SLT/ SWISS LEGALTECH ASSOCIATION

LAW&TECH INSIGHTS MAGAZINE

2026-7

EVALUATING EXTERNAL AI TOOLS:

A practical framework for Swiss Businesses

By Brechtje Lindeboom, General Counsel SwissSign AG and Crystal Dubois, Attorney-at-Law at Bonnard Lawson

Editorial Team :

Nicolas Torrent, Ziyu Liu, Nomungerel Jamsranjav

www.swisslegaltech.ch

INTRODUCTION

AI tool adoption is accelerating inside companies. Marketing wants AI-powered content generation. HR wants automated resume screening. Sales wants contact enrichment platforms. Finance wants predictive analytics dashboards. A word of clarification: this article is not about generic AI assistants such as Claude, Co-Pilot, or ChatGPT. It is about the wider category of *specialized external AI tools*: applications that perform specific business functions driven by machine learning, from AI hiring screeners to contact enrichment databases and automated scoring systems.

For Swiss counsels, every adoption decision in this space simultaneously triggers obligations under the revised Federal Act on Data Protection (FADP)[1], the GDPR where applicable, the Swiss Code of Obligations, and increasingly under the EU AI Act[2]. Depending on the nature of the tool and the potential harm it could cause, product liability regimes may also be relevant[3].

The question is no longer *whether* AI tools will arrive on counsel's desk for sign-off, it is whether counsel will be ready with a structured evaluation framework when they do. This article proposes such a framework, surveys the leading international and domestic evaluation models, and distils the red flags that every lawyer should look for before approving any external AI tool deployment.

STEP-BY-STEP EVALUATION FRAMEWORK

When a business unit approaches counsel seeking approval to deploy an external AI tool, the following seven-step process provides a structured and documentable evaluation.

It is understood that not all contracts or terms of use offered by AI tool vendors can be negotiated, particularly where large platform providers offer standardized take-it-or-leave-it products[4]. This article focuses on those vendor relationships where negotiation is feasible, while also noting where counsel must document the conscious acceptance of a risk that cannot be contractually mitigated.

Step 1: INTAKE AND SCOPING

Before any legal analysis begins, counsel must understand **what the tool actually does.**

These are the typical questions counsel must address:

- What categories of data does it process such as personal, sensitive, biometric, employee data?
- Does it make, inform, or merely assist decisions?
- Is it customer-facing, employee-facing, or purely operational?
- Does the tool inform or automate decisions about individuals?
- Could its outputs be relied upon externally?

Many AI tools marketed as productivity solutions quietly process personal data at scale. Contact enrichment databases, AI hiring tools, and behavioral analytics platforms are typical examples where the data processing implications are underestimated at the point of purchase.

The VISCHER GAIRA tool provides a practical, freely available risk assessment framework for this initial scoping[5].

Step 2: LEGAL BASIS FOR DATA PROCESSING

Under both the FADP and the GDPR, every processing activity requires a valid legal basis. AI tools that enrich contact databases, profile employees, track website behavior, or automate scoring rarely qualify for a simple consent basis, given the scale and opacity of the processing involved. Counsel must assess whether legitimate interest is available, document that assessment, and ensure it withstands scrutiny; particularly where the tool processes data of individuals who have had no contact with the company.

Switzerland's Federal Data Protection and Information Commissioner has published guidance stressing that the mere fact that data is publicly accessible does not constitute a legal basis for AI- enabled repurposing[6].

Step 3: DATA TRANSFER AND LOCALIZATION RISKS

Most external AI tools rely on infrastructure operated by US-based vendors, which raises two distinct categories of risk.

The first is regulatory: cross-border data transfers trigger obligations under both the FADP and the GPDR (if applicable). For transfers governed by the FADP and GDPR, the Swiss-US Data Privacy Framework and the EU-US Data Privacy Framework provide an adequacy basis[7], but only where the specific vendor holds active DPF certification; a point counsel must verify on a case-by-case basis. Otherwise, Standard Contractual Clauses published by the EU Commission, and approved by the Federal Data Protection and Information Commissioner remain the primary transfer mechanism[8].

The second category is structural: routing data through foreign jurisdictions exposes it to the laws of those jurisdictions, including government access requests, and may compromise trade secrets or contractual confidentiality obligations that the company owes to its own clients or partners.

