

Privacy Responsibilities Across Provider Agent Memory and Tools

A Shared Data Map and Rights Test for Managers

Phil Hatch | Akholi

October 23, 2026

Vendor privacy managers should trace personal information through the stores and tools an agent uses. A processing schedule becomes operational only when both firms can locate information, apply instructions, and evidence correction or deletion where required.

Map the Information Beyond the Conversation

The buyer's vendor privacy manager should require a data map that follows the outsourced workflow through retrieval, working context, persistent memory, logs, tools, and subcontractors. A conversation transcript describes only part of that path. Personal information may remain in a retrieval index or support log after the visible session closes.

Begin with one defined processing activity and a named data owner on each side. Record where information enters, which components can receive it, what each retains, and how it leaves. Distinguish case content from operational metadata and inferred information, because their purposes and retention needs may differ.

The ICO's agentic AI foresight report identifies unnecessary processing, broad purposes, supply-chain responsibility, and difficulty exercising information rights. It supports examining the architecture, while remaining a foresight product rather than a complete legal compliance test. Managers need to connect those concerns to the actual service design.¹

¹ Information Commissioner's Office, *ICO Tech Futures: Agentic AI* (Information Commissioner's Office, accessed October 23, 2026), executive summary and "The ICO's role," <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-agentic-ai>.

Connect Each Store to a Responsible Organization

For every store, identify who determines the processing purpose and relevant means, who operates it, and who can implement a rights request. The technical operator is not automatically the legal controller. A single provider can act in different roles for different activities, and the contract should reflect those facts.

The European Data Protection Board’s controller and processor guidance explains why actual decisions matter more than a label. It also expects processing agreements to contain concrete information about implementation rather than merely repeat the GDPR. The shared data map proposed here supplies operational detail for that legal assessment.²

The study describes evidence confined to each firm’s tools. In privacy operations, an equivalent gap would prevent the buyer from confirming whether a request reached every relevant store. The banking accounts motivate testing the chain; they do not establish privacy failure rates or legal breach in this service.³

Test a Rights Request Through the Whole Workflow

Figure 1 proposes a store-level test record. Use a synthetic identifier or a properly authorized request and follow it through the service. The test should establish where the information is found, what action is required, who performs it, and what evidence returns to the buyer. Protect the test data and results.

For correction, verify the relevant source and derived operational copies. Updating the source may not refresh a retrieval index or stored summary. For deletion where required, test whether an active agent can recreate the deleted entry from another retained source. A successful deletion message from one interface is not sufficient evidence.

Record legitimate limits separately. A legal hold, security investigation, or backup architecture may require restricted retention or delayed deletion. The record should identify the reason, access restrictions, expiry or review condition, and any required communication. Managers should not promise immediate deletion from every medium when the design cannot deliver it.

² European Data Protection Board, *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR* (European Data Protection Board, adopted July 7, 2021; version 2.1 corrected September 20, 2022), version 2.1, executive summary and part I, secs. 2–3, https://www.edpb.europa.eu/system/files/documents/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

³ Phil Hatch, *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*, version 1.8.2 (Akholi, forthcoming manuscript dated November 1, 2026), Part 2, sec. 5.1, “Agent Actions Visible Only Inside Each Firm’s Own Tools,” <https://doi.org/10.2139/ssrn.7164559>.

Figure 1. Test information rights at each retained store

Store or path	Manager decision	Test evidence
Source and retrieval	Correction and index refresh	Located records and updated retrieval
Persistent memory	Purpose scope and retention	Changed or removed operational memory
Tools and subcontractors	Recipient and assistance duties	Downstream action confirmation
Logs backups and holds	Justified restricted retention	Access limits and expiry conditions

Author's proposed operating framework. Adapt to the service and applicable jurisdiction; not an empirically validated standard.

Source: Phil Hatch, proposed framework developed for this paper.

Control Memory and Tool Changes

Persistent memory should have an approved purpose, scope, access model, and retention rule. The provider should distinguish memory needed for an active case from cross-case reuse. Adding a memory feature can change the processing even when the service description and model remain unchanged.

