

BEYOND COMPLIANCE THEATRE

Data Protection Moves into the Design Room

Why data protection had moved from the approval gate into the design room

Giovanni Leonardi

November 2019



Data Protection Moves into the Design Room

Transformation · No. 289

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

“Once regulation determines what data can be collected, why it can be used and how long it can be kept, it has entered the product model itself.”

The Meeting That Changed the Backlog

In the autumn of 2019, a transformation team entered a fortnightly design review expecting to approve the final version of a new customer-onboarding journey. The screens were polished, the delivery plan was green and the commercial sponsor wanted the service live before year-end.

The data-protection specialist asked a simpler question: why did the form require 42 fields?

Eleven fields had no clear purpose beyond “we may need them later”. Six were retained because the old paper form had always contained them. Four would feed an analytical model that nobody had yet defined. The team had spent three months improving the interface without challenging the appetite for data beneath it.

The meeting ended with 19 fields, a rewritten privacy notice, a new retention schedule and a two-week delay. On the programme plan, this looked like regulatory interference. In reality, it was the first serious product decision the team had made.

Compliance Has Moved Upstream

The common assumption is that regulation sits at the edge of delivery. Product teams decide what to build; legal and compliance teams check that the result is permissible. That division of labour is tidy, familiar and increasingly false.

The General Data Protection Regulation has made data protection visible in the architecture of services. Purpose limitation affects which information is collected. Data minimisation affects the form itself. The right of access affects record design and retrieval. Retention affects storage, operating procedures and supplier contracts. Privacy by design affects decisions before a line of code is committed.

These are not comments on a finished product. They are choices about what the product is.

Once regulation determines what data can be collected, why it can be used and how long it can be kept, it has entered the product model itself.

This is why the regulator has, in effect, become a product owner. Not because a supervisory authority is writing user stories, but because regulatory principles now shape priorities, acceptance criteria and the definition of value. A service that converts well but cannot explain its use of personal data is not a successful service with a compliance defect. It is a defective service.

The Strong Objection

There is a serious counterargument. Product ownership requires judgement about customers, economics and operational feasibility. A regulator supplies boundaries, not a vision. Elevating compliance too far can create defensive design: more notices, more approvals, less experimentation and a mistaken belief that avoiding criticism is the same as creating value.

That objection is right about the danger, but wrong about the remedy. The answer is not to return regulation to a late-stage gate. It is to translate regulatory intent into design choices early enough that teams retain room to exercise judgement.

The difference is visible in the questions asked:

- A late compliance review asks, “Can we release this?”
- A product-minded review asks, “Why does the service need this data at all?”
- A defensive interpretation asks, “What wording protects us?”
- A design interpretation asks, “What would make the exchange of data intelligible and fair?”

The first pair manages permission. The second designs trust.

The practical shift is from treating regulation as a veto exercised at the end to treating it as a design input exercised at the beginning.

What Leaders Were Missing

By late 2019, many organisations had completed their initial inventories, rewritten notices and introduced impact assessments. The visible work created a comforting impression that the regulatory change had been absorbed. But documentation was never the difficult part. The difficult part was changing who had authority when product convenience conflicted with data discipline.

Three patterns now separate genuine adaptation from compliance theatre.

- The data-protection specialist joins discovery. If the role appears only at approval, the cheapest choices have already passed.

- Every data field has an owner and a purpose. “Potential future use” is not a requirement; it is an unpriced liability.
- Delivery evidence includes deletion and retrieval. Teams demonstrate not only that information can enter the service, but that it can be found, corrected and removed across operational systems.

Return to the onboarding example. Removing 23 fields did more than reduce regulatory exposure. Average completion time fell from twelve minutes to seven in the next round of testing. Calls asking why particular information was required almost disappeared. The change worked because data minimisation and customer effort were not competing objectives; the excess data had been serving neither.

That is the overlooked lesson of this period. Regulation is often presented as the cost of protecting the individual from the organisation. In well-designed services, it can also expose habits that have survived without challenge: collecting because storage is cheap, retaining because deletion is awkward, and requesting consent because purpose has not been settled.

The Product Decision Hiding in Plain Sight

Leaders should resist the theatrical response: appointing more reviewers, adding another sign-off and calling the resulting delay governance. The more useful response is to recognise that regulatory judgement has become part of product judgement.

That means product owners must understand purpose, lawful use and retention well enough to make informed trade-offs. Data-protection specialists, in turn, must express principles as design consequences rather than distant prohibitions. Neither profession can succeed by throwing documents over the boundary to the other.

The organisations that learn this will not make the regulator their literal product owner. They will do something more mature: internalise the questions the regulator has forced into view.

The real change is not that compliance now has a louder voice. It is that a product can no longer be considered well designed when its treatment of personal data is unintelligible, excessive or impossible to reverse.