

BEYOND THE REPORTING LINE

The DPO Who Reported to Legal — Why GDPR Compliance Missed the Point

What a single reporting line reveals about the distance between data-protection compliance and genuine organisational change.

Giovanni Leonardi

July 2019



Contents

1. Executive Summary	3
2. The Tell on the Org Chart	3
3. Why Legal Was the Natural Home	4
4. What the Regulation Was Actually Asking For	4
5. How a Reporting Line Becomes a Ceiling	5
6. The Independence Paradox	6
7. The Case for Leaving It in Legal — and Its Limits	7
8. What a Better Answer Looks Like	7
9. The Wider Pattern	8

The DPO Who Reported to Legal — Why GDPR Compliance Missed the Point

Transformation · No. 229

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

“Where you place a capability is a statement about what kind of problem you think it is.”

1. Executive Summary

Twelve months after the General Data Protection Regulation took effect, most large organisations can demonstrate that they comply. They have appointed a Data Protection Officer, rewritten their privacy notices, assembled a register of processing activities, and worked through the backlog of consent re-permissioning. On paper, the programme is closed. And yet the change the regulation was reaching for — a shift in how organisations actually hold, move, and account for personal data — has, in a great many of them, not happened at all.

The reason is often visible in a single line on the organisation chart. In the majority of enterprises, the DPO was appointed into, or made to report through, the legal function. That choice was understandable and, on its own terms, defensible. But it quietly reframed a question about organisational design as a question about legal risk. A function built to make the organisation defensible will produce defensibility — not redesign. The reporting line was never a neutral administrative detail; it encoded a mental model, and the mental model set the ceiling of the response.

The deeper pattern has little to do with data protection specifically. It is what happens whenever a demand for transformation is received by a function whose reflexes then decide what the organisation is prepared to do about it. Understanding why compliance succeeded and change did not is, in the end, an essay about where you put things, and what that decision silently commits you to.

2. The Tell on the Org Chart

Picture the memo that circulated in the spring of last year, in some form, across thousands of organisations. A reorganisation, modest in appearance. A new box: Data Protection Officer. A reporting line, drawn with a certain relief, into the office of the General Counsel. The appointee was frequently a capable privacy lawyer, sometimes seconded from the legal team itself, occasionally hired in at pace as the deadline approached. The box was drawn, the statutory obligation discharged, and the organisation moved on to the next item on a very long list.

A year later, the same organisation can produce its evidence of compliance on request. What it often cannot do is answer a simple operational question with any confidence: where does a given customer's personal data actually live, and what would it take to find all of it? The privacy notice is immaculate. The underlying reality — the sprawl of systems, the copies in spreadsheets, the data pulled into a reporting warehouse years ago and never reconciled — is exactly as it was.

This is the tell. The regulation was satisfied at the level of documentation and left untouched at the level of architecture. And the line on the org chart is not merely a symptom of that gap; it is one of its causes. Where you place a capability is a statement about what kind of problem you think it is. Placed under the General Counsel, data protection was declared, before anyone wrote a word of policy, to be a legal problem. Everything that followed obeyed that declaration.

3. Why Legal Was the Natural Home

It would be too easy, and unfair, to treat the decision as negligence. The pull towards legal was strong, and much of it was rational.

The regulation reads like law, because it is law. Its language is the language of controllers and processors, lawful bases and legitimate interests, rights and obligations. Confronted with a text like that, an organisation reaches instinctively for the people fluent in it. The penalties, too, spoke in a register the legal and risk functions were built to hear: fines described as a share of global turnover concentrate the corporate mind, and they concentrate it on exposure. The General Counsel already owned the relationships with regulators, already ran the machinery of privilege and disclosure, already sat close enough to the board to raise an alarm. Housing the DPO there put the role near the authority it would sometimes need to invoke.

There was, further, a genuine competence argument. Much of the first year's work really was legal work — re-papering contracts with processors, constructing defensible consent mechanisms, interpreting guidance as it emerged. A DPO without ready access to that expertise would have struggled through the crush of the deadline.

The decision to house data protection in legal was not a mistake of competence. It was a mistake of framing — and framing mistakes are the hardest kind to see, because every individual action that follows from them looks entirely correct.

So the instinct was sound as far as it went. The difficulty is that it did not go far enough, and the very reasonableness of each step disguised where the sequence was leading.

