EventLake

For data protection officers and privacy counsel

DATA PROTECTION · RETENTION · ERASURE

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 TENSION

Evidence wants long, erasure wants short

Both are real obligations, reconcilable only if retention is a property of the record class, not of the disk it landed on.

THE MECHANISM

Destroy the key, not the haystack

A per-subject key rendered unusable makes that subject's personal data unreadable in every copy of the event store at once — verifiably. The events survive, with the subject reduced to a pseudonymous reference.

THE RECEIPT

The erasure is itself an event

What was erased, when, on whose instruction, under which basis — recorded without re-recording the content.

One subject, four lifetimes, each with a stated reason

a single global window is wrong twice

`authentication`	`13 months`	supports account-compromise investigation; expires on schedule
`endpoint telemetry`	`90 days`	the shortest window that still supports hunting and rule backtesting
`actions & approvals`	`7 years`	what the organisation did and on whose authority — an accountability record
`erasure request`	`key destroyed`	personal data unreadable everywhere at once; the erasure recorded, the content not

WHAT YOU CAN DEMONSTRATE

A lawful basis per class. Each retention window carries the reason it exists, so a notice describes what the platform is actually doing.

Erasure across backups. The one honest answer to a request made against an append-only store, and a verifiable one.

Holds that stay visible. A legal hold names its custodian, its scope and its matter, and stays on the hold register until someone releases it. A hold nobody can see is how you retain what you promised not to.

WHAT WE WILL NOT CLAIM

There is 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, and keep identifying detail in the linked events under their own class.

A vendor claiming to have solved this in the product is overselling.

BRING US YOUR DPIA

A working session with your privacy team, not a slide deck.

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”.

Book a session

contact@eventlake.com

We ask for a work email and a phone number, and we tell you what we will do with them before you submit. We do not sell contact data, and one unsubscribe stops everything.