Step 4: AI-SPECIFIC RISK CLASSIFICATION

AI-specific risk classification matters since the greater the potential impact of an AI tools outputs on people's lives (e.g., their job prospects, their credit, their access to services) the more safeguards the law requires before that tool may be deployed.

The EU AI Act formalizes this logic through a tiered risk framework. High-risk AI systems under Annex III include systems used in employment and HR management, specifically recruitment, screening, evaluation and promotion decisions, as well as creditworthiness assessment and biometric categorization.

Swiss companies subject to the Act, who deploy those systems internally, must conduct a fundamental rights impact assessment for high-risk systems. Even for companies outside the EU AI Acts direct territorial scope, this classification is a useful calibration tool.

Step 5: VENDOR DUE DILIGENCE

The Data Processing Agreement is the central document. Counsel must review it for:

- Scope of processing;
- Sub-processor lists and notification obligations;
- Data deletion rights upon termination;
- Portability provisions; and
- Whether customer data is used to train or fine-tune the vendor's AI models. This last point is frequently buried in definitional language within Terms of Service rather than the DPA. A clause permitting model training on customer inputs violates the purpose limitation principle under both the GDPR and FADP and must be negotiated out or treated as an explicit accepted risk documented in the approval record.

Two further contractual issues warrant specific attention.

First, *IP rights in AI outputs:* counsel should verify whether the AI tools outputs — generated text, reports, recommendations — may be freely used by the company or whether the vendor imposes restrictions. Ideally, contracts should confirm that outputs belong to the customer.

Second, *transparency about AI in the vendors own supply chain:* a growing number of companies now require suppliers to sign an 'AI Annex' disclosing whether and how AI is used in the services or products they deliver.

Step 6: INTERNAL GOVERNANCE

Where processing of personal data is likely to result in high risk to data subjects' personality or fundamental rights a Data Protection Impact Assessment (DPIA) is mandatory under Art. 22 FADP and Art. 35 GDPR[9].

For HR-facing tools, transparency obligations toward employees arise under Art. 328b of the Swiss Code of Obligations[10], which restricts employers to processing employee personal data necessary for the employment relationship.

Where the AI tool produces decisions with significant effects on individuals, Art. 21 FADP and Art. 22 GDPR's restrictions on automated decision-making apply.

Internally within the company, a clear sign-off matrix is essential for auditability[11]. This means a documented record specifying:

- which individual or role is authorized to approve deployment of a given AI tool;
- which role is responsible for ongoing monitoring of the tool's outputs and compliance posture;
- which role holds the authority to revoke approval or decommission the tool if risks materialize.

This documentation creates an auditable governance trail required by the accountability obligation under Art. 5(2) GDPR and Art. 8 FADP and is critical evidence in any regulatory inquiry or data breach investigation.

Step 7: ONGOING MONITORING AND EXIT STRATEGY

Tool approval is not a one-time event. Counsel should establish review triggers linked to significant vendor updates, regulatory developments, or incident reports.

Contractual exit provisions must be reviewed before signature. Indeed, the right to export data, the right to request deletion, and the absence of onerous lock-in provisions are minimum requirements.

A vendor who cannot satisfy these conditions in negotiation signals a governance posture incompatible with responsible AI adoption.

EXISTING EVALUATION MODELS AND THEIR LIMITATIONS

THE EU AI ACT'S CONFORMITY ASSESSMENT

The EU AI Act is the world's first comprehensive horizontal legislative framework for AI governance, covering AI systems across all sectors and risk levels[12]. A word of comparative context is warranted: China has also been an early mover in AI regulation, adopting its Algorithmic Recommendations Rules in 2022 and Interim Measures for Generative AI Services in 2023. China's approach, however, is fundamentally different in character — it prioritizes state-supervised content alignment and national security over individual rights protection, and operates through sector-specific administrative guidelines rather than a cross-sectoral rights-based statute[13]. The EU AI Act therefore stands apart as the first framework to embed fundamental rights protections into binding, comprehensive AI governance at legislative level.

For high-risk AI systems, the Act mandates technical documentation, human oversight measures, transparency obligations toward affected persons, and in certain cases third-party conformity assessment.

Prof. Philipp Hacker has characterized the Act's liability architecture as a 'half-hearted approach' arguing that it contains no individually enforceable rights for affected persons, leaving enforcement entirely to regulatory authorities rather than injured parties[14]. In his January 2024 paper on the final trilogue text, Hacker further noted that the compliance timeline is compressed and the burden on companies — particularly SMEs — has been underestimated[15]. Separately, Hacker has criticized the Act's treatment of general-purpose AI systems (GPAIs) as inconsistent and underdeveloped relative to the risks these systems present across deployment contexts[16].

