



Espresso Data Privacy™
by Yoosana

LEITFADEN

Löschen, das man belegen kann

In sieben Schritten vom Löschkonzept zur belegten Löschung – für Organisationen mit vielen Systemen

1

Löschobjekte bilden

2

Fristen und Auslöser festlegen

3

Systeme und Personendaten finden

4

Reihenfolge und Abhängigkeiten klären

5

Freigaben und Sperren regeln

6

Über alle Systeme löschen

7

Belegen und überwachen

Gelöscht ist erledigt

Viele Organisationen haben ein Löschkonzept und ein Verzeichnis. Woran es meist fehlt, ist die Umsetzung: Die Daten liegen in vielen Systemen, die Fristen hängen an Ereignissen, und wenn die Revision nach dem Nachweis fragt, beginnt die Suche. Dieser Leitfaden zeigt in sieben Schritten, wie aus Regeln belegte Löschungen werden.

Was gelöscht ist ...

kann nicht mehr abfließen

Weniger Daten bedeuten weniger Schaden bei einer Datenschutzverletzung.

muss nicht mehr beauskunftet werden

Auskunftsbegehren werden kürzer und schneller.

verfälscht keine Auswertung mehr

Veraltete Daten verschwinden aus Berichten und Analysen.

kostet nichts mehr

Kein Speicher, keine Sicherung, keine Migration.

Die sieben Schritte

- 1 Löschobjekte bilden** Fachliche Einheiten statt Tabellen
- 2 Fristen und Auslöser festlegen** Jede Frist braucht einen Startzeitpunkt
- 3 Systeme und Personendaten finden** Auch Ablagen, Postfächer, Exporte, KI-Daten
- 4 Reihenfolge und Abhängigkeiten klären** Abhängige Daten zuerst löschen
- 5 Freigaben und Sperren regeln** Löschsperren zentral, mit Grund und Ablauf
- 6 Über alle Systeme löschen** Zentral steuern, dezentral löschen
- 7 Belegen und überwachen** Nachweis aus den Rückmeldungen der Systeme

Für Datenschutzverantwortliche, IT-Leitung, Compliance und Revision in Organisationen mit gewachsener, hybrider IT.

1 Löschojekte bilden

Worum es geht

Gelöscht wird nicht Tabelle für Tabelle, sondern in fachlichen Einheiten. Ein Löschojekt fasst Daten zusammen, die aus demselben Grund aufbewahrt und gemeinsam gelöscht werden – etwa ein Vertrag mit allen Zahlungen und der Korrespondenz dazu. ISO/IEC 27555 spricht von Gruppen personenbezogener Informationen, die frühere DIN 66398 von Datenarten.

So gehen Sie vor

- ✓ Vom Verzeichnis der Bearbeitungstätigkeiten ausgehen:
Welche Daten werden wofür bearbeitet?
- ✓ Daten mit gleichem Zweck und gleicher Frist zu Löschojekten gruppieren.
- ✓ Die Geschäftsobjekte zuordnen, die gemeinsam gelöscht werden müssen.
- ✓ Für jedes Löschojekt eine verantwortliche Stelle bestimmen.

Typische Fehler

- ✗ Zu fein: Jede Tabelle bekommt eine eigene Regel – niemand behält den Überblick.
- ✗ Zu grob: «Kundendaten» als ein Block – die Fristen passen nicht.
- ✗ Nur die IT oder nur der Rechtsdienst sitzt am Tisch.

Beispiel

Ein Schadenfall mit Rentenzahlung verteilt sich auf mehrere Geschäftsobjekte: Schadenmeldung, Leistungsakte, Rente. Für das Löschen bilden sie ein Löschojekt mit einer gemeinsamen Regel.

PRÜFFRAGE

Kann eine Fachperson zu jedem Löschojekt in einem Satz sagen, welche Daten dazugehören und warum sie aufbewahrt werden?

