



Espresso Data Privacy™
by Yoosana

GUIDE

Deletion you can prove

Seven steps from deletion concept to proven deletion – for organisations with many systems

- 1**
Form deletion objects
- 2**
Set retention periods and triggers
- 3**
Find systems and personal data
- 4**
Clarify order and dependencies
- 5**
Govern approvals and holds
- 6**
Delete across all systems
- 7**
Prove and monitor

Deleted means done

Many organisations have a deletion concept and a register. What is usually missing is putting them into practice: the data sits in many systems, retention periods depend on events, and when internal audit asks for proof, the search begins. This guide shows in seven steps how rules become proven deletions.

What is deleted ...

can no longer leak

Less data means less damage in a data breach.

no longer needs to be disclosed

Access requests become shorter and faster.

no longer distorts any analysis

Outdated data disappears from reports and analyses.

no longer costs anything

No storage, no backup, no migration.

The seven steps

- 1 Form deletion objects** Business units instead of tables
- 2 Set retention periods and triggers** Every period needs a starting point
- 3 Find systems and personal data** File shares, mailboxes, exports, AI data too
- 4 Clarify order and dependencies** Delete dependent data first
- 5 Govern approvals and holds** Deletion holds in one place, with reason and expiry
- 6 Delete across all systems** Central control, local deletion
- 7 Prove and monitor** Proof from the systems' confirmations

For data protection officers, IT management, compliance and internal audit in organisations with grown, hybrid IT.

1 Form deletion objects

What it is about

Data is not deleted table by table, but in business units. A deletion object groups data that is kept for the same reason and deleted together – for example a contract with all its payments and correspondence. ISO/IEC 27555 speaks of groups of personally identifiable information, the former DIN 66398 of data types.

How to proceed

- ✓ Start from the record of processing activities: which data is processed for what purpose?
- ✓ Group data with the same purpose and the same retention period into deletion objects.
- ✓ Assign the business objects that have to be deleted together.
- ✓ Appoint a responsible owner for each deletion object.

Typical mistakes

- ✗ Too fine: every table gets its own rule – nobody keeps the overview.
- ✗ Too coarse: «customer data» as one block – the periods do not fit.
- ✗ Only IT or only legal is at the table.

Example

An insurance claim with a pension payment spans several business objects: claim notification, benefit file, pension. For deletion they form one deletion object with a common rule.

CHECK QUESTION

Can a business expert say in one sentence for each deletion object which data belongs to it and why it is kept?

2 Set retention periods and triggers

What it is about

A period without a starting point cannot be implemented. The retention period is a lower limit – for example ten years for business records and accounting vouchers under Swiss law (Art. 958f CO). The deletion period is an upper limit: personal data may not be processed longer than the purpose requires (Art. 6(4) FADP, Art. 5(1)(e) GDPR).

How to proceed

- ✓ Record the period, justification and legal basis for each deletion object.
- ✓ Define the starting point, such as the end of the contract or the closing of a case.
- ✓ Form deletion classes: combinations of period and starting point shared by several deletion objects.
- ✓ Have the retention schedule approved and give each period a review date.

Typical mistakes

- ✗ «Ten years» – but from when?
- ✗ Limitation periods are confused with retention obligations.
- ✗ The period changes in the document, the systems are not updated.

Example

«Contract data is deleted in all systems ten years after the end of the contract, unless a deletion hold exists because of litigation.»

CHECK QUESTION

Can you calculate for every record when it is due – without anyone having to ask?

3 Find systems and personal data

What it is about

Retention periods only help if you know where the data is. Much personal data is not in the core systems but in file shares, mailboxes, exports, test environments – and increasingly in AI data such as transcripts and prompt logs.

How to proceed

- ✓ List the leading system and all downstream systems for each deletion object.
- ✓ Record data flows between systems: where is data copied to?
- ✓ Search file shares and databases for personal data regularly and assess the findings.
- ✓ Assign findings to a deletion object and update the register.

Typical mistakes

- ✗ Only the core systems are considered.
- ✗ Copies, exports and test data are forgotten.
- ✗ Searched once, never again – a scan is a snapshot.

Example

A customer export for an analysis has been sitting on a file share for years. In the core system the customer was deleted long ago – in the export she was not.

CHECK QUESTION

Do you know for each deletion object in which systems it occurs – including copies?

4 Clarify order and dependencies

What it is about

Data depends on other data: a payment refers to a contract, a contract to a person. Deleting in the wrong order leaves references pointing nowhere or brings processes to a halt.

How to proceed

- ✓ Map the dependencies between systems and business objects.
- ✓ Define deletion chains: dependent data is deleted first.
- ✓ Decide per system: delete, anonymise or archive.
- ✓ Allow objections: a system may object if it still needs the data, for example for an open claim.

Typical mistakes

- ✗ Each system deletes on its own and at its own pace.
- ✗ Data is anonymised where it should be deleted – or vice versa.
- ✗ Open cases are overlooked and deleted too.

Example

First the payments are deleted in the finance system, then the contract in the core system, finally the person in the partner system – each only once the previous step is confirmed.

CHECK QUESTION

What happens in the second system when the first one has deleted the record?



