PRIVACY IS NOT A POWERPOINT

The cost of weak data governance?

Anonymised cases involving retention failures, Nov 2024–Nov 2026

Retention failures formed part of the sanctioned breaches in every case

CASE / CONSEQUENCE	WHAT WENT WRONG	GOVERNANCE CONTROL NEEDED
€403m fine · Sep 2026	Location data retained excessively across features, alongside other GDPR failures.	Set justified retention periods and enforce them across every feature.
€27m fine · Jan 2026	A mobile operator kept subscriber data for too long, alongside security failures.	Automate deletion when the justified retention period expires.
€1m fine · Dec 2025	A former supplier kept 46m+ users' data after its contract ended.	Inventory every copy and verify supplier deletion at contract end.
€240k fine · Dec 2024	Each contact-data update restarted a five-year retention period.	Use a justified deletion deadline. Avoid automatic retention renewal.

Every copy needs a deletion deadline and evidence that deletion happened.

The PowerPoint problem



THE POLICY

Delete inactive customer contact data after 24 months.

THE QUESTION

How will every new destination become part of the controlled scope?



THE POLICY

Use personal data only for approved purposes.

THE QUESTION

Where does “purpose limitation” live technically?



POLICY

A retention period ends with deletion.

THE QUESTION

How can we implement retention without a trigger?



THE REQUEST

“Delete my data.”

THE QUESTION

Do we know enough about our data landscape to execute the right we promised the customer?

How will every new destination become part of the controlled scope?

Policy: Delete inactive customer contact data after 24 months.

THE MISSING TRANSLATION

Known scope: CRM.

Actual scope: CRM → campaign platform → warehouse → analyst export → vendor suppression file.

Broken link: no maintained lineage or onboarding control for new destinations.



A policy needs a defined system scope.

Where does “purpose limitation” live technically?

Policy: Use personal data only for approved purposes.

THE MISSING TRANSLATION

Operational control stack:

- purpose metadata and permitted-use classification
- dataset and use-case ownership
- access and query restrictions
- approval for new uses
- monitoring of exports, sharing and model training



An approved purpose needs enforceable rules.

How can we implement retention without a trigger?

Policy: Data needs to be deleted or anomized by the end of retention time.

THE MISSING TRANSLATION

What triggers the retention period: the end of the customer relationship or the creation of the data?

Must we delete the data on the day the retention period ends, or is a grace period for technical deletion allowed?



A deadline needs a starting point.

Can we execute erasure across the full data landscape?

Request: “Delete my data.”

THE MISSING TRANSLATION

The privacy team contacts known system owners.
CRM and Marketing: deleted. Billing: legal retention.
Data warehouse? Analytics datasets? Exports?
Vendor systems? Derived data?
Can we execute the right we promised the customer?



Deletion must be complete.

The PowerPoint problem

Treating a documented privacy process as proof that the technology follows it.

On paper, everything looks great.

- ✓ **Privacy Policy**
- ✓ **ROPA**
- ✓ **DPIA**
- ✓ **Retention Policy**
- ✓ **Privacy Notice**
- ✓ **Processor Agreements**
- ✓ **Training**

So... are we compliant?

We don’t know.

None of these documents prove what is actually happening to the data.

The Privacy Implementation Gap

WHAT WE SAY SHOULD HAPPEN

Policies · ROPA · DPIA · Standards

↓ THE GAP ↓

WHAT ACTUALLY HAPPENS

Applications · APIs · Databases · Pipelines · Vendors · Users

Most privacy organisations are very good at governing the top half. But compliance ultimately happens in the bottom half. If we cannot trace the requirement through this chain, we have documentation of intent, not evidence of implementation.

How we usually think: governance on paper

A complete-looking model can still leave the operational reality ungoverned.

THE GOVERNANCE MODEL

Policies › Processes › Roles › Controls › Compliance

THE POLICY SAYS

"Delete customer data after X months."