2 Fristen und Auslöser festlegen

Worum es geht

Eine Frist ohne Startzeitpunkt lässt sich nicht umsetzen. Die Aufbewahrungsfrist ist eine Untergrenze – etwa zehn Jahre für Geschäftsbücher und Buchungsbelege (Art. 958f OR). Die Löschfrist ist eine Obergrenze: Personendaten dürfen nicht länger bearbeitet werden, als der Zweck es erfordert (Art. 6 Abs. 4 DSGVO, Art. 5 Abs. 1 lit. e DSGVO).

So gehen Sie vor

- ✓ Für jedes Löschojekt Frist, Begründung und Rechtsgrundlage festhalten.
- ✓ Den Startzeitpunkt bestimmen, etwa das Vertragsende oder den Abschluss eines Falls.
- ✓ Löschklassen bilden: Kombinationen aus Frist und Startzeitpunkt, die sich mehrere Löschojekte teilen.
- ✓ Das Fristenverzeichnis freigeben lassen und jeder Frist ein Überprüfungsdatum geben.

Typische Fehler

- ✗ «Zehn Jahre» – aber ab wann?
- ✗ Verjährungsfristen werden mit Aufbewahrungspflichten verwechselt.
- ✗ Die Frist ändert sich im Dokument, die Systeme werden nicht nachgezogen.

Beispiel

«Vertragsdaten werden zehn Jahre nach Vertragsende in allen Systemen gelöscht, ausser es besteht eine Löschsperre wegen eines Rechtsstreits.»

PRÜFFRAGE

Lässt sich für jeden Datensatz berechnen, wann er fällig ist – ohne dass jemand nachfragen muss?

3 Systeme und Personendaten finden

Worum es geht

Fristen helfen nur, wenn bekannt ist, wo die Daten liegen. Viele Personendaten liegen nicht in den Kernsystemen, sondern in Dateiablagen, Postfächern, Exporten, Testumgebungen – und zunehmend in KI-Daten wie Transkripten und Prompt-Protokollen.

So gehen Sie vor

- ✓ Je Löschojekt das führende System und alle Folgesysteme auflisten.
- ✓ Datenflüsse zwischen den Systemen festhalten: Wohin werden Daten kopiert?
- ✓ Ablagen und Datenbanken regelmässig nach Personendaten durchsuchen und die Funde bewerten.
- ✓ Funde einem Löschojekt zuordnen und das Verzeichnis nachführen.

Typische Fehler

- ✗ Nur die Kernsysteme werden betrachtet.
- ✗ Kopien, Exporte und Testdaten werden vergessen.
- ✗ Einmal gesucht, nie wieder – ein Suchlauf ist eine Momentaufnahme.

Beispiel

Ein Kundenexport für eine Auswertung liegt seit Jahren auf einer Dateiablage. Im Kernsystem ist die Kundin längst gelöscht – im Export nicht.

PRÜFFRAGE

Wissen Sie für jedes Löschojekt, in welchen Systemen es vorkommt – auch in Kopien?

4 Reihenfolge und Abhängigkeiten klären

Worum es geht

Daten hängen voneinander ab: Eine Zahlung verweist auf einen Vertrag, ein Vertrag auf eine Person. Wer in der falschen Reihenfolge löscht, hinterlässt Verweise ins Leere oder bringt Abläufe zum Stillstand.

So gehen Sie vor

- ✓ Abhängigkeiten zwischen Systemen und Geschäftsobjekten aufzeichnen.
- ✓ Löschketten festlegen: Abhängige Daten werden zuerst gelöscht.
- ✓ Je System die Art bestimmen: löschen, anonymisieren oder archivieren.
- ✓ Einwände vorsehen: Ein System darf widersprechen, wenn es die Daten noch braucht, etwa bei einer offenen Forderung.

Typische Fehler

- ✗ Jedes System löscht für sich und nach eigenem Takt.
- ✗ Anonymisiert wird, wo gelöscht werden müsste – oder umgekehrt.
- ✗ Offene Fälle werden übersehen und mitgelöscht.

Beispiel

Erst werden die Zahlungen im Finanzsystem gelöscht, dann der Vertrag im Kernsystem, zuletzt die Person im Partnersystem – jeweils erst, wenn der vorherige Schritt bestätigt ist.

PRÜFFRAGE

Was geschieht im zweiten System, wenn das erste den Datensatz gelöscht hat?

