

Privacy Accountability Across the Buyer and Provider Agent Chain

An Executive Decision on Purpose and Responsibility

Phil Hatch | Akholi

October 23, 2026

Executives should approve a processing activity map before delegating work to provider agents. Responsibility follows the actual purposes and decisions in the chain, while contractual labels alone cannot establish who controls personal information.

Approve the Processing Purposes Before the Service

The chief privacy officer and executive sponsor should approve what the outsourced agent may do with personal information before authorizing the service. A broad instruction to improve customer service cannot settle whether the provider may retain conversation memory, infer sensitive characteristics, reuse cases for training, or send information to additional tools.

The decision should cover the complete chain of processing activities. Buying one service can involve different organizational roles for case handling, security logging, product improvement, and model training. Executives need a map showing those activities and the decisions each organization makes, rather than one label attached to the entire supplier relationship.

The European Data Protection Board explains that controller and processor roles depend on the actual determination of purposes and means. A processor that determines its own purposes may become a controller for that processing. The legal assessment should therefore examine conduct as well as the agreement.¹

¹ 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.

Find Where the Purpose Changes

Consider a hypothetical outsourced customer-service agent that retrieves account records, resolves a request, and remembers the interaction. Retrieval for the agreed service may have one justification; retaining a reusable profile for unrelated services creates another question. The fact that both activities occur in the same software does not make their purposes identical.

The provider should describe its own uses and the uses permitted to underlying suppliers. The buyer should distinguish necessary service processing from optional improvement, advertising, evaluation, or training. If a supplier cannot explain a use, management should exclude the relevant data or suspend that processing until the purpose and responsibility are resolved.

The ICO's agentic AI foresight report identifies broad purposes, unnecessary access, supply-chain roles, and information rights as emerging concerns. It is a forward-looking analysis, not an approval of deployment or a complete statement of current UK law. Its practical significance is that architecture and privacy accountability must be assessed together.²

Require an Executive Accountability Map

Figure 1 proposes the minimum decisions for approval. Each activity should identify the purpose, responsible organization, permitted data, receiving services, retention basis, and rights owner. The map should distinguish an agreed instruction from a provider choice that changes the processing purpose. Privacy counsel should assess the legal role for that activity.

The executive sponsor should resolve commercial and operational dependencies exposed by the map. A provider may require a particular store or tool to perform the service. The buyer must then decide whether that design fits its obligations and risk appetite, whether a different design is feasible, or whether the service should remain restricted.

The study's accounts of fragmented visibility between firms help explain why a contract schedule can drift from actual delivery. They do not establish a privacy violation. The appropriate use of that evidence is to require a trace from the approved processing description to observed data movements in the outsourced service.³

² 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>.

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. Privacy approval follows processing activities

Activity	Executive decision	Evidence required
Service delivery	Approve defined purpose and roles	Instructions and actual data path
Memory and reuse	Permit or prohibit each further use	Store policy and runtime configuration
Information rights	Assign response and assistance	End to end rights test
Exit and retention	Approve continuing duties	Export and retained copy record

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.

Preserve Local Rights in a Global Service

A common operating map should support separate EU, UK, Swiss, and other applicable legal conclusions. Switzerland's data protection commissioner states that the FADP applies to AI-supported processing and addresses transparency and high-risk impact assessment. Swiss obligations should be analyzed on their own terms rather than assumed identical to the GDPR.⁴

For the UK, counsel should check the effective provisions and guidance following the Data (Use and Access) Act. For EU activities, assess the relevant GDPR duties and the processing roles reflected in the facts. A shared global service can have different disclosure, transfer, retention, and decision-review requirements for different entities and individuals.

The approval record should explain how local requirements reach the runtime. A restriction written only in a country annex is ineffective if the agent cannot identify which cases it governs. Management should require reliable case routing and exception handling, with a named person responsible when jurisdiction or purpose is uncertain.

Make Rights and Exit Work Across the Chain

The buyer should select a synthetic or properly authorized case and test access, correction, deletion where applicable, and restrictions on further processing. The test should reach

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>.

relevant provider stores and underlying services. A response from the primary application cannot establish that a persistent memory entry or downstream copy was addressed.

The board need not approve every technical component. It should require management to resolve material purpose and responsibility decisions and report exceptions. The chief privacy officer can delegate routine implementation within that mandate while retaining escalation for new uses or unresolved rights. This division keeps executive attention on consequential choices and gives delivery teams a usable operating boundary instead of an obligation to return to the board for every ordinary configuration change.

Not every copy should be erased on the same schedule. Legal retention, security evidence, backups, and continuing disputes may require different treatment. The decision record should identify the reason, access restriction, expiry or review condition, and communication to the individual where required. Unsupported promises of immediate universal deletion create another accountability gap.

Exit deserves the same attention as onboarding. The firms should demonstrate export of necessary records, withdrawal of access, handling of retained copies, and continuing assistance with rights and investigations. The chief privacy officer should have an escalation route if the provider cannot produce the evidence needed to close the relationship responsibly.

Approve Bounded Processing and Review Material Change

The executive approval should identify allowed purposes, unresolved questions, and prohibited uses. A provider change that introduces a new purpose, store, recipient, or material inference should reopen the assessment. Management should fund the privacy work and technical controls together, because a legal instruction cannot compensate for a system unable to enforce it.

The proposed map gives executives a basis for deciding which processing they are authorizing and which evidence they require. Approval should remain conditional on the firms maintaining that explanation as delivery changes. Where the explanation fails, restrict the affected processing rather than assume the original supplier contract continues to cover it.

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 an executive processing activity map that connects purpose decisions to cross-firm evidence and change approval. 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.”