BUT THE DATA LIVES HERE

CRM | Billing | Warehouse | Reporting DB

Excel exports | Backups | Vendors | Data lake

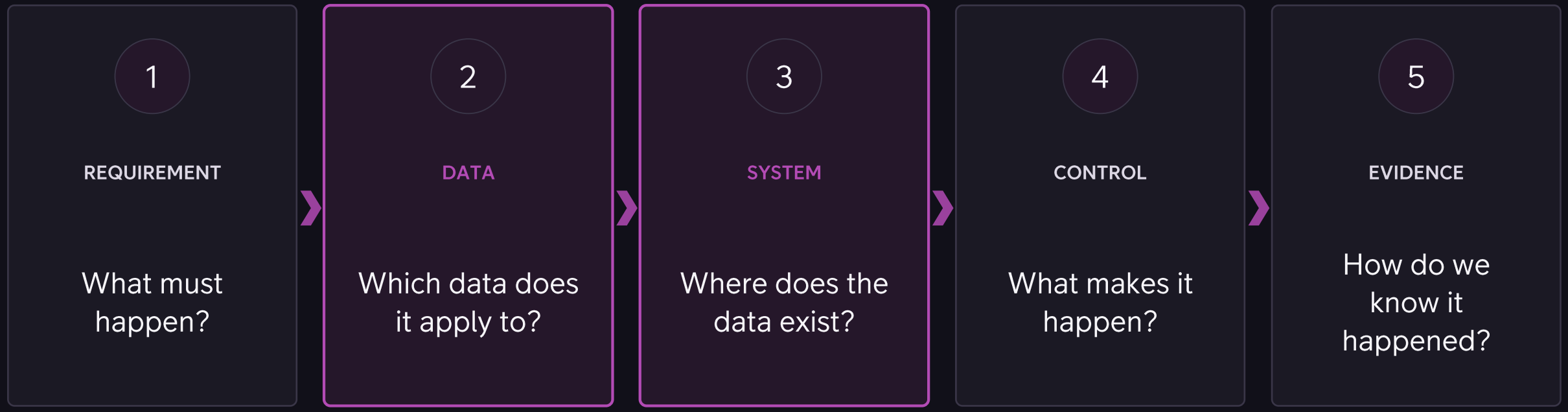
Which system actually deletes it?

Policies, processes and roles can look complete while the link to data, system behaviour and evidence is still missing.

The gap is not documentation.
The gap is traceability.

How we should think

Trace every requirement through the data and systems that must deliver it.



DATA MANAGEMENT MAKES THE PROMISE DELIVERABLE IN SYSTEMS

If I cannot follow this chain, I don’t know whether the requirement has actually been implemented.

Data management makes privacy requirements implementable

A retention requirement becomes executable only when it is connected to real data, events and systems.

POLICY REQUIREMENT

Delete customer contact data
12 months after the relationship ends.

DATA MANAGEMENT

Connects the obligation to the data landscape.

TECHNICAL CONTROLS

Delete, anonymise, restrict and record.

Data management helps by:

01

Identifying the data and systems

Data scope: e-mail address used for customer administration purposes

02

Mapping the flows

System scope: all cointaining e-mail address used for customer administration purposes

03

Connecting the trigger

Trigger: 24 months after customer relationship ends. Techincal deletion process during the month of retention deadline.

04

Attaching the rule

to the relevant data and copies

05

Providing control inputs

that systems can act on

Data management does not delete the data.

It provides the knowledge and structure that make reliable deletion possible.

POLICY defines the obligation • DATA MANAGEMENT provides the context • TECHNOLOGY executes the control • EVIDENCE proves the result

Data management enables to connect privacy obligation to the
data,
systems,
owners,
flows and events
needed to make the fulfillment of the obligation possible.

What organisations actually need to build

Data discovery

Know what exists.

Metadata & classification

Know what it is.

Ownership

Know who decides.

Lineage

Know where it goes.

Lifecycle controls

Control how long it exists.

Access controls

Control who can use it.

Privacy in change processes

Make privacy happen before production.

Evidence

Demonstrate that controls operate.

Policies define the promise.

Data management practices make it implementable.

Operations deliver it.

Evidence proves it.