

BEYOND DOCUMENTED COMPLIANCE

# Documented Everything, Changed Nothing

One year into GDPR, why the organisations that documented everything changed almost nothing

Giovanni Leonardi

July 2019



# Contents

|                                                           |   |
|-----------------------------------------------------------|---|
| 1. Executive Summary                                      | 3 |
| 2. A Programme That Finished, and a Practice That Did Not | 3 |
| 3. The Comfortable Home                                   | 4 |
| 4. What Independence Was Meant to Mean                    | 4 |
| 5. The Artefact and the Reality                           | 5 |
| 6. The Case for Legal, Taken Seriously                    | 6 |
| 7. What the Misplacement Cost                             | 7 |
| 8. The Mirror the Regulation Held Up                      | 8 |
| 9. A Year In                                              | 8 |

# Documented Everything, Changed Nothing

Transformation · No. 282

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

---

*“The artefact said yes; the reality had never learned the word no.”*

---

## 1. Executive Summary

---

A year on from the twenty-fifth of May 2018, almost every large organisation can produce the evidence of its compliance. The records of processing are written. The privacy notices have been rewritten in the plainer language the regulation asked for. Consent is captured, somewhere, in some form. A Data Protection Officer has been appointed, and the appointment letter is on file. What far fewer organisations can honestly say is that the way they collect, hold, share and reason about personal data is materially different from the way it was two years ago.

This essay argues that these two facts — the completeness of the paperwork and the persistence of the old habits — are the same fact seen from two sides, and that the join between them is visible in a detail most programmes treated as administrative: where the DPO was made to sit, and to whom that person reported. In a great many organisations the answer was identical. The DPO reported to the General Counsel, or to a head of compliance who reported to the General Counsel, and the regulation was thereby filed under law. Once filed under law, it became a thing to be satisfied rather than a thing to be absorbed. The documents were produced, the risk was logged, and the data went on moving exactly as before.

The placement was not a clerical accident. It expressed a genuine and defensible reading of what the General Data Protection Regulation was. This essay takes that reading seriously before setting out why, a year into the new regime, it looks increasingly like the reason so much effort has changed so little.

## 2. A Programme That Finished, and a Practice That Did Not

---

Picture the closing meeting of a readiness programme in the late spring of 2018. The slide is green. Every workstream has reported complete. The Article 30 records of processing exist. The privacy notices are live. The consent banner is deployed. The DPO has been designated and the notification lodged with the supervisory authority. Somebody thanks the programme team, the budget line is closed, and the temporary hires drift back to the agencies they came from. On the twenty-fifth of May the organisation is, by every measure the programme was given, compliant.

Return to that same organisation a year later and the striking thing is how little of the data itself has moved. The marketing function still holds the lists it held before, enriched from the same third parties, scored by the same models. The same twelve systems hold overlapping copies of the same customers, and no two of them agree. A subject who withdrew consent in one channel is still being processed in three others, because withdrawal was captured but never propagated. The records of processing — that heroic spreadsheet of some sixteen hundred activities, assembled by consultants over eight weeks in the spring — has not been opened since it was signed off. It was produced as a deliverable, not as a map anyone intended to navigate by.

Nothing here is a failure of effort. The effort was enormous. It is a failure of framing, and the framing was set, quietly and early, by an organisational decision that almost nobody debated: the regulation belonged to the lawyers, and so the person who owned it would sit among them.

### 3. The Comfortable Home

---

It is worth being fair about why legal was the natural home. The regulation reads like law because it is law. Its language is the language of obligations and derogations, of controllers and processors, of lawful bases and legitimate interests balanced against the rights and freedoms of the data subject. When a document is written in that register, the instinct of any well-run organisation is to hand it to the people fluent in that register. Lawyers read statutes for a living. They are comfortable with ambiguity that must be interpreted rather than resolved, and the regulation is full of it.

There was a second, quieter reason. The headline the whole programme was organised around was the fine: up to four per cent of global annual turnover, or twenty million euros, whichever is higher. A number of that size does not read as an operational matter. It reads as a risk, and risk of that magnitude belongs, by long convention, in the part of the organisation that manages legal and regulatory exposure. The DPO became, in effect, the custodian of a liability. And a custodian of liability is measured by whether the liability crystallises — by whether the fine lands — not by whether the underlying practice improves.

So the role went to legal, and with it went the frame. The question the organisation had learned to ask was: are we compliant? It is a lawyer's question, and it has a lawyer's answer — a defensible position, a documented basis, a file that would stand up. It is not the same question as: do we govern our data? The tragedy of the past year is that a great many organisations answered the first question well and never noticed they had stopped asking the second.

### 4. What Independence Was Meant to Mean

---

The regulation itself anticipated some of this, though not, perhaps, the form it would take. Article 38 is unusually specific about the position of the DPO. The officer must be involved properly and in a timely manner in all matters relating to the protection of personal data. The officer must not receive instructions regarding the exercise of those

tasks, must not be dismissed or penalised for performing them, and — the phrase that matters most here — must "directly report to the highest management level" of the organisation.