4. What the Regulation Was Actually Asking For

Read past its legal surface and the regulation is, at heart, a demand about organisational design. Its centre of gravity is the accountability principle: the requirement not merely to

comply but to be able to demonstrate, on an ongoing basis, that you comply. That is not a drafting task. It is an operating-model task. It asks who is accountable for a given category of data, how that accountability is exercised, and what evidence the organisation can produce that its stated intentions and its actual behaviour are the same thing.

Look at the specific obligations in that light and the pattern is unmistakable. Data protection by design and by default asks that privacy considerations be built into systems and processes at the point they are conceived — an engineering and product discipline, not a review performed afterwards by someone with a red pen. The record of processing activities, done honestly, is a map of how data actually flows through the enterprise — a data-architecture artefact wearing a compliance label. The data protection impact assessment is a design gate. Data minimisation is a decision about what to collect and what to build. The right to erasure presumes that deletion is something the organisation's systems can actually perform.

Every one of these lives in the space where technology, operations, and process meet. None of them is discharged by a well-drafted notice. The regulation was asking organisations to change how they engineer their handling of personal data — and it dressed that demand in legal clothing, which is precisely how it came to be handed to the tailors.

“The regulation asked organisations to redesign how they handle data. Most heard a request to describe how they handle data — and description, however thorough, changes nothing.”

5. How a Reporting Line Becomes a Ceiling

A function optimises for the outcome it is measured on, and the legal function is measured on defensibility. Give data protection to legal and it will be pursued, diligently and intelligently, as an exercise in making the organisation defensible. That means documentation, paper trails, notices, contractual protection, and the ability to show a regulator a coherent account of intent. These are real and necessary things. They are also not the same thing as changing how data is handled, and the difference is where the programme quietly fails.

Consider a concrete case, composited from a recurring shape. An organisation completes its record of processing activities: more than three hundred processing activities, catalogued, owned, and signed off. A genuine achievement, months of work. Then, in the fourteenth month, a single subject access request arrives from a former customer. Answering it fully takes thirty-eight person-days spread across nine systems, because although every processing activity had been described, no one had been asked to make the data findable. The register documented the world without touching it. The same

organisation's retention schedule specifies, correctly, that certain records be deleted six years after a relationship ends — and its systems have no deletion mechanism at all, and have never deleted anything, because building one was an engineering commitment nobody in the compliance framing was positioned to demand.

The reporting line produced this. Not through any failure of effort, but because it pointed all that effort at the wrong surface.

Dimension	Compliance framing (data protection in legal)	Design framing (data protection in the operating model)
What "done" looks like	The documentation is complete and defensible	The data can actually be found, minimised, and deleted
Primary artefact	The privacy notice and the paper trail	The data flows and the systems that hold them
What it optimises for	Making the organisation defensible to a regulator	Changing how the organisation handles data
Who is expected to act	The DPO and the legal team	Product, engineering, and operations, with the DPO as conscience
What it leaves untouched	The architecture	Very little that matters

The table is a caricature, deliberately, but the caricature is recognisable. When the ceiling of the response is defensibility, the architecture is always what is left standing.

6. The Independence Paradox

There is a sharper irony still, and it lives in the regulation's own text. The DPO is granted a striking degree of statutory independence: the role must not receive instructions on how to perform its tasks, must not be penalised for doing so, must be free of conflicts of interest, and must report to the highest level of management. The intent is plain. The DPO is meant to be a source of independent judgement, able to tell the organisation things it would rather not hear.

Bury that role beneath the General Counsel and the independence begins to erode in ways no policy document acknowledges. The DPO's advice now flows upward through a filter whose professional instinct is to manage exposure and preserve privilege. The person meant to report to the highest level of management reports, in practice, to someone who reports to it. And a subtler conflict appears: the legal function's job is often to defend decisions already taken, while the DPO's job is sometimes to reopen them. Placing the second inside the first asks one set of loyalties to contain another.

Most organisations that made this choice would insist, sincerely, that their DPO is independent — and would point to the statute as proof. But independence is not only a legal status; it is a lived condition, shaped by who sets your objectives, who writes your appraisal, and whose discomfort you learn to anticipate. The org chart can honour the

letter of Article 38 while quietly draining its spirit.

7. The Case for Leaving It in Legal — and Its Limits

The strongest version of the counter-argument deserves a fair hearing, because it is not weak.

