

BEYOND THE REPORTING LINE

The DPO Who Reported to Legal

One year into the regulation, where organisations placed their Data Protection Officer revealed whether they had understood it at all

Giovanni Leonardi

May 2019



The DPO Who Reported to Legal

Transformation · No. 228

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

“Placing the DPO inside legal put the accountability function exactly where it could see the least.”

1. The line on the org chart

The email went round on a Tuesday. The organisation was pleased to announce that, in line with new regulatory requirements, the Deputy General Counsel would be taking on the role of Data Protection Officer, effective immediately, alongside her existing responsibilities. A paragraph of reassurance followed: robust processes, external counsel on hand, full confidence in the arrangements. Then everyone went back to work.

I have read a version of that email in more organisations than I can count, and the striking thing is how little the wording varied. The name changed; the shape did not. A senior lawyer, already busy, absorbs a statutory title. The role is announced as a compliance appointment and slotted into the legal function, reporting to the General Counsel. A box is ticked. And in the placing of that one box — who the Data Protection Officer is, and to whom they report — you can read almost everything about whether the organisation understood what the General Data Protection Regulation actually asked of it.

Twelve months on from the regulation coming into force, that is my contention: the reporting line was the diagnosis. Where an organisation put its DPO told you, more reliably than any policy document or any wall of freshly written procedures, whether it had grasped that this was a question of organisational design rather than a question of law.

2. Why legal was the obvious home — and why that was the error

The instinct to house data protection in the legal function is easy to understand. GDPR arrived wrapped in the language of law: articles and recitals, lawful bases, penalties expressed as a share of global turnover large enough to frighten a board. It reads like a statute, so it was received as one. And legal departments exist precisely to receive statutes — to interpret obligations, to weigh regulatory risk, to stand between the organisation and a penalty. Handing the regulation to the lawyers felt not merely defensible but responsible.

The error is quiet, and it is an error of category. A statute of the older kind tells you what you may not do, and legal's job is to keep you the right side of the line. GDPR did something different. Through the accountability principle it made the organisation responsible not only for obeying the rules but for being able to demonstrate,

continuously, that the way it collected, used, shared and retained personal data was lawful, proportionate and designed with the person behind the record in mind. That is not a line to stay behind. It is a property that has to be built into thousands of ordinary decisions — which fields a form captures, how long a log is kept, whether a new supplier arrangement needs a data-sharing agreement, what a product team may do with the behavioural data it has quietly started collecting.

Those decisions are not made in the legal department. They are made in product, in marketing, in operations, in the data teams — usually at speed, usually without anyone pausing to consult a lawyer. A function that sits at the end of the process, answering is this allowed? once the design is already set, is structurally too late. GDPR needed someone in the room when purposes were decided, not someone informed when the contract was already drafted. Placing the DPO inside legal put the accountability function exactly where it could see the least.

The accountability principle did not ask the organisation to obey a rule. It asked the organisation to be able to prove, at any moment, that it had thought — and to have thought early enough for the thinking to change anything.

3. Independence is a position, not a paragraph

The regulation was unusually specific about the DPO. The role was to be independent, free from instruction on how to carry out its tasks, protected from dismissal for carrying them out, and — the part most often waved through — free of any conflict of interest. A DPO could not also be the person who determined the purposes and means of processing. That is why a Head of Marketing or a Head of IT could not credibly wear the hat: they would be marking their own homework.

Reporting into legal rarely triggered the same alarm, and it should have. The conflict there is subtler, but it is real. A legal function under a General Counsel is oriented, quite correctly, toward defending the organisation — toward what can be justified if challenged, what will survive a regulator's inquiry, what keeps the penalty at bay. That is a litigation-defence logic, and it is not the same as a data-protection logic. Data protection, done properly, sometimes asks the organisation to collect less than it lawfully could, to delete data it would rather keep, to forgo a use that is defensible but not respectful of the individual. A DPO whose reporting line runs through the organisation's chief defender will, over time, absorb the defender's instincts. The independence the regulation demanded was never a paragraph in a job description or a dotted line drawn to the board on a chart. It was a position in the flow of decisions — and a reporting line into legal quietly compromised it.

4. What the org chart actually produced

Let me make this concrete, because the abstraction flatters everyone involved. Consider the arrangement I have watched play out again and again: a DPO drawn from within the

legal team, sitting three layers below the executive, covering an organisation of several thousand people, with the role formally scoped at perhaps two days a week on top of an existing legal workload. Over a year that organisation makes dozens of consequential decisions about personal data — a new customer-analytics capability, a loyalty scheme, a support centre moved offshore, a marketing platform that enriches its records from third-party sources.

The DPO is genuinely consulted on a handful of them. Not through anyone's bad faith — simply because the role sits outside the paths those decisions travel along. The rest surface later, and often the way they surface is the whole story: not in a design review, but in a subject access request months after the fact, when a customer asks for a copy of their data and the answer reveals a data flow nobody had entered in the record of processing the regulation required. The DPO learns of the organisation's own processing from the evidence assembled to satisfy an outsider. That is not a person failing at their job. That is an org chart working exactly as it was drawn.

“Put the accountability function two days a week and three layers down, and you have not created accountability. You have created somewhere to file the paperwork after the decision is already made.”

5. The strongest case for the lawyers — and why it still fails

The serious objection deserves a serious hearing, because it is not foolish. Data protection, the argument runs, is a specialist legal discipline. Someone has to read the regulation, follow the guidance issuing from the supervisory authorities, interpret consent and legitimate interest, judge when an impact assessment is required. Who better than a lawyer? And the independence requirement, the argument continues, can be met structurally — a formal reporting line to the highest level of management, a guarantee against dismissal — without uprooting the person from the function where the expertise already lives. On this reading, putting the DPO in legal is not a misunderstanding at all; it is the natural home for a legal role, with independence bolted on.

I take the point about expertise, and I would not staff the role with someone who cannot read the regulation. But the objection mistakes the smaller part of the job for the whole of it. The legal interpretation was, in practice, the least of the work. The guidance settled; the hard questions of lawful basis were, for most organisations, answered once and then reused. What did not settle, and what actually consumed the role, was operational: getting data protection considered early, keeping the record of processing honest as the business kept changing shape, making sure a hundred teams who had never read a recital in their lives designed with the person in mind. That is not legal interpretation. It is organisational plumbing, and it required standing in the flow of decisions rather than proximity to the case law. A dotted line to the board does not put you in that flow. Where

you actually sit does.

6. Reading the chart a year on

None of this argues that the DPO should have been handed a grand title or a large empire. Accountability is not a matter of headcount, and the organisations that treated the role as an internal regulator to be feared tended to get the worst of both worlds. It is a matter of position — of whether the person charged with data protection could see decisions as they were being taken and had the standing to shape them before they hardened. Some of the organisations that understood this best gave the role no fanfare at all. They simply made sure the DPO was present where data was designed into products and written into partnerships, reported cleanly to the top rather than through a function with an agenda of its own, and was judged on whether the organisation thought early rather than on whether it stayed out of trouble.

A year in, you did not need to audit an organisation to guess how seriously it had taken any of this. You needed only to look at the chart and ask two questions: who is the DPO, and to whom do they report. If the answer was a busy lawyer reporting to the General Counsel, the organisation had told you, without meaning to, that it still believed the regulation was a law to be complied with rather than a way of working to be built. The rules had been in force for twelve months. The harder question — the one the reporting line was quietly answering on everyone's behalf — was whether anything about how the organisation actually decided had changed at all.