

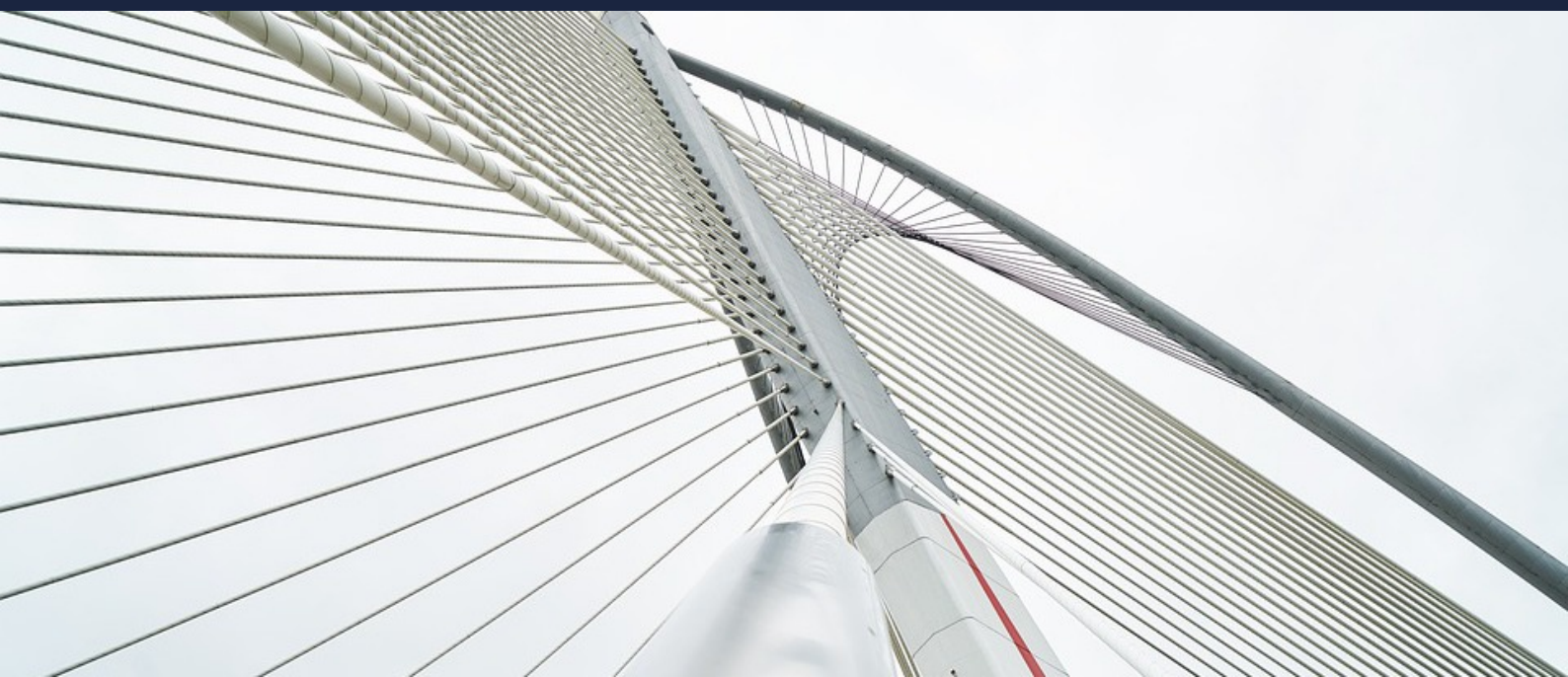
BEYOND THE DATA MODEL

Data Ownership — The Question Nobody Could Answer

A Practitioner's Perspective on Why Organisations Discovered That Data Governance Was a Political Problem, Not a Technical One

Giovanni Leonardi

February 2019



Data Ownership — The Question Nobody Could Answer

Leadership · No. 64

Originally written February 2019 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“When the regulator asked who owned the customer data, what they actually exposed was that nobody in the organisation had the authority, the incentive, or the courage to claim it.”

1. The Question That Broke the Room

It usually happens in a workshop. Someone — a regulator, an auditor, sometimes a newly appointed data protection officer with an inconvenient streak of diligence — asks the question: who owns this data?

The room goes quiet. Not because the answer is complicated, but because there is no answer. Or rather, there are several answers, all of them partial, none of them authoritative, and most of them designed to deflect responsibility rather than accept it.

The marketing director says the data belongs to marketing, because they collected it. The IT director says it belongs to IT, because they store it. The finance director says it belongs to the business, which is a way of saying it belongs to nobody. The chief data officer — if one exists — says it belongs to the organisation, which is a more sophisticated way of saying the same thing.

This scene has played out in every large organisation I have worked with over the past eighteen months. The arrival of GDPR did not create the data ownership problem, but it did something arguably more valuable: it made the problem impossible to ignore.

2. Why Ownership Matters Now

Data ownership has been a perennial topic in enterprise architecture and data management circles for decades. It has generated frameworks, maturity models, RACI matrices, and countless consultant presentations. And yet, in most organisations, the question remains functionally unanswered.

What changed in 2018 was the consequence of not answering it. When the GDPR came into force, the question of data ownership acquired regulatory teeth. The regulation does not use the language of ownership — it speaks of controllers and processors — but the

practical effect is the same. Someone must be accountable for every processing activity involving personal data. Someone must authorise it, document it, assess its risks, and respond when things go wrong.

The organisations that had clear data ownership were able to map their processing activities, complete their records of processing, and respond to data subject access requests with reasonable efficiency. The organisations that did not — which is to say, most of them — discovered that GDPR compliance was not primarily a legal or technical challenge. It was a political one.