5 Freigaben und Sperren regeln

Worum es geht

Nicht alles, was fällig ist, darf sofort gelöscht werden: Bei Rechtsstreit, Untersuchung oder Verfahren wird angehalten (Legal Hold). Und wo das Risiko hoch ist, gibt eine berechtigte Person die Löschung frei. Auch Löschanträge betroffener Personen gehören in diesen Ablauf (Art. 32 Abs. 2 lit. c DSGVO, Art. 17 DSGVO).

So gehen Sie vor

- ✓ Löschsperren an einer zentralen Stelle führen – mit Grund, Verantwortlichem und Ablauf.
- ✓ Freigaben nach Risiko regeln, etwa für die ersten Läufe, grosse Mengen oder besonders schützenswerte Daten.
- ✓ Rollen klären: wer Fristen festlegt, wer freigibt, wer ausführt, wer kontrolliert.
- ✓ Löschanträge über denselben Weg in alle betroffenen Systeme geben.

Typische Fehler

- ✗ Sperren werden per E-Mail vereinbart und geraten in Vergessenheit.
- ✗ Alles braucht eine Freigabe – es entsteht ein Stau.
- ✗ Nichts braucht eine Freigabe – das Vertrauen fehlt.

Beispiel

Für einen Kunden läuft ein Rechtsstreit. Seine Daten erhalten eine Löschsperre bis zum Abschluss des Verfahrens; danach werden sie im nächsten Lauf gelöscht.

PRÜFFRAGE

Wo sehen Sie heute alle aktiven Löschsperren auf einen Blick?

6 Über alle Systeme löschen

Worum es geht

Jede Anwendung kennt ihre Daten und ihre Fachlogik am besten – deshalb löscht sie selbst, über ihre vorhandenen Funktionen. Gesteuert wird zentral: was wann wo gelöscht wird, in welcher Reihenfolge und mit welchen Prüfungen.

So gehen Sie vor

- ✓ Eine zentrale Löschststeuerung gibt die fälligen Löschungen vor und sammelt die Rückmeldungen.
- ✓ Die Anwendungen über eine offene Schnittstelle anbinden, zum Beispiel REST oder Nachrichten.
- ✓ Schritt für Schritt vorgehen: mit dem führenden System beginnen, weitere folgen.
- ✓ Jede Anwendung meldet zurück, was sie gelöscht hat; bleibt eine Rückmeldung aus, wird gewarnt.

Typische Fehler

- ✗ An der Anwendung vorbei direkt in der Datenbank löschen.
- ✗ Alles auf einmal umstellen wollen.
- ✗ Einmal aufräumen statt dauerhaft löschen.

Beispiel

Jede Nacht ermittelt die Steuerung die fälligen Fälle, verteilt die Aufträge in der festgelegten Reihenfolge und wartet auf die Bestätigung jeder Anwendung.

PRÜFFRAGE

Läuft Ihr Löschen auch dann, wenn niemand daran denkt?

7 Belegen und überwachen

Worum es geht

Wer löscht, muss es belegen können: Die DSGVO verlangt den Nachweis (Art. 5 Abs. 2 DSGVO), und auch in der Schweiz zählt bei Revision, Aufsicht oder Beschwerde, was sich belegen lässt. Ein Nachweis entsteht aus den Rückmeldungen der Systeme – nicht aus dem Auftrag.

So gehen Sie vor

- ✓ Je Löschlauf ein Protokoll: Grundlage, Systeme, Ergebnis je System, Anzahl, Freigaben und Ausnahmen.
- ✓ Keine gelöschten Inhalte und so wenige Personendaten wie möglich ins Protokoll.
- ✓ Nachweise geschützt ablegen und den Zugriff eng begrenzen; auch für Nachweise eine Frist festlegen.
- ✓ Regelmässig auf die Kennzahlen schauen: fällig, gelöscht, gesperrt, offen.

Typische Fehler

- ✗ Eine Tabelle oder ein Ticket gilt als Nachweis – es zeigt den Auftrag, nicht die Wirkung.
- ✗ Das Protokoll enthält genau die Daten, die gelöscht werden sollten.
- ✗ Niemand schaut auf ausbleibende Rückmeldungen.