The European Commission has made available a number of free resources, such as the Single Information[17], to help stakeholders determine whether they are subject to legal obligations and understand the steps they need to take to comply.

INTERNATIONAL STANDARDS AND GOVERNANCE FRAMEWORKS

Beyond the EU AI Act, a growing body of international standards and governance frameworks provides practical benchmarks for evaluating AI tools. These are voluntary but increasingly used as calibration tools for due diligence and regulatory accountability.

ISO/IEC 42001:2023 is the world's first AI management system standard. Published in December 2023, it requires organizations to establish governance structures, risk management processes, and third-party supplier oversight across the AI lifecycle — following the same Plan-Do-Check-Act methodology as ISO 27001. For counsel evaluating a vendor, ISO 42001 certification is a meaningful governance signal. ISO 42001 sits within a broader family of AI-specific standards developed by ISO/IEC JTC 1/SC 42[18].

Counsel can identify which domain-specific standards apply to a given deployment — whether in healthcare, finance, or HR — by consulting the AI Standards Hub's searchable Standards Database[19], which currently covers over 500 standards from more than 15 international standards development organizations.

The NIST AI Risk Management Framework (AI RMF 1.0), released in January 2023, is a voluntary, flexible framework structured around four core functions — Govern, Map, Measure, and Manage[20]. Although a US instrument, it has become a globally referenced benchmark and is aligned with both ISO 42001 and the OECD AI Principles through published crosswalks. It provides a common language for assessing vendor governance representations, particularly when dealing with US-based providers.

The OECD AI Principles, first adopted in 2019 and updated in 2024, are the first intergovernmental standard on AI, covering transparency, accountability, robustness, and respect for human rights[21]. The EU AI Act and the NIST AI RMF both draw on the OECD's definitions, making these principles a useful normative anchor for cross-border evaluation.

Sector-specific guidance narrows these frameworks further. In the Swiss financial sector, FINMA published Guidance 08/2024 in December 2024[22], requiring supervised institutions to maintain an inventory of AI tools, assign clear accountabilities, ensure data quality, perform ongoing testing, and document processes — with the same expectations extending to third-party AI providers. Counsel should check whether equivalent guidance has been issued by the relevant sectoral regulator before completing any evaluation.

Effective AI governance requires a cross-functional internal team. IT and cybersecurity teams must be involved from the outset: AI tools introduce attack surfaces that go beyond conventional software vulnerabilities, including prompt injection, where malicious inputs manipulate AI outputs, and risks arising from the integration of third-party models into sensitive workflows. Business decision-makers must also be part of the process, both to define acceptable use boundaries and to own the organizational accountability that legal sign-off cannot substitute for.

KEY RED FLAGS: WHAT COUNSEL MUST WATCH FOR

When evaluating any external AI tool, the following issues should trigger elevated scrutiny or refusal:

1. **Model training on customer data.** The vendor's DPA or Terms of Service permit use of customer or user inputs to train, fine-tune, or improve AI models. This is often buried in definitional or 'service improvement' clauses.

2. **No data deletion mechanism.** The vendor cannot demonstrate a contractual, time-bound process for deleting all personal data upon contract termination.

3. **Black-box decision-making.** The tool produces consequential outputs — scoring, ranking, screening — with no explainability, audit trail, or human override mechanism.

4. **EU AI Act high-risk classification.** The tool falls within Annex III of the AI Act (HR and employment decisions, credit assessment, biometrics, critical infrastructure). This classification exists because these are the areas where AI tools carry the highest potential to harm fundamental rights — affecting someone's job, finances, or freedom. Falling into this category triggers mandatory fundamental rights impact assessments and human oversight obligations and demands correspondingly elevated scrutiny regardless of whether the EU AI Act formally applies to the deploying company.

5. **Invalid transfer mechanism.** The vendor is based in a third country without valid SCCs (Standard Contractual Clauses — model data transfer contracts approved by the European Commission), BCRs (Binding Corporate Rules — intra-group transfer codes approved by a data protection authority), or active DPF certification[23] covering the relevant data flows to the specific processing entity.

6. **DPA carve-outs for AI improvement.** The DPA contains carve-outs permitting use of Customer Personal Data for 'service development' or 'AI improvement'. This is a standard market practice that is legally problematic under the purpose limitation principle.

