study, the following research hypotheses are established:

- **Hypothesis 1:** Probabilistic system disclaimers satisfying the Point-of-Use In-Product Placement Principle possess significantly higher judicial enforceability than generic liability exclusions buried within legacy SaaS boilerplate.
- **Hypothesis 2:** The operationalisation of multi-dimensional risk-classification

ISSN: 2582-6433

taxonomies during procurement serves to mitigate regulatory vulnerabilities and prevent unauthorised data leakage under the EU AI Act and GDPR.

V. RESEARCH METHODOLOGY

This study adopts a qualitative doctrinal legal research methodology supplemented by a comparative risk-assessment framework. The doctrinal analysis examines judicial decisions, regulatory guidance, and statutory frameworks in the United States and the European Union, with particular emphasis on intellectual property rights, contractual enforceability, data governance, and AI-related regulatory obligations. The study also reviews commonly used contractual instruments, including Master Services Agreements (MSAs), Data Processing Agreements (DPAs), and AI-specific contractual provisions employed in enterprise software procurement.

To complement the doctrinal analysis, the study develops a comparative risk-classification framework for assessing organisational exposure arising from the deployment of third-party AI systems. The framework evaluates four key factors: (i) the degree of influence exercised by AI over organisational decision-making, (ii) the level of transparency surrounding the underlying model and processing activities, (iii) the operational sensitivity of the business function in which the AI is deployed, and (iv) the extent of reliance on third-party vendors, subprocessors, and API integrations.

By systematically analysing these factors, the framework provides a structured method for identifying legal, regulatory, and operational risks associated with AI procurement and deployment. The resulting assessment assists organisations in determining appropriate contractual safeguards, compliance controls, and governance measures before integrating AI systems into business operations.

VI. LITERATURE REVIEW

The legal scholarship on artificial intelligence in enterprise software primarily focuses on intellectual property rights, copyright law, contractual risk allocation, and the rapidly evolving regulatory landscape. In the United States, recent debates have centred on whether the use of copyrighted works to train large language models constitutes fair use. Judicial decisions in *Bartz*

ISSN: 2582-6433

v. Anthropic[1] and *Kadrey v. Meta Platforms, Inc.*[2] suggest that AI training may qualify as a transformative use where copyrighted materials are used to extract patterns and relationships rather than reproduce expressive content. At the same time, commentators note that the use of pirated or unlicensed datasets remains legally vulnerable, particularly where licensing markets for such works already exist.

Scholars have also examined the copyrightability of AI-generated outputs. Following *Thaler v. Perlmutter*[3], the prevailing position is that works generated entirely by artificial intelligence are not eligible for copyright protection in the absence of meaningful human authorship. Nevertheless, academic discussion continues regarding whether substantial human involvement through prompt engineering, curation, or creative direction may satisfy the authorship requirement.

Another significant area of scholarship concerns regulatory enforcement against misleading claims regarding artificial intelligence. Commentators highlight the increasing willingness of regulators to challenge so-called "AI washing," where organisations exaggerate the capabilities or reliability of AI systems. Particular attention has been given to remedies requiring the deletion of unlawfully obtained data and, in some cases, the destruction of models trained on such data.

The literature further identifies growing regulatory fragmentation within the United States. State-level legislation increasingly imposes obligations relating to transparency, algorithmic accountability, privacy protection, and high-risk AI deployment. These developments are complemented by emerging litigation involving automated decision-making systems, consent-based data collection, professional liability, and the use of generative AI in regulated sectors.

Despite the expanding body of scholarship on copyright, privacy, and AI governance, relatively little attention has been paid to how these legal risks converge within enterprise AI Software-as-a-Service (SaaS) contracts. Existing studies often analyse intellectual property,

[1] Bartz v. nthropic PBC, 3:24-cv-05417 (N.D. Cal.).
[2] Kadrey v. Meta Platforms, Inc., No. 3:23-cv-03417 (N.D. Cal.)
[3] Thaler v. Perlmutter, 687 F. Supp. 3d 140,. 142 (D.D.C. 2023).