A new tool may introduce a new recipient, location, retention policy, or independent use. Require the provider to supply those facts before enabling it. The buyer's privacy and security owners should assess the change, update instructions, and determine whether notices, contracts, or transfer measures need revision.

Swiss guidance confirms that data protection applies to AI-supported processing, including transparency about purpose and data sources. That provides a separate Swiss reference. EU and UK activities need their own current legal assessment, including the UK's effective legislative changes; the shared map should preserve the differences.⁴

⁴ Federal Data Protection and Information Commissioner, "AI and Data Protection," Federal Data Protection and Information Commissioner, September 24, 2025, "Transparent information" and "Protection of fundamental rights," <https://www.edoeb.admin.ch/en/ai-and-data-protection>.

Make Retention and Exit Observable

The retention schedule should identify the trigger for each store: case closure, elapsed period, contract end, or another justified event. Assign an owner for failed jobs and exceptions. A scheduled deletion that repeatedly fails without escalation can leave the written policy unrelated to actual retention.

Test correction against derived information as well as the original field. A corrected customer address may leave an old address in a summary, retrieval index, scheduled communication, or delegated task. The manager should identify which copies require action and verify the result in the next permitted use. Where a retained record must remain unchanged for evidentiary reasons, restrict its operational reuse and preserve the reason for retention rather than overwrite history without explanation.

At exit, reconcile exported data, access withdrawal, active tasks, persistent memory, and retained copies. Require evidence of completed actions and explanations of authorized retention. Continuing rights assistance may be necessary after operational delivery ends, so the agreement should specify contacts, response expectations, and access to evidence.

Avoid collecting excessive content to prove compliance. A record of the request, affected stores, action result, responsible party, and protected evidence reference can be more appropriate than a second complete copy of the individual's information. Privacy assurance should not create an unnecessary new repository.

Accept the Map Only After a Working Test

The manager should review the completed map with privacy counsel, security, the process owner, and the provider. Unresolved stores or recipients should be treated as unresolved processing conditions. Limit the affected use while the parties establish purpose, responsibility, and enforceable instructions.

Repeat the rights test after material changes to memory, retrieval, tools, retention, or subcontractors. The result should show that the buyer can locate information and obtain the required action through the relationship. That evidence turns a processing schedule into a controllable operating model.

Evidence and Source Note

The study is a nonrepresentative cross-section of 850 vendor delivery-team respondents on 150 engagements serving Tier 1 financial institutions, collected during January–June 2026. Neither banks nor vendors corroborated the accounts. It establishes reported experience, not causation, legal breach, or market prevalence. Its application here is a mechanism to investigate, not an estimate of conditions in other industries. The author-supplied version 1.8.2 is dated November 1, 2026 and is cited as a forthcoming manuscript consulted October 23, 2026.⁵

This is an analytical decision paper based on the supplied study and selected primary public sources checked through October 23, 2026. The original contribution is a shared store-level data map and rights test, distinct from the executive purpose approval in AAO-003. The proposed method has not been independently validated. Legal requirements depend on the entity, activity, jurisdiction, and effective provisions; supervisory observations, research, and professional commentary have distinct authority.

Bibliography

European Data Protection Board. *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*.

European Data Protection Board, adopted July 7, 2021; version 2.1 corrected September 20, 2022.

[https://www.edpb.europa.eu/system/files/documents/2023-](https://www.edpb.europa.eu/system/files/documents/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf)

[10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf](https://www.edpb.europa.eu/system/files/documents/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf).

Federal Data Protection and Information Commissioner. “AI and Data Protection.” Federal Data Protection and Information Commissioner. September 24, 2025. <https://www.edoeb.admin.ch/en/ai-and-data-protection>.

Hatch, Phil. *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*. Version 1.8.2. Akholi.

Forthcoming manuscript dated November 1, 2026. Author-supplied manuscript consulted October 23, 2026.

<https://doi.org/10.2139/ssrn.7164559>.

Information Commissioner’s Office. *ICO Tech Futures: Agentic AI*. Information Commissioner’s Office, accessed October 23, 2026. <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-agentic-ai>.

⁵ Hatch, *Agentic AI Outsourcing*, Introduction, “Executive Summary” and “Evidentiary Basis and Its Limits.”