7. **Absence of transparency to data subjects.** Employees or customers affected by AI- informed decisions are not informed in advance, breaching Arts. 12-13 GDPR, Art. 19 FADP, and, for significant automated decisions, Art. 22 GDPR, Art.21 FDAP.

8. **No bias or fairness auditing.** The vendor cannot demonstrate any testing for discriminatory outputs, particularly where the tool informs employment or credit decisions.

9. **Onerous exit provisions.** Contractual terms prevent practical data portability or impose penalties that make exit disproportionately costly, prolonging exposure after a tool should be discontinued.

CONCLUSION

The role of counsel in AI governance has expanded well beyond legal compliance review.

Each external AI tool introduced into a company's operational ecosystem carries layered obligations: data protection, employment law, consumer protection, liability for third-party tool outputs, etc.

Only counsel is positioned to assess these in their totality. The frameworks reviewed here, the growing body of enforcement actions, and the scholarship of leading academics and practitioners converge on a single principle: the approval of an external AI tool is an act of institutional governance, not a formality.

Counsel who builds structured, documented evaluation processes, and who convene the right internal stakeholders to each deployment decision, will protect their organizations from exposure and, in doing so, define what responsible AI adoption actually looks like in practice.

This article reflects the authors' own views and does not constitute legal advice. The article was drafted with the assistance of generative AI and reviewed, verified, edited, and approved by the authors, who take full responsibility for its content, accuracy, and conclusions

REFERENCES

1. Swiss Federal Act on Data Protection (FADP), in force 1 September 2023
2. EU AI Act (Regulation (EU) 2024/1689), Official Journal of the EU, 12 July 2024
   The Act's extraterritorial scope (Art. 2) reaches Swiss companies whose AI systems are placed on the EU market or whose AI-generated outputs are used by persons located in the EU.
3. EU revised Product Liability Directive (Regulation (EU) 2024/2853) Expressly covers AI-enabled products and software. At Swiss level, the Swiss Product Liability Act (PrHG / SR 221.112.944) may also apply.
4. David Rosenthal / VISCHER, Part 15: What you should legally consider when retaining AI providers (VISCHER AI Blog Series)
5. David Rosenthal / VISCHER, Part 4: How to assess the risks of both small and large AI projects (VISCHER AI Blog Series)
6. Federal Data Protection and Information Commissioner AI and data protection and Conclusion of preliminary investigation X formerly Twitter: use of personal data for training the AI Grok
7. EU-US / Swiss-US Data Privacy Framework (DPF).
8. David Rosenthal (VISCHER), FAQ on the EU Standard Contractual Clauses and Transfer Impact Assessments (English, free PDF)
9. Art. 22 FADP (mandatory DPIA under Swiss law): Art. 35 GDPR (DPIA under EU law): https://gdpr-info.eu/art-35-gdpr/
10. Art. 328b Swiss Code of Obligations (OR/CO)
11. Auditability obligation arises from: Art. 5(2) GDPR (accountability principle); Art. 8 FADP; Art. 9 and Art. 12 EU AI Act (risk management and record-keeping for high-risk AI systems). The sign-off matrix specifies internally: who approves deployment, who monitors ongoing compliance, and who can revoke or decommission the tool.
12. Philipp Hacker, 'AI Regulation in Europe: From the AI Act to Future Regulatory Challenges'(2023) and EU AI Act: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
13. IAPP, 'Preparing for compliance: Key differences between EU, Chinese AI regulations'

14. Philipp Hacker, ‘The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future’ (2023) 51 Computer Law and Security Review 105871
15. Philipp Hacker, ‘Comments on the Final Trilogue Version of the AI Act’(January 2024)
16. Philipp Hacker, ‘What’s Missing from the EU AI Act’, Verfassungsblog (December 2023)
17. https://ai-act-service-desk.ec.europa.eu/en
18. https://www.iso.org/standard/42001
19. https://aistandardshub.org/ai-standards-search/
20. https://www.nist.gov/itl/ai-risk-management-framework
21. https://oecd.ai/en/ai-principles
22. https://www.finma.ch/en/news/2024/12/20241218-mm-finma-am-08-24/
23. SCCs: Standard Contractual Clauses (Art. 46 GDPR / Art. 16 FADP). BCRs: Binding Corporate Rules (Art. 47 GDPR). DPF: Swiss-US & EU-US Data Privacy Framework. See reference 7.