ISSN: 2582-6433

data protection, and regulatory compliance in isolation. This paper seeks to address that gap by examining how ownership rights, liability allocation, vendor dependencies, and statutory compliance obligations interact within the practical context of B2B AI procurement and deployment.

VII. RESEARCH & ANALYSIS

The integration of generative artificial intelligence into enterprise Software-as-a-Service (SaaS) platforms has fundamentally altered traditional approaches to contractual risk allocation. Conventional SaaS contracts were designed for deterministic software systems that operate according to predictable inputs and outputs. Generative AI systems, however, produce probabilistic outputs that may be inaccurate, biased, fabricated, or legally problematic despite functioning as intended. As a result, contractual frameworks developed for traditional cloud services are increasingly inadequate for managing AI-specific risks.

A. *Ownership and Control of AI Data*

One of the most significant areas of concern is the ownership and use of data. Enterprise customers frequently provide proprietary information, trade secrets, customer records, and commercially sensitive documents as prompts or inputs to AI systems. While vendors often seek broad rights to use such data for model improvement and training purposes, these provisions can create substantial intellectual property and confidentiality risks. The analysis demonstrates that organisations should distinguish between customer inputs, generated outputs, and vendor-owned models when negotiating contractual rights. Failure to clearly allocate ownership and usage rights may result in the unintended transfer of commercially valuable information into a vendor's training ecosystem.

B. *Liability Allocation in Probabilistic Systems*

The study further reveals that liability allocation has emerged as a central challenge in AI procurement. Traditional limitation-of-liability clauses, which typically cap damages at a multiple of subscription fees, may be insufficient where AI-generated outputs contribute to regulatory violations, discriminatory decisions, financial losses, or reputational harm. Because the consequences of AI failures can extend far beyond ordinary software outages, contractual mechanisms must account for the unique risks posed by autonomous and semi-autonomous decision-making systems. Enhanced indemnity provisions, differentiated liability caps, and clearly defined responsibilities for compliance failures therefore become increasingly

ISSN: 2582-6433

important.

C. *Regulatory Compliance and Deployer Responsibility*

The analysis also highlights the growing disconnect between contractual allocations of responsibility and statutory regulatory obligations. Under emerging regulatory frameworks, particularly within the European Union, certain compliance duties remain non-transferable regardless of contractual wording. Even where vendors provide assurances regarding model safety or legal compliance, enterprise deployers may remain directly responsible for ensuring appropriate human oversight, record-keeping, transparency, and risk management. Consequently, organisations cannot rely solely on contractual indemnities as a substitute for internal governance and compliance processes.

D. *Enforceability of AI Disclaimers*

Another recurring issue concerns the legal effectiveness of AI-related disclaimers. Vendors commonly attempt to limit liability through broad disclaimers regarding accuracy, hallucinations, or professional advice. However, contemporary regulatory and judicial developments suggest that disclaimers hidden within lengthy terms of service may provide limited protection. Disclosures that are presented clearly at the point of use and immediately before reliance is placed on AI-generated content are more likely to satisfy notice requirements and support enforceability. This indicates a broader shift from passive contractual disclosure towards active user-facing risk communication.

The fragmented nature of the modern AI supply chain further complicates accountability. Enterprise AI services frequently depend on multiple actors, including foundation model developers, cloud infrastructure providers, API intermediaries, and downstream application vendors. When harmful outcomes occur, determining responsibility becomes significantly more difficult because each participant controls only part of the overall system. This fragmentation increases legal uncertainty and strengthens the case for more comprehensive contractual due diligence during procurement.