3. The Politics of Data

Data ownership is political because data is power. The division that controls the customer database controls the customer relationship. The function that controls the management information controls the narrative. The team that controls the analytics platform controls the insight.

In most large organisations, these power dynamics have evolved organically over years, often decades. They are encoded in system architectures, in organisational structures, in budget allocations, and in the informal networks of influence that determine how things actually get done. They are deeply entrenched, and they resist disruption.

Asking who owns the data is, in this context, not a neutral question. It is a question about who has power, who should have power, and who is willing to accept the accountability that comes with it. The reason the room goes quiet is not confusion. It is self-preservation.

Data ownership frameworks fail not because they are technically inadequate, but because they attempt to resolve a political question through architectural means. The org chart is the real data model.

Consider the practical dynamics:

- The business unit that generates the data rarely wants to own it, because ownership implies cost, governance overhead, and accountability for quality.
- The IT function that stores the data emphatically does not want to own it, because ownership implies business accountability that IT has spent years trying to escape.
- The data management function that governs the data may want to own it in principle, but typically lacks the organisational authority to enforce ownership decisions.
- The C-suite, which should arbitrate ownership, rarely engages with the question because it appears technical, unglamorous, and difficult.

The result is an ownership vacuum — not because nobody cares, but because claiming ownership has more downside than upside for any individual leader.

4. The Stewardship Compromise

The most common organisational response to the ownership vacuum is the concept of data stewardship. Rather than resolving who owns the data, organisations appoint stewards — typically middle managers in business units — to take responsibility for data quality and governance within defined domains.

Stewardship is a pragmatic compromise, and in some organisations it works adequately. But it has a structural limitation: stewards are given responsibility without commensurate authority. They can identify data quality issues but cannot compel the changes needed to fix them. They can flag governance concerns but cannot override the business decisions that create them. They can document the problems but cannot solve them.

The stewardship model works when the issues are operational — a misspelled field, a duplicate record, a missing validation rule. It fails when the issues are strategic — a disagreement about whether customer data should be centralised or federated, a conflict between data sharing and data protection, a tension between commercial exploitation and ethical use.

These strategic questions require ownership in the full sense: the authority to make binding decisions, the budget to implement them, and the accountability for their consequences. Stewardship, by design, stops short of this.

5. What the Regulator Exposed

The most revealing aspect of GDPR's impact on data ownership has been the way regulatory enquiries have exposed the gap between formal governance and operational reality.

When a supervisory authority asks an organisation to demonstrate its lawful basis for a specific processing activity, the question cascades through the organisation in a way that reveals every weakness in the ownership structure. The data protection officer identifies the processing activity. The legal team assesses the lawful basis. But then someone must confirm the purpose of the processing — and that requires a business owner. Someone must confirm the data flows — and that requires IT. Someone must confirm the retention period — and that requires a policy that may not exist, or may exist but may not be followed.

The pattern I have observed is that organisations can typically answer the regulator's question for any individual processing activity, given enough time and effort. What they cannot do is answer it systematically, at scale, across the enterprise. The effort required to trace ownership for one processing activity is manageable; the effort required to trace it for hundreds or thousands is not sustainable without a fundamentally different approach to data governance.

“When the regulator asked who owned the customer data, what they actually exposed was that nobody in

the organisation had the authority, the incentive, or the courage to claim it.”

6. Towards a Workable Answer

If data ownership is fundamentally a political question, then the solution must be political, not architectural. This does not mean abandoning data governance frameworks; it means recognising that frameworks without executive mandate are diagrams, not governance.

The organisations I have seen make genuine progress on data ownership share a common characteristic: they have a senior leader — typically at board or executive committee level — who has accepted personal accountability for data as a strategic asset. Not a dotted-line accountability buried in a job description, but a visible, consequential accountability with associated objectives, resources, and reporting.

This leader does not need to be a technologist. In fact, the most effective data owners I have observed come from operational or commercial backgrounds, because they understand the business context in which data creates and destroys value. What they need is the authority to convene, to arbitrate, and to enforce — and the willingness to have the uncomfortable conversations about power that data ownership inevitably requires.

The practical elements that follow from this are straightforward, if not easy:

- A clear, published data ownership policy that assigns named owners to defined data domains, with explicit accountabilities.
- A governance forum with the authority to resolve ownership disputes — not an advisory committee, but a decision-making body with executive sponsorship.
- Incentive alignment: data ownership responsibilities reflected in performance objectives and bonus structures, so that ownership carries real consequences.
- Investment in the operational capability to exercise ownership — data quality tooling, metadata management, lineage tracking — so that owners can actually see and manage what they own.

None of this is novel. The data management profession has been advocating these elements for years. What has changed is the urgency. The regulatory environment no longer permits the luxury of treating data ownership as an aspirational maturity-model goal. It is now a compliance requirement, and the gap between aspiration and reality is where regulatory risk lives.

7. The Leadership Challenge

Ultimately, data ownership is a leadership problem. It requires leaders who are willing to claim accountability for something that is difficult to measure, expensive to govern, and certain to generate conflict. It requires organisations that are willing to treat data

governance as a strategic investment rather than a cost centre. And it requires boards that are willing to engage with data as a first-order strategic concern, not a technical detail to be delegated downward.

The GDPR era has made one thing clear: the question of data ownership will be answered. The only choice is whether it is answered deliberately, by leaders who understand its implications, or involuntarily, by regulators who have lost patience with the silence.