It runs like this. Regulatory expertise is scarce and genuinely resides in legal; a DPO cut off from it is worse, not better. The role's independence is protected by statute regardless of where the box sits, so the reporting line is a red herring. Much of the work — contracts, consent, regulatory correspondence — is irreducibly legal and belongs with lawyers. And for the great majority of organisations, too small to stand up a parallel data function, legal is simply the only home with the standing and the proximity to authority that the role requires. On this view, the reporting line is pragmatic, and the critics are chasing an ideal that most enterprises cannot afford.

Each of these points is true. None of them answers the objection. The failure described here was never a failure of legal competence — the legal work was, in most cases, done well. It was a failure of operating model: the reporting line determined what kind of authority the DPO could exercise, and authority over notices is not authority over architecture. The DPO who can veto a privacy statement but cannot require an engineering team to build a deletion capability has exactly the powers the compliance framing grants and none of the powers the design demand requires. Statutory independence, similarly, is necessary but not sufficient; a right not to be instructed is thin protection when your objectives, your budget, and your standing are all set from inside the function whose reflexes you are meant to challenge. And the resourcing argument, properly understood, points the other way: an organisation that cannot afford to redesign its data handling has not been let off the redesign — it has simply chosen to document the gap rather than close it.

The pragmatic case, in short, explains why the decision was made. It does not establish that the decision worked.

8. What a Better Answer Looks Like

The corrective is not a new box in a different place, drawn with the same confidence that drew the last one. It is a change in what the role is for.

Treat data protection as a design discipline rather than a compliance obligation and several things follow. The DPO's centre of gravity moves towards the places where data is architected — into the conversations about what systems collect, how they store, and whether they can delete — rather than the places where data handling is described after the fact. The accountability principle becomes an operating reality: named owners for categories of data, exercising real authority over how that data is treated, with the DPO as the independent conscience holding them to it rather than the sole party responsible for it. The reporting line runs high enough, and clear enough of conflicting loyalties, that the role's statutory independence is a lived condition and not merely a clause. And where

a Chief Data Officer exists, the relationship between the two is worked out deliberately — the one accountable for making data valuable, the other for making it lawful and safe, neither subordinate to the other's instincts.

I have watched the difference this makes turn on something as small as which meetings the DPO is in the room for. When the role is present at the point where a system is designed, minimisation and deletion are cheap, because they are built in. When it arrives afterwards, they are expensive or impossible, because they must be retrofitted into architecture that never anticipated them. The whole economics of data protection is decided upstream, and the reporting line determines whether the DPO is upstream or down.

Data protection is decided at the point of design, not the point of documentation. Where the organisation places the role determines which of those two points it can actually reach.

None of this is free of tension, and it would be dishonest to pretend otherwise. A DPO embedded in design risks capture by the very teams whose work must be challenged; a DPO held apart to preserve independence risks irrelevance. The balance between embeddedness and independence is genuinely difficult, and no org chart resolves it permanently. But it is the right difficulty to be wrestling with. The compliance framing spared organisations that struggle by never engaging it — and left the architecture untouched as the price.

9. The Wider Pattern

Step back from data protection and the shape of the story is familiar. An external demand for change arrives at the organisation's boundary. It is handed to whichever function its surface most resembles. And that function, doing its honest best, translates the demand into its own vocabulary — after which the vocabulary, not the original intent, governs what gets done. Security handed wholly to the technology function becomes a matter of tools rather than behaviour. A demand for genuine inclusion handed wholly to human resources becomes a matter of process compliance. Data protection handed to legal became a matter of defensibility. In each case the receiving function's reflexes, entirely reasonable in themselves, quietly set the ceiling of the response.

This is why the reporting line deserves more attention than it usually receives. It is one of the earliest and most consequential decisions an organisation makes about a transformation, and it is almost always made administratively, in the first days, before anyone has thought hard about what the change actually requires. By the time the limits of the framing become visible, the framing has hardened into structure, budgets, and careers, and is far more difficult to move than a line on a chart ever should be.

The lesson is not that legal was the wrong home in some absolute sense; for parts of the work, it was exactly right. The lesson is that the placement decision is a design decision in its own right, and that it should be made by asking what kind of problem this really is — not what kind of problem it superficially resembles. The organisations that closed the gap

between the regulation's intent and their own reality were, almost without exception, the ones that understood early that they had been handed an organisational-design problem wearing a lawyer's clothes. The rest are compliant, and unchanged, and increasingly aware that those are not the same thing.