N
Monthly Newsletter September 2026

DISPUTE RESOLUTION

Schellenberg Wittmer

Maintaining Privilege in AI-assisted Internal Investigations

Charles Goumaz, Benjamin Borsodi, Louis Burrus, Clara Gehner

Key Take-aways

1.
Swiss law has no AI-specific privilege rules. Whether AI-generated investigation outputs are protected turns on counsel-directed legal analysis – a question Swiss courts have yet to resolve.

2.
Several regimes may apply cumulatively; privilege, data protection, and the blocking statute – each constraining how and where AI tools may be used.

3.
Privilege over AI outputs is won or lost before deployment. Poor governance produces unprotected, potentially discoverable investigation material at the worst possible moment.

1 Background

Artificial intelligence (**AI**) tools are increasingly being employed in **corporate internal investigations**. The primary drivers are practical: AI dramatically reduces first-pass document review times, identifies patterns in large datasets that human reviewers might miss, extracts key data points for tabular comparison, and rapidly produces structured interview records. In complex, multijurisdictional investigations spanning millions of documents, these advantages are material.

Yet deploying AI in investigations raises legal questions that Swiss law has not yet directly addressed. Chief among them is **legal privilege**: when AI tools generate investigation outputs – such as summaries, relevance flags, and interview transcripts – are those outputs protected from disclosure to criminal prosecutors, regulatory authorities, and adverse parties in civil proceedings? The answer, under current Swiss law, is uncertain.

2 Privilege for external counsel: the critical fault line

Swiss law protects **attorney-client privilege** through several overlapping regimes. Under Art. 321 of the Swiss Criminal Code (**SCC**), a lawyer or their auxiliary commits a criminal offense by disclosing confidential client information. Art. 13 of the Lawyers' Act (**LA**) provides that attorneys admitted to practice in Switzerland must keep all information that has been entrusted to them by their client, or prospective client, confidential. Procedurally, pursuant in particular to articles 160, 163 and 166 of the Swiss Civil Procedure Code (**CPC**), art. 171 and 264 of the Swiss Criminal Procedure Code (**CrimPC**) and art. 13, 16 and 17 of the Federal Act on Administrative Procedure (**APA**), a party to litigation (as well as non-parties to the litigation) has the right to refuse to produce privileged material in the proceedings; and on the same basis, an attorney and/or the client is also entitled to refuse to testify with respect to privileged information.

Swiss courts haven't ruled on privilege for AI-generated investigative outputs.

Under this framework, privilege protection is broad and depends on whether the work was performed within a legal mandate, at the direction of a qualified attorney, and in connection with the attorney's **typical professional activity** – namely, advising and representing clients in legal matters.

As a reminder, the Federal Supreme Court's recent case law has restricted the scope of an attorney's "typical professional activity" in the investigation context. Tasks performed in internal investigations – particularly those that are **primarily fact-gathering** rather than legal analysis – are not automatically considered the typical work of a lawyer.

Privilege Rule #1: Establish a formal legal mandate before activating any AI tool.

This is the critical fault line for AI-assisted investigation work, since none of these provisions were drafted with AI-generated outputs in mind. The statutory framework addresses communications between attorney and client – letters, memoranda, advice, instructions. It does not address outputs generated autonomously by a machine processing the client's data at counsel's direction. As a result, courts asked to determine whether an AI-generated document review summary or an interview transcript is privileged must work by analogy from principles developed for human-generated legal work.

Thus, the critical inquiry is not whether a human or AI generated the document, but who instructed the tool, in what capacity, and for what purpose. Consequently, when an attorney retains an AI-assisted review platform under a formal legal mandate to conduct an internal investigation, and the tool processes data **under that attorney's direction**, the resulting outputs should arguably constitute attorney work product. In this analysis, the tool serves as the lawyer's instrument rather than an independent actor.

That argument holds only so far as the chain of confidentiality is preserved: because the data is routed to a third-party provider, the outputs are likely to remain protected only where the provider can be treated as the lawyer's auxiliary – contractually bound to professional secrecy and technically barred from accessing or re-using the data – or where the tool runs in a closed, on-premise environment. A public platform used on consumer terms is unlikely to meet that threshold, and the disclosure to the provider may itself defeat the very secrecy the mandate was meant to protect.

Conversely, if an in-house compliance team, human resources department, or executive under investigation independently uses an AI tool – outside of a formal legal mandate and an attorney-client relationship – the tool's outputs will not attract privilege. In Swiss companies, employees routinely use AI tools to process sensitive data without legal oversight. This autonomous use, however well-intentioned, lacks legal protection.

3 The new in-House counsel privilege: narrower than it appears

On January 1, 2025, the revised CPC introduced a **limited in-house counsel privilege** under Art. 167a CPC. This privilege is subject to three cumulative conditions. First, the legal entity invoking the privilege must be registered in a commercial register. Second, a lawyer admitted to the bar in Switzerland or in their country of origin must head the company's internal legal department. Third, and most critically for AI-assisted investigations, the activity must fall within the typical scope of an attorney's professional activity – namely, legal advice and representation.

Two significant limitations apply. First, the new privilege applies **only in civil proceedings**. It provides no protection in criminal proceedings under the CrimPC, nor in regulatory enforcement proceedings before FINMA or other supervisory authorities. This is a fundamental constraint: Art. 167a CPC offers no shelter in the most serious corporate investigations.