Read plainly, that last requirement sits awkwardly with a reporting line that runs into the General Counsel, who reports to the chief executive, who reports to the board. A DPO two or three removes from the highest management level is not, in the ordinary meaning of the words, directly reporting to it. The regulation wanted the role wired straight to the top precisely so that it could not be filtered, softened or deprioritised by an intervening function with its own agenda.

The Article 29 Working Party saw the other half of the problem before the regulation even took effect. Its guidance on Data Protection Officers, issued in December 2016 and revised the following spring, warned in terms that the role could not be combined with a position that determines the purposes and means of processing. It named the likely offenders directly: chief executive, chief operating officer, head of marketing, head of human resources, head of IT — and, tellingly, head of legal. The concern was conflict of interest. A person who both advises the business on how to process data and independently oversees whether that processing is lawful cannot do the second job honestly if the first job is where their loyalty and their career sit.

*"Independence" in the regulation was meant to protect the DPO's judgement from the organisation's convenience. In practice, reporting into legal too often produced the opposite: an independence of location — a role sealed off in a specialist function — that left the officer with authority over documents and none over the data.*

That distinction — independence of judgement versus independence of location — is the hinge of the whole matter. What the drafters wanted was a voice that could not be overruled on the substance. What many organisations delivered was a voice that could not reach the substance at all, because it had been placed where the substance was not decided. Legal does not choose which data the marketing function collects, or how long the operations function keeps it, or whether the analytics team builds a model on it. Those choices are made elsewhere, every day, by people who never see the DPO and were never asked to.

## 5. The Artefact and the Reality

There is a particular kind of document the past year has produced in enormous quantities, and it deserves a name. Call it the compliance artefact: a record, produced to demonstrate that an obligation has been met, whose production is complete once it exists. The Article 30 record is the purest example. It is required. It is real work to assemble. And in the great majority of organisations it is a photograph taken once, framed, and hung on a wall nobody walks past.

The reason the artefact and the reality drift apart is mechanical, not moral. A record of processing describes the state of the world on the day it was written. The world does not stop. A new supplier is onboarded, a new dataset is acquired, a team spins up a proof of

concept on a copy of the customer file — and none of it flows back into the document, because the document was owned by a function that does not sit in the path of those decisions. The DPO in legal learns of the new processing when something goes wrong, if then. The record and the reality were the same on the twenty-fifth of May 2018 and have been diverging quietly ever since.

This is the deeper sense in which compliance missed the point. The regulation's true instrument is not any single article but the accountability principle that runs through all of them: the requirement not merely to comply but to be able to demonstrate compliance, continuously, as an ongoing property of the organisation. Accountability of that kind is an operational capability. It lives in the systems, the data flows, the decision gates where new processing is proposed. It cannot be discharged by a specialist holding a folder. And a role positioned to hold the folder rather than to stand in the flow was, structurally, never going to deliver it.

---

*“A compliance programme can be finished. Governing data cannot; it is a practice, not a project, and a practice has to live where the work is done.”*

---

## 6. The Case for Legal, Taken Seriously

---

It would be too easy to leave it there, as though the organisations that placed their DPO in legal had simply blundered. They had not. There is a serious case for that placement, and it has to be met on its strongest terms rather than a caricature.

The first argument is competence. Somebody in the organisation has to be able to read the regulation as law — to weigh whether legitimate interest can carry a particular processing activity, to construct the balancing test, to judge when a Data Protection Impact Assessment tips into the territory that requires prior consultation with the regulator. That is legal work, and it needs a legal mind. Placing the DPO anywhere else risks the law being read by amateurs.

The second is privilege and candour. Advice that sits within the legal function can, in some jurisdictions and some circumstances, attract legal professional privilege. An organisation is more willing to examine its own weaknesses honestly when the examination is protected. Push the DPO out into the business and you may lose the confidential space in which uncomfortable truths can be surfaced and fixed before a regulator ever sees them.

The third is simply that the regulator itself thinks in legal terms. When the supervisory authority comes, it comes asking about lawful bases and documented decisions. Facing a legal interlocutor with a legal counterpart is not obviously wrong.

Each of these is true. None of them, on inspection, actually argues for the DPO reporting into legal — and that is the distinction the past year has blurred. The organisation

certainly needs legal competence applied to data protection; it does not follow that the person accountable for whether data is governed should be a subordinate of the person accountable for legal risk. Privilege protects advice; it does not require that the officer overseeing the whole practice be housed inside the advisory function, and where privilege becomes the reason the DPO's findings never leave the legal team, it has become part of the problem. And meeting the regulator in its own language is a task for an afternoon, not an organising principle for a role that has to shape behaviour across the entire enterprise every other day of the year.

The steelman, in short, establishes that legal must be involved. It does not establish that legal should be in charge. Those two claims were conflated, and the conflation is most of what went wrong.