E. *Shadow AI and Organisational Governance*

Finally, the rise of unsanctioned "shadow AI" usage demonstrates that AI governance is no longer solely a contractual issue. Employees can access external AI systems independently of organisational approval processes, creating risks relating to confidentiality, data protection, and regulatory compliance. The analysis therefore supports the adoption of structured risk-

ISSN: 2582-6433

classification frameworks that enable organisations to assess AI tools according to factors such as decision-making influence, transparency, organisational impact, and third-party dependency. Such frameworks provide a practical basis for distinguishing acceptable uses from high-risk deployments requiring enhanced oversight.

Overall, the findings indicate that effective AI governance requires a combination of contractual safeguards, regulatory compliance mechanisms, and organisational controls. Neither traditional SaaS agreements nor regulatory compliance measures alone are sufficient. Instead, organisations must adopt integrated governance structures capable of addressing the interconnected legal, technical, and operational risks associated with enterprise AI deployment.

VIII. RECOMMENDATIONS

The analysis suggests that effective governance of enterprise AI SaaS systems requires a combination of contractual safeguards, regulatory compliance measures, and organisational controls. Four broad strategies emerge from the research.

A. Strengthening Data Governance Through AI-Specific Contractual Protections

Organisations should move beyond standard SaaS contractual templates and negotiate AI-specific data protection provisions. Particular attention should be paid to the use of customer inputs, prompts, and outputs for model training and improvement. Contracts should clearly define ownership rights over customer-generated data, restrict unauthorised training activities, and establish transparent obligations regarding data retention and deletion. Where third-party model providers or subprocessors are involved, equivalent data protection obligations should extend throughout the supply chain to ensure consistent accountability.

B. Adopting Risk-Based Liability Allocation Mechanisms

Traditional limitation-of-liability clauses may not adequately address the potentially significant consequences of AI-related failures. A risk-based approach to liability allocation is therefore desirable. Higher levels of liability protection may be appropriate for incidents involving data breaches, confidentiality violations, intellectual property disputes, or regulatory non-compliance. Such an approach allows contractual remedies to better reflect the scale and nature of risks associated with AI-enabled decision-making systems.

C. Integrating Contractual Compliance Measures with Regulatory Obligations

The research demonstrates that contractual protections alone cannot eliminate legal exposure

ISSN: 2582-6433

where regulatory obligations are imposed directly on deployers. Organisations should therefore ensure that procurement agreements support compliance with applicable legal frameworks, including data protection and AI governance regulations. Key considerations include access to operational logs, transparency regarding model performance, audit rights, and evidence of governance and risk-management practices adopted by vendors. Compliance responsibilities should be clearly allocated while recognising that certain statutory obligations remain non-transferable.

D. Developing Organisational Controls to Address Shadow AI

The increasing use of unauthorised AI tools by employees presents significant governance challenges. Organisations should establish clear internal policies governing AI usage, provide approved alternatives for business functions, and implement appropriate technical safeguards to prevent unauthorised processing of confidential or personal information. Training programmes, access controls, monitoring mechanisms, and risk-classification frameworks can further support responsible AI adoption while reducing the likelihood of compliance failures and data leakage incidents.

Taken together, these measures demonstrate that successful AI governance requires a holistic approach that combines contractual risk allocation, regulatory compliance, and organisational oversight. As AI technologies continue to evolve, organisations that adopt integrated governance frameworks will be better positioned to manage legal uncertainty while benefiting from technological innovation.

IX. CONCLUSION

The commercialisation of non-deterministic artificial intelligence within the SaaS ecosystem has shattered the legacy paradigm of technology procurement and contractual architecture. Traditional, deterministic software frameworks, predicated upon the assumption of predictable inputs yielding repeatable results, are fundamentally incapable of insulating organisations from the systemic risks of proprietary data ingestion, algorithmic bias, and non-linear liability exposures. By bifurcating data rights into discrete categories of inputs and outputs, establishing robust tiered liability architectures, and deploying conspicuous point-of-use disclaimers, enterprise buyers can successfully navigate the legal friction inherent in probabilistic systems.