STEP 5 OF 7

5 Govern approvals and holds

What it is about

Not everything that is due may be deleted immediately: litigation, investigations or proceedings put deletion on hold (legal hold). And where the risk is high, an authorised person approves the deletion. Erasure requests from data subjects also belong in this process (Art. 32(2)(c) FADP, Art. 17 GDPR).

How to proceed

- ✓ Keep deletion holds in one central place – with reason, owner and expiry.
- ✓ Set approvals by risk, for example for the first runs, large volumes or sensitive data.
- ✓ Clarify roles: who sets periods, who approves, who executes, who controls.
- ✓ Route erasure requests the same way into all affected systems.

Typical mistakes

- ✗ Holds are agreed by email and forgotten.
- ✗ Everything needs an approval – a backlog builds up.
- ✗ Nothing needs an approval – trust is missing.

Example

A customer is involved in litigation. His data receives a deletion hold until the proceedings are closed; after that it is deleted in the next run.

CHECK QUESTION

Where do you see all active deletion holds at a glance today?



STEP 6 OF 7

6 Delete across all systems

What it is about

Each application knows its data and business logic best – so it deletes itself, using its existing functions. Control is central: what is deleted where and when, in which order and with which checks.

How to proceed

- ✓ A central deletion control issues the due deletions and collects the confirmations.
- ✓ Connect the applications through an open interface, for example REST or messaging.
- ✓ Proceed step by step: start with the leading system, others follow.
- ✓ Each application reports back what it has deleted; if a confirmation is missing, an alert is raised.

Typical mistakes

- ✗ Deleting directly in the database, bypassing the application.
- ✗ Trying to switch everything over at once.
- ✗ Cleaning up once instead of deleting continuously.

Example

Every night the control determines the due cases, distributes the jobs in the defined order and waits for each application to confirm.

CHECK QUESTION

Does your deletion run even when nobody thinks about it?

7 Prove and monitor

What it is about

Whoever deletes must be able to prove it: the GDPR requires accountability (Art. 5(2) GDPR), and in Switzerland too, what counts in an audit, a regulatory review or a complaint is what can be proven. Proof comes from the systems' confirmations – not from the job.

How to proceed

- ✓ One log per deletion run: basis, systems, result per system, count, approvals and exceptions.
- ✓ No deleted content and as little personal data as possible in the log.
- ✓ Store proof securely with tightly limited access; set a retention period for proof as well.
- ✓ Look at the key figures regularly: due, deleted, on hold, open.

Typical mistakes

- ✗ A spreadsheet or a ticket counts as proof – it shows the job, not the effect.
- ✗ The log contains exactly the data that should have been deleted.
- ✗ Nobody looks at missing confirmations.

Example

Internal audit asks for last quarter's deletions. A report shows per run what was deleted, what was on hold and which system did not delete and why.

CHECK QUESTION

Could you show tomorrow what was deleted last quarter – and what was not, with the reason?

Checklist

To tick off – the two most important points per step.

1 Form deletion objects

- ☐ Deletion objects are formed and described in business terms.
 - ☐ Each deletion object has a responsible owner.
-

2 Set retention periods and triggers

- ☐ Every period has a justification, legal basis and starting point.
 - ☐ The retention schedule is approved and has review dates.
-

3 Find systems and personal data

- ☐ All systems are known for each deletion object, including copies.
 - ☐ File shares and databases are searched regularly.
-

4 Clarify order and dependencies

- ☐ Dependencies and deletion chains are defined.
 - ☐ For each system it is decided: delete, anonymise or archive.
-

5 Govern approvals and holds

- ☐ Deletion holds are kept centrally, with reason and expiry.
 - ☐ Approvals and roles are set by risk.
-

6 Delete across all systems

- ☐ The applications delete themselves, centrally controlled.
 - ☐ Missing confirmations trigger an alert.
-

7 Prove and monitor

- ☐ Each deletion run produces a log from the confirmations.
 - ☐ Key figures are reviewed regularly.
-

Legal basis

Art. 6(4) FADP	Destroy or anonymise personal data as soon as it is no longer needed
Art. 32(2)(c) FADP	The data subject can demand deletion and enforce it in court
Art. 5(1)(e) and (2) GDPR	Storage limitation and accountability
Art. 17 GDPR	Right to erasure
Art. 958f CO	Retention of business records and accounting vouchers: ten years
ISO/IEC 27555	Guidelines on the deletion of personally identifiable information; successor to DIN 66398

This guide provides an overview and does not replace legal advice in individual cases. Sectors such as insurance, banking or healthcare have additional regulations. As of October 2026.

How Espresso Data Privacy helps

Espresso Data Privacy is the Privacy Operations Cockpit for organisations with many systems – operated with you, in your own data centre, in your cloud or with an operating partner.

1-2	Privacy Register	Register, deletion objects and retention schedule with approval
3	Data Discovery	Find personal data in file shares, databases and Microsoft 365
4-6	Data Deletion	Deletion chains, deletion holds, objections, approvals and central control
5	Subject Request	Record erasure requests and pass them to all systems
7	Data Deletion	Log per deletion run from the systems' confirmations

Proven in operation: In production since 2024 – reference: Pax, the Swiss pension insurer.

Conversation or demo

We are happy to show you, using your case, what the seven steps look like in your systems.

✉ info@espressodataprivacy.com
🌐 espressodataprivacy.com