## 7. What the Misplacement Cost

Abstraction can only carry this so far; the cost is concrete, and it is worth making it concrete. Consider a composite drawn from the recognisable shape of many organisations over the past year — no single one, but true to all of them.

The consent banner went live on the website in May 2018 and, on the numbers, worked beautifully: some ninety-seven per cent of visitors clicked accept. The figure was reported upward as a success. What the figure concealed was that acceptance was captured at the front door and never wired to anything behind it. When a customer later exercised the right to withdraw, the withdrawal was recorded in the consent system and propagated to none of the twelve downstream platforms that actually held and used the record. The organisation could show, on demand, that it had asked for consent. It could not show that consent, once refused, changed what happened to the data. The artefact said yes; the reality had never learned the word no.

Alongside it sat the subject access request. The regulation gives the individual the right to a copy of their data and gives the organisation one month to provide it. The requests arrived — a slow trickle at first, then a steadier flow as awareness grew through the year — and landed on a team of two, sitting in legal, with no automated means of retrieving a single person's data from those same twelve systems. Each request became a manual archaeology across the estate. The thirty-day clock ran hot. A backlog formed. And the backlog was invisible to the board, because the metric the board had been given was are we compliant — to which the answer, technically, remained yes, right up until the day it very publicly would not be.

Here is the mechanism laid bare. Every one of these failures was a failure of flow — of consent that did not flow, of data that could not be gathered back, of a record that did not keep pace with reality. Flow is an operational property. The role that might have owned it had been placed in the one function that stands outside the flow by design. The organisation had bought itself an expert in the law of data protection and left itself with no one accountable for the practice of it.

| Compliance framing (DPO in legal)        | Governance framing (DPO wired to the flow)                        |
|------------------------------------------|-------------------------------------------------------------------|
| Question asked: are we compliant?        | Question asked: do we govern our data?                            |
| Core artefact: the record, produced once | Core artefact: the data flow, maintained continuously             |
| Success measured by: absence of a fine   | Success measured by: data behaving as the individual was promised |
| Role's real authority: over documents    | Role's real authority: over decisions about data                  |
| Time horizon: the twenty-fifth of May    | Time horizon: every day after it                                  |

### 8. The Mirror the Regulation Held Up

Step back from data protection specifically and a more general pattern comes into view, one that anyone who has watched large-scale change will recognise. A regulation of this kind does not merely impose obligations; it holds a mirror to the organisation and shows, unforgivingly, how that organisation is actually put together. Where a firm was already clear about what data it held and why, the regulation was demanding but coherent. Where a firm did not know what it held – where ownership of data was contested or simply absent – the regulation exposed the vacancy, and the organisation reached, as organisations under pressure always do, for the response that felt safest rather than the one that would actually have worked.

Filing the whole thing under legal was that safe response. It converted an unbounded organisational question – who is accountable for our data, and how would we know if we were mishandling it? – into a bounded legal one – can we defend our position? The bounded question is answerable, and being answerable, it is comforting. But comfort was the wrong objective. The regulation was, read generously, an invitation to build a capability the organisation had always lacked and had always half-known it lacked. Treated as a compliance exercise, the invitation was declined without anyone quite deciding to decline it.

This is why the reporting line of one role turns out to carry so much weight. It was never really about the DPO as an individual. It was about what the organisation believed it was doing. A DPO wired to the highest management level and standing in the path of decisions about data is an organisation saying: this is a matter of how we run ourselves. A DPO tucked three layers into legal is an organisation saying: this is a matter of not getting caught. The two organisations produced almost identical binders in May 2018. They are not producing remotely similar outcomes now.

### 9. A Year In

The reason this can be written now, rather than as prediction, is that the first serious enforcement signals have begun to arrive. A year on, the supervisory authorities are moving from guidance to action, and the figures attached to their early notices are of the order everyone feared — nine figures, not the token penalties of the previous regime. The abstraction of the fine is becoming concrete, and as it does, the distinction this essay has laboured is turning from an argument into a reckoning. The organisations discovering that documented compliance is not the same as governed data are discovering it the expensive way.

None of this means the lawyers were wrong to be involved, or that the records of processing were wasted effort, or that appointing a DPO was a mistake. It means that the point of the exercise was mislocated. The regulation asked organisations to become accountable for personal data as an ongoing operational fact. A significant number heard, instead, a request to become defensible — and built the role, the reporting line and the whole programme to deliver defensibility. They succeeded, and the success is precisely the problem, because a defensible organisation that has not changed how it handles data has merely documented the exposure it still carries.

The corrective is not another programme. It is a question, asked honestly at the highest level: is the person accountable for our data positioned to change what happens to it, or only to describe it? Where the answer is only to describe it, the reporting line is the first thing to move — not because the line itself is magic, but because moving it forces the prior question into the open. A DPO who reports to the top, and who stands where decisions about data are actually made, cannot help but turn the organisation's attention from the artefact to the reality. That was the point all along. It was available from the first day of the regulation. It was, in a great many places, quietly filed away under law, and it is still waiting to be picked up.