Ultimately, the mitigation of AI vendor risk has evolved beyond a mere operational assessment; it now constitutes a critical regulatory and governance mandate. As regulatory bodies across

ISSN: 2582-6433

the United States and European Union increasingly enforce non-transferable deployer accountability, organisations must undergo a structural transition from passive boilerplate templates toward highly active, multi-dimensional risk-classification taxonomies. Those enterprises that proactively restructure B2B instruments, mandate log export portability, and implement technical barriers against shadow AI will secure a significant competitive, operational, and regulatory advantage within the modern AI-driven corporate landscape.

X. WORKS CITED

1. Lawyer to Draft AI SaaS Agreements | Andrew S. Bosin — NJ Technology Attorney, https://www.njbusiness-attorney.com/lawyer-to-draft-ai-saas-agreements/
2. AI Vendor Risk Management: Assessing Third Party AI Suppliers - ISMS. online, https://www.isms.online/iso-42001/ai-vendor-risk/
3. AI Contract Review and Negotiation Attorneys in South Florida - George Law, https://georgelaw.com/ai-contract-review-negotiation-attorneys-south-florida/
4. A SaaS Agreement Has up to 50 Clauses. Six Carry the Risk. — GC AI, https://gc.ai/blog/saas-agreement
5. The Essential SaaS Compliance Checklist for 2026 - Zylo, https://zylo.com/blog/saas-compliance-checklist
6. AI & SaaS Startup Lawyer | SaaS Law Firm Andrew S. Bosin LLC – AI & SaaS Startup Lawyer, https://www.njbusiness-attorney.com/
7. AI Contract Lawyer for Startups (2026 Guide to AI Vendor Agreements), https://www.njbusiness-attorney.com/ai-contract-lawyer-for-startups/
8. Artificial Intelligence 2026 - Germany | Global Practice Guides ..., https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2026/germany
9. Shadow AI in Organisations: A Practical Framework for Detection ..., https://www.preprints.org/manuscript/202602.1924
10. AI Liability Disclaimers: Howto Limit Legal Exposure for AI Outputs ..., https://www.njbusiness-attorney.com/ai-liability-disclaimers/
11. Best AI Software Contract Lawyer (2026 Legal Guide for Startups & Businesses), https://www.njbusiness-attorney.com/best-ai-software-contract-lawyer/
12. What Is the EUAI Act? Compliance Beyond the Deadline | Opstream, https://www.opstream.ai/blog/what-is-the-eu-ai-act/
13. AI Vendor Due Diligence Checklist 2026: 50+ Questions – AI Buzz,

ISSN: 2582-6433

https://aibuzz.blog/ai-vendor-due-diligence-checklist/

14. AI governance audit readiness: A guide for security teams, https://www.nudgesecurity.com/post/ai-governance-audit-readiness
15. AI Risk & Liability: Structuring Responsibility for AI-Driven Decisions - WCR Legal, https://wcr.legal/services/ai-law/governance-risk/ai-risk-liability/
16. AI policy and compliance for companies - Scouts by Yutori, https://scouts.yutori.com/b3db5ed5-4b5c-48bb-b7ee-38365e02f18c
17. Internet and Computer Law Year in Review 2025–2026: AI Copyright Fair Use, the CDA Circuit Split, and the Age Verification Flood Gate, https://www.law.berkeley.edu/research/bclt/bclt-legal-analysis/internet-computer-law-s1/
18. AI SaaS agreement (customer friendly) - Practical Law, https://uk.practicallaw.thomsonreuters.com/w-048-8335?originationContext=knowHow&transition Type=Know How Item & context Data =%28sc.DocLink%29
19. TechLaw Blog — AI, SaaS, Privacy & Tech Law Insights | GalkinLaw, https://galkinlaw.com/blog/
20. Is per-seat SaaS structurally broken for advanced AI? The massive incentive paradox exposed in the recent Harvey vs Mike OSS debate.: r/legaltech - Reddit, https://www.reddit.com/r/legaltech/comments/1u13ueu/is_perseat_saas_structurally_broken_for_ advanced/