Second, the **scope of "typical legal activity"** for in-house counsel remains contested under Swiss case law. Courts have indicated that operational tasks, compliance monitoring, and certain investigative fact-gathering activities may not qualify. When in-house counsel deploys an AI tool to classify documents or analyze misconduct, but compliance or management uses the output primarily for non-legal purposes rather than to prepare legal advice, the connection to a privileged activity weakens.

To mitigate the risk of creating detailed but unprotected analytical documents, Swiss companies must implement and enforce clear internal policies. These policies must specify that AI tools may only process investigation-related data within an approved, counsel-directed workflow. This restriction applies equally to consumer AI tools accessed through personal accounts and to corporate platforms.

Privilege Rule #2: Train all personnel with investigation roles on prohibited AI use.

---

4 FADP: AI Vendors as data processors

Under the revised Federal Act on Data Protection (**FADP**), **processing investigation data through a third-party AI vendor** constitutes a disclosure to a processor. This triggers obligations independent of legal privilege, and breaching them can undermine privilege arguments in two distinct ways.

The first obligation is to enter into a **data processing agreement** with the AI vendor governing its data-use purposes, required security measures, and – critically – whether it may use client data to train or improve its models. If the vendor uses investigation data to train its models, this may constitute a breach of professional secrecy, potentially waiving any privilege claim.

The second obligation is to **restrict personal data transfers to countries lacking adequate protection**, unless specific safeguards are in place. Because the FADP applies fully to AI-supported processing, transferring data to AI systems hosted outside Switzerland requires either an adequacy determination covering the recipient or appropriate safeguards, such as Standard Contractual Clauses adapted for Swiss requirements.

Privilege Rule #3: Require enterprise-grade contractual protections from AI vendors.

Since 15 September 2024 the United States benefits from a Swiss adequacy decision, but only for vendors self-certified under the Swiss-U.S. Data Privacy Framework (**DPF**); for any non-certified US recipient, Swiss-adapted SCCs remain necessary. Crucially, DPF adequacy is a data-protection mechanism only; it does not dispense with the foreign-lawful-access assessment required where the data is subject to professional secrecy, so a DPF-certified US vendor does not, on its own, resolve the data-residency concern addressed below.

An investigation team that uploads employee communications, HR records, or transaction data to a US-hosted AI platform without a compliant transfer mechanism may breach the FADP. This disclosure outside the privileged channel may ultimately destroy the very privilege the team seeks to preserve.

5 The "blocking statute": data residency as a hard constraint

Switzerland's primary **blocking statute**, Art. 271 SCC, prohibits performing or facilitating activities on Swiss territory on behalf of a foreign authority that Swiss law reserves for public officials, unless the Swiss federal government grants prior authorization. Additionally, Art. 273 SCC prohibits disclosing Swiss business and industrial secrets to a foreign government, while Art. 162 SCC penalizes disclosing third-party business secrets in breach of statutory or contractual confidentiality duties.

Privilege Rule #4: Maintain data residency in Switzerland for investigations with cross-border potential.

These provisions may apply when transferring investigation data – such as client relationships, business strategies, or commercial transactions – to a foreign AI vendor. Indeed, Art. 271 SCC, in particular, has been applied to lawyers who, while managing cross-border investigations, helped produce Swiss-located materials for foreign authorities outside official mutual legal or administrative assistance channels.

Storing or processing Swiss investigation data on a cloud-hosted AI platform with servers in the United States exposes that data to compelled foreign access, notably under the US Cloud Act; and should such data then be produced to a foreign authority outside the channels of mutual legal and administrative assistance, Art. 271 and 273 SCC may be engaged.

This risk is particularly acute in investigations with US DOJ or OFAC dimensions, given the extraterritorial reach of US authorities. Consequently, such investigation data must be stored and processed within Switzerland.

6 Conclusion

Using AI tools in corporate investigations offers significant advantages. Swiss companies and their counsel already use these tools; the key question is whether they deploy them within a legal framework that preserves the protections that make the investigation process viable.

The analysis points to a clear structural conclusion: protecting the privilege of AI-generated investigation outputs depends almost entirely on **decisions made before activating the tools**. The companies best positioned to navigate these constraints establish governance frameworks before an investigation begins. Engaging counsel before processing the first document, securing vendors under appropriate data protection terms, using Swiss-hosted servers, and strictly prohibiting autonomous AI use form the building blocks of a defensible position. Companies that invest in this framework will ensure that AI tools remain a powerful, legally protected component of their investigative capability. Those that do not may find themselves explaining, under the worst possible circumstances, why their investigation's key outputs enjoy no privilege at all.




Charles Goumaz
Partner, Geneva
Charles.Goumaz@swlegal.ch

Benjamin Borsodi
Partner, Geneva
Benjamin.Borsodi@swlegal.ch

Peter Burckhardt
Partner, Zurich
Peter.Burckhardt@swlegal.ch

Simone Nadelhofer
Partner, Zurich
Simone.Nadelhofer@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P.O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.com

Geneva
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.com

Singapore
Schellenberg Wittmer Pte Ltd
50 Raffles Place, #40-05
Singapore Land Tower
Singapore 048623
www.swlegal.sg