

BEYOND THE BANNER

Consent Is a Control, Not a Checkbox

A Practitioner's Perspective on Consent and Privacy by Design in the First Year of GDPR

Giovanni Leonardi

November 2018



Consent Is a Control, Not a Checkbox

Transformation · No. 224

Originally written November 2018 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

"We built the doorbell and never wired it to the house."

1. The banner is the least interesting part of consent

Six months after the regulation came into force, almost every organisation I look at has a consent banner. Very few of them have a consent architecture. That distinction is not a quibble — it is the whole of the problem, and it explains why so much of the past year's effort has produced compliance on paper and incoherence in practice.

The banner is the visible artefact. It is what the board saw in the demo, what the agency delivered on time, what the legal team reviewed and signed. It sits on top of a website or an app and asks a question. But the question it asks — do you consent? — only means something if the answer travels somewhere, is remembered, is honoured by every downstream system that subsequently touches the person's data, and can be withdrawn as easily as it was given. In most organisations none of those four things is reliably true. The answer is captured at the front door and then quietly abandoned. We built the doorbell and never wired it to the house.

The pattern I have watched repeat across sector after sector this year is the same: enormous energy spent on the interface where consent is asked, almost none on the machinery by which consent is kept. And keeping consent — persisting it, propagating it, binding it to a purpose, honouring its withdrawal — was always the hard part. The asking was never the work.

2. How consent became a bolt-on

To understand why the architecture is missing, it helps to be honest about how the run-up to May actually went inside most organisations.

The programme was framed, from the first steering meeting, as a legal and compliance exercise with a hard deadline. That framing was not wrong, but it was consequential. A legal-and-compliance framing pulls the centre of gravity towards documents: policies, registers, records of processing, an impact-assessment template, and — most visibly — the wording of a consent notice. These are necessary. But they describe the system that ought to exist; they do not build it. When the clock is running down, the artefacts that a working group can produce in a room get produced, and the artefacts that require months of engineering across a dozen systems get deferred, then quietly dropped.

So the consent statement was drafted with great care. The consent system was assembled by accident — bolted together from whatever was already to hand. A tag manager here, a third-party banner vendor there, a cookie script inherited from a marketing campaign three years ago, a customer-record flag that half the integrations ignore. Nobody designed this. It accreted. And an accreted architecture has a predictable property: no single part of it knows what any other part has promised the customer.

*“The consent statement was drafted with great care.
The consent system was assembled by accident.”*

The result is an organisation that can show a regulator a beautifully worded notice and a screenshot of a banner, and cannot answer the only question that actually matters: for this specific person, what did we ask, what did they say, and is every system that holds their data currently behaving in a way consistent with that answer? In my experience, when you ask that question directly, the room goes quiet.

3. What was actually delivered

It is worth naming the gap precisely, because the two things are so easily conflated. Most organisations have delivered consent as a record. What privacy by design was asking for was consent as an architecture. They are not the same object, and the difference is not one of maturity — it is one of kind.

Consent as a record	Consent as an architecture
A timestamp and a checkbox captured at collection	A living state every system reads before it acts
Lives in one place — usually where it was collected	Propagates to every system that processes the data
Tied to a form or a page	Bound to a purpose, and enforced per purpose
Withdrawal is a support ticket and a manual scramble	Withdrawal is a signal that flows and takes effect everywhere
Proves you asked	Proves you are honouring what was said

An organisation with consent-as-a-record has bought itself a liability that looks like a safeguard. It holds the evidence that it asked the question, which means it has also created the evidence that it may not be honouring the answer. The record without the architecture is worse than useless — it is self-incriminating.

4. What a designed consent architecture actually requires

If we were to design the thing deliberately rather than let it accrete, what would it have to contain? The list is not exotic. Every element on it is well within reach of the engineering teams most organisations already have. What has been missing is not capability but ownership and intent.

1. A canonical consent record. One authoritative place where a person's consent state lives, keyed to an identity the whole organisation shares — not seven copies in seven systems, each drifting out of step with the others.
2. Purpose-binding. Consent is never global; it is always for something — this processing, that communication, this profiling. The record must hold consent per purpose, and each system must know which purposes it is entitled to rely on.
3. Propagation. When the state changes, the change must reach every system that processes the data, and it must reach them quickly. A withdrawal that takes a fortnight to filter through the estate is a withdrawal in name only.
4. Enforcement at the point of processing. The consuming systems must actually check the state before they act, rather than assume that because consent existed at collection it exists still. This is the step most often skipped, because it is the most invasive to retrofit.
5. Lifecycle and withdrawal. Consent is not permanent. It expires, it is refreshed, it is withdrawn. Treating it as a one-time event rather than a state with a lifecycle is the original design error from which most of the others follow.
6. Auditability. The whole thing must be reconstructable after the fact — what was asked, what was answered, when it changed, and what each system did in consequence.

Read that list back and notice what it is. It is not a legal specification. It is a systems architecture — a data model, a propagation mechanism, an enforcement pattern, and an audit trail. Consent was always going to be an engineering problem wearing legal clothing. The organisations that struggled most this year are the ones that never got past the clothing.

5. The organisational question underneath

There is a reason the architecture went unbuilt, and it is not technical. It is that no one owned it.

Consider how the responsibilities actually distributed themselves. Legal owned the words — the notice, the policy, the lawful basis. Marketing owned the banner and, quietly, a strong interest in as many people as possible clicking "accept". Engineering owned the tags and the integrations but received the requirement as "make the banner work", not "build a consent architecture". Data protection, where it existed as a function at all, owned the paperwork. And so the one thing that needed a single owner with authority across all four — the consent architecture as a coherent system — had no owner at all. It fell precisely into the gap between the functions, which is exactly where hard cross-cutting problems always fall.

- Legal could specify what should be true but could not build it.
- Marketing was structurally motivated to keep the mechanism shallow.

- Engineering built what it was asked for, and it was not asked for this.
- Data protection documented the intended state without the mandate to enforce it.

This is the deeper pattern, and it is not really about privacy at all. Consent architecture failed for the same reason master data management has failed for twenty years and enterprise integration for longer: it is a horizontal concern in organisations built as vertical silos, and horizontal concerns starve unless someone with real authority is made accountable for them end to end. The regulation did not create this problem. It simply chose a place to expose it that came with a fine attached.

6. Privacy by design was asking an architecture question

Which brings me to the phrase that has been quoted more than it has been understood this year. Privacy by design. It is written into the regulation as an obligation, and it has largely been received as an aspiration — a value to affirm, a principle to cite in the policy's opening paragraph.

But read plainly, privacy by design is not a value statement. It is an engineering instruction. It says: the protection of personal data must be built into the architecture of your systems from the outset, as a structural property, not applied afterwards as a coat of compliance paint. It is addressed to the people who design data models and system boundaries and processing pipelines. The trouble is that in most organisations that instruction arrived through the legal function, was translated into documents, and never reached the people it was actually written for — or reached them stripped of the authority to act on it.

Privacy by design was never a legal principle to be affirmed. It is an architectural instruction addressed to the people who design systems — and in most organisations, it was delivered to the wrong department.

So here is the perspective I would offer to anyone still treating this as last year's project, now closed. You do not have a consent problem that a better banner will solve. You have an architecture that nobody designed and nobody owns. Until consent is treated as a first-class system — with a canonical record, purpose-binding, propagation, enforcement, a lifecycle, and a single accountable owner sitting above the functional silos — you do not really have consent. You have a record that you asked. And in the years ahead I suspect the distance between asking and honouring is precisely the distance that regulators, and customers, will learn to measure.

The doorbell works beautifully. It is time we wired it to the house.