Beispiel

Die Revision fragt nach den Löschungen des letzten Quartals. Ein Bericht zeigt je Lauf, was gelöscht wurde, was gesperrt war und welches System warum nicht gelöscht hat.

PRÜFFRAGE

Können Sie morgen zeigen, was im letzten Quartal gelöscht wurde – und was nicht, mit Grund?

Checkliste

Zum Abhaken – je Schritt die zwei wichtigsten Punkte.

1

Löschobjekte bilden

- ☐ Löschobjekte sind gebildet und fachlich beschrieben.
 - ☐ Jedes Löschobjekt hat eine verantwortliche Stelle.
-

2

Fristen und Auslöser festlegen

- ☐ Jede Frist hat Begründung, Rechtsgrundlage und Startzeitpunkt.
 - ☐ Das Fristenverzeichnis ist freigegeben und hat Überprüfungsdaten.
-

3

Systeme und Personendaten finden

- ☐ Für jedes Löschobjekt sind alle Systeme bekannt, auch Kopien.
 - ☐ Ablagen und Datenbanken werden regelmässig durchsucht.
-

4

Reihenfolge und Abhängigkeiten klären

- ☐ Abhängigkeiten und Löschketten sind festgelegt.
 - ☐ Je System ist bestimmt: löschen, anonymisieren oder archivieren.
-

5

Freigaben und Sperren regeln

- ☐ Löchsperren werden zentral geführt, mit Grund und Ablauf.
 - ☐ Freigaben und Rollen sind nach Risiko geregelt.
-

6

Über alle Systeme löschen

- ☐ Die Anwendungen löschen selbst, zentral gesteuert.
 - ☐ Ausbleibende Rückmeldungen lösen eine Warnung aus.
-

7

Belegen und überwachen

- ☐ Je Löschlauf entsteht ein Protokoll aus den Rückmeldungen.
 - ☐ Kennzahlen werden regelmässig geprüft.
-

Rechtsgrundlagen

Art. 6 Abs. 4 DSG	Personendaten vernichten oder anonymisieren, sobald sie nicht mehr erforderlich sind
Art. 32 Abs. 2 lit. c DSG	Die betroffene Person kann die Löschung verlangen und einklagen
Art. 5 Abs. 1 lit. e und Abs. 2 DSGVO	Speicherbegrenzung und Rechenschaftspflicht
Art. 17 DSGVO	Recht auf Löschung
Art. 958f OR	Aufbewahrung von Geschäftsbüchern und Buchungsbelegen: zehn Jahre
ISO/IEC 27555	Leitlinien zur Löschung personenbezogener Informationen; Nachfolgerin der DIN 66398

Dieser Leitfaden gibt einen Überblick und ersetzt keine Rechtsberatung im Einzelfall. Branchen wie Versicherungen, Banken oder das Gesundheitswesen haben zusätzliche Vorschriften. Stand: Oktober 2026.

Wie Espresso Data Privacy unterstützt

Espresso Data Privacy ist das Privacy Operations Cockpit für Organisationen mit vielen Systemen – betrieben bei Ihnen, im eigenen Rechenzentrum, in Ihrer Cloud oder bei einem Betreiber-Partner.

1-2	Privacy Register	Verzeichnis, Löschobjekte und Fristenverzeichnis mit Freigabe
3	Data Discovery	Personendaten in Ablagen, Datenbanken und Microsoft 365 finden
4-6	Data Deletion	Löschketten, Löschsperrern, Einwände, Freigaben und zentrale Steuerung
5	Subject Request	Löschbegehren erfassen und in alle Systeme geben
7	Data Deletion	Protokoll je Löschlauf aus den Rückmeldungen der Systeme

Im Betrieb bewährt: Seit 2024 im Produktivbetrieb – Referenz: Pax, die Schweizer Vorsorgeversicherung.

Gespräch oder Demo

Wir zeigen Ihnen gern an Ihrem Fall, wie die sieben Schritte in Ihren Systemen aussehen.

 info@espressodataprivacy.com
 espressodataprivacy.com