

CHARTING LEGAL LANDSCAPES

Navigating International Complexity, One Issue at a Time
by GC Law Firm

绘制法律图景

逐一应对国际复杂性。

GC律師事務所提供

Red Flags & Exit Strategy: Protecting Business in the Long Run

Preventing vendor lock-in and managing software litigation risks

警示信号与退出策略：长期保护企业商业利益

防止供应商锁定并管理软件诉讼风险



GIOVANNI CATANZARO
—
LAW FIRM

CHARTING LEGAL LANDSCAPES

may 2026

Navigating International Complexity, One Issue at a Time

by GC Law Firm



Abstract

The final phase of a Software-as-a-Service (SaaS) agreement dictates the long-term security of corporate digital assets. Managing advanced legal risks, defining interoperability rights, and establishing clear departure frameworks are essential to prevent operational paralysis and costly cross-border disputes.

Software-as-a-Service (SaaS) 协议的最终阶段决定了企业数字资产的长期安全。管理高级法律风险、明确互操作性权利并建立清晰的退出框架，对于防止业务瘫痪和昂贵的跨境纠纷至关重要。

- Key words:
- Decompilation
 - Vendor Lock-in
 - Escrow Agreement
 - Jurisdiction
 - GDPR
 - Portability.

Advanced Risk Management: Red Flags and Exit Strategies

高级风险管理：警示信号与退出策略

By GC Law

1. Decompilation Rights and Interoperability

1. 反编译权利与互操作性

Software reverse-engineering faces strict statutory boundaries, making precise contractual carve-outs mandatory for business continuity.

软件逆向工程上面临着严格的法律限制，这使得针对业务连续性的明确合同豁免条款成为核心必要。

Parameter 参数	Details and Implications 详情与影响
Statutory Limitations 法律限制	Decompilation is generally prohibited under IP law, but statutory exceptions exist solely to ensure interoperability between independent software systems. 知识产权法明确禁止反编译，但法律规定的例外情况仅限于确保独立软件系统之间的互操作性。
Red Flag Risks 警示信号风险	Clauses that entirely deny source code access during emergencies (e.g., provider insolvency) present massive operational risk if not mitigated by a source code escrow agreement. 在紧急情况下（如供应商破产）完全拒绝访问源代码的条款带来了巨大的运营风险，除

非通过源代码托管协议 (Escrow Agreement) 予以缓解。

2. Data Governance and Portability (GDPR Compliance)
2. 数据治理与数据可携权（遵循 GDPR）

Preventing critical technical dependencies requires a robust alignment with European privacy regulations and standardized data recovery paths.
防止关键技术依赖需要与欧洲隐私法规以及标准化的数据恢复路径保持紧密一致。

Dimension / 维度	Details and Implications 详情与影响
Privacy Framework 隐私框架	The SaaS provider operates strictly as a Data Processor under a Data Processing Agreement (DPA), binding them to strict operational boundaries (Art. 28 GDPR). SaaS 供应商在数据处理协议 (DPA) 下严格作为数据处理者运营，使其受到严格的运营边界约束 (GDPR 第 28 条)
Portability Rights 数据可携权	The client maintains the absolute right to export corporate data in structured, commonly used, and machine-readable formats (Art. 20 GDPR). 客户保留以结构化、常用且机器可读的格式导出企业数据的绝对权利 (GDPR 第 20 条).
Lock-in Prevention 防止锁定	Absent a comprehensive, pre-negotiated exit strategy and migration plan, the client risks becoming an operational "hostage" to the provider's infrastructure.

如果缺乏全面且预先协商的退出策略与迁移计划，客户将面临在业务运营上面临成为供应商基础设施“人质”的风险。

3. Litigation, Jurisdiction, and Emerging Trends.

3. 诉讼、管辖权与 2026 年新趋势

Cross-border tech contracts must resolve forum complexities and anticipate architectural disputes arising from advanced automation technologies.

跨境技术合同必须解决管辖法院的复杂性，并预测因先进自动化技术引起的架构争议。

Aspect 维度	Details and Implications 详情与影响
Forum Selection 管辖权选择	Overseas jurisdictions or costly international arbitration clauses (e.g., AAA for US-based providers, Luxembourg for EU operations) dramatically inflate litigation overheads. 海外管辖权或昂贵的国际仲裁条款（例如美国供应商指定的 AAA，欧盟业务指定的卢森堡）会急剧增加诉讼开支。
2026 Tech Horizons 2026 年技术前沿	The legal landscape sees an increase in litigation tied to integrated AI architectures, systemic algorithm failures, and liability for opaque data processing models. 法律领域中与嵌入式人工智能架构、系统性算法故障以及不透明数据处理模型的责任相关的诉讼呈上升趋势。

4. Strategic Recommendations and Conclusions

4. 战略建议与结论

Proactive corporate governance requires a continuous alignment of technical reality with contractual parameters.

前瞻性的企业治理要求技术现实与合同参数保持持续一致。

- *Systemic Audits: Organizations must conduct periodic, verified audits of SLA compliance to compile evidence prior to any contract scaling or termination phases.*

系统性审计：企业必须对SLA合规情况进行定期的、经过验证的审计，以便在任何合同扩展或终止阶段之前收集证据。

- *Algorithmic Transparency: Ensure explicit contractual transparency regarding how integrated AI components process, utilize, or retain sensitive corporate data layers.*

算法透明度：确保合同中对嵌入式人工智能组件如何处理、利用或保留敏感的企业数据层具有明确的透明度。

GC
GIOVANNI CATANZARO
—
LAW FIRM

Mail: info@gc-law-firm.com
Web: studioglegiogiovannicatanzaro.it
PEC: giovanni.catanzaro@venezia.pecavvocati.it
Mob: +39 333 88 80 834

Venezia
Via Alessandro Poerio, 27
30171 - Venezia Mestre
Tel/Fax: +39 041 456 14 88
Mail: venezia@gc-law-firm.com

Gorizia
Viale XXIV Maggio, 1
34170 - Gorizia
Tel/Fax: +39 0481 786733
Mail: gorizia@gc-law-firm.com

Dubai
48 Burj Gate, 10th Floor, room #1001
Downtown - Dubai (UAE)
Mob: +971 031 220 9859
Mail: dubai@gc-law-firm.com

Member of: **SC** **LA** **和** **INSTITUTION**

RESEARCH INSTITUTE OF ECONOMIC
OFFICE IN THE FIELD
INSTITUTE OF ECONOMIC RESEARCH