SOLUTION DESCRIPTION

Multi-regime data governance

Consent, subject rights, erasure and grievance across regimes that do not agree with each other — with every finding citing the law that governs it.

The problem is not the number of laws

An organisation operating across several jurisdictions is usually competent at reading each regime individually. What defeats the tooling is that the regimes make **different demands of the same record**. One requires a retention floor for a class of data; another grants an erasure right over it. One treats a lawful basis as consent that can be withdrawn; another treats the same processing as a legal obligation that cannot.

Most platforms respond with a single global setting — one retention window, one erasure behaviour — chosen to satisfy the strictest regime. That is simultaneously too aggressive for the obligation that requires retention and too coarse for the regime that requires a documented basis per purpose. It does not fail an audit. It fails the first request that asks *why*.

Four mechanisms

A record class carries its basis, not just its window

Retention is declared per class with the reason it exists and the regime that requires it. Where two regimes disagree about the same class, the disagreement is represented rather than resolved by picking the longer number — which is what makes the conflict visible to the people whose job it is to decide.

Erasure destroys a key, not a haystack

A per-subject key rendered unusable makes that subject's personal data unreadable in every copy of the event store — replicas, backups and archives — at once, and the operation is verifiable. The events and their seals survive, with the subject reduced to a pseudonymous reference. It is the only honest answer to an erasure right exercised against an append-only store.

Every finding cites its governing law

A governance finding that says “this is a violation” without naming the provision is an opinion. Findings carry the regime and the article, so a compliance team can act on them without re-deriving the reasoning — and can disagree with the mapping where they read it differently.

Grievance and subject requests are events

A request received, acknowledged, actioned and closed is a sequence in the same store as everything else, on the same clock. Statutory clocks become queries rather than a spreadsheet somebody maintains.

Security telemetry is personal data, and the defensive purpose does not suspend the obligation. Who signed in from where, on which device, reading which files. A platform that retains all of it indefinitely so that evidence is always available has described a liability, not a control. The reconciliation is that retention is a property of the record class rather than of the disk it landed on.

Where the regimes actually diverge

Three axes account for most of the operational difficulty, and a platform that models them separately can carry several regimes without a setting per country.

`lawful basis`	whether the processing rests on consent, legitimate interest, or a legal obligation — and therefore whether it can be withdrawn at all
`transfer conditions`	where a record may be processed, and what must accompany it when it crosses a border
`statutory clocks`	how long you have to acknowledge, to complete, and to notify — the numbers differ, and they are the ones most often missed

What we will not claim

We do not assert that you are compliant with anything. A mapping from a control to a provision is only meaningful against your interpretation of your obligations in your jurisdiction, and a vendor asserting compliance on your behalf is doing you a disservice. What we provide is the evidence layer that makes your own mapping demonstrable, and findings that name the provision so you can disagree with them precisely.

There is also a residue no architecture dissolves. An incident narrative that names a person's actions is meaningful evidence and remains personal data. The resolution is procedural — minimise what the narrative names, keep identifying detail in the linked events under their own class — and a vendor claiming to have solved that in the product is overselling.

EventLake

NEXT STEP

Bring the assessment you have to complete. We will walk each class, each window, each transfer, and tell you where the answer is “that is your decision, not ours” — which is more of the document than a vendor session usually admits.

Further reading: Paper 06 *Evidence should be a query* · the *Trust & assurance brief*. All published, none behind a form. **eventlake.com**