AGAD Service GmbH – Ihre Daten unser Schutz –

AGAD

Partner im Wettbewerb.

DATENSCHUTZ ZUM FEIERABEND

Daten löschen, aber richtig!
– Das Löschkonzept im Unternehmen nach der DSGVO

Christopher Pröpper

8. Juli 2025

AGAD
Partner im Wettbewerb.

Überblick:

Teil 1: Die Notwendigkeit eines Löschkonzepts

1. Einführung: Warum über Datenlöschung sprechen?
2. Gesetzliche Grundlagen
3. Risiken bei fehlender Datenlöschung
4. Praxisbeispiele aus Aufsichtsbehörden und Unternehmen

Teil 2: Umsetzung eines Löschkonzepts – Handlungsempfehlungen für Unternehmen

1. Ziel und Zweck eines Löschkonzepts
2. Struktur eines Löschkonzepts
3. Konkreter Leitfaden zur Erstellung
4. Tipps zur technischen und organisatorischen Umsetzung
5. Fazit und offene Fragerunde

AGAD
Partner im Wettbewerb.

Teil 1: Die Notwendigkeit eines Löschkonzepts

AGAD
Partner im Wettbewerb.

1. Einführung: Warum über Datenlöschung sprechen?

- In Zeiten zunehmender Digitalisierung sammeln Unternehmen mehr Daten denn je.
- Daten sind wertvoll – aber auch problematisch, wenn sie unnötig gespeichert oder falsch verarbeitet werden.
- Die DSGVO verpflichtet Unternehmen nicht nur zur Datensparsamkeit, sondern auch zur aktiven Löschung personenbezogener Daten, sobald der Zweck entfällt (Artt. 5 I lit. c, 17 DSGVO).
- Fehlt ein geregeltes Vorgehen bei der Verarbeitung von Daten, führt das zu „Datensammlungen“ ohne Systematik – mit hohen Risiken für Datenschutzverletzungen und -verlust, möglichem Reputationsverlust und Bußgeldern.

Exkurs:

Grundsätzlich dürfen personenbezogene Daten für unternehmensbezogene Zwecke gespeichert und verarbeitet werden. Allerdings bedarf es dazu einer entsprechenden Rechtsgrundlage (Art. 6 I lit. a-f DSGVO). Die gängigsten beiden Rechtsgrundlagen sind dabei wohl Art. 6 I lit. b und Artikel 6 I lit. f DSGVO. (Verarbeitung aufgrund Vertragsverhältnisses und das berechtigte Interesse).

Weiterhin müssen die verarbeiteten Daten auch dem Grundsatz der Datensparsamkeit (Datenminimierung) gemäß Art. 5 I lit. c DSGVO standhalten. *„Personenbezogene Daten müssen dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“.*

2. Gesetzliche Grundlagen im Hinblick auf die Datenlöschung

Eine Reihe gesetzlicher Grundlagen aus der DSGVO bzw. dem BDSG verpflichten direkt zur Datenlöschung:

Artikel 5 DSGVO – Grundsätze der Verarbeitung

Datenspeicherung ja, aber nur für vorher festgelegte Zwecke und nur solange der Grund zur Speicherung nicht entfallen ist. -> Es muss vorher klar sein, wofür die Daten erhoben werden!

- **Insbesondere: Art. 5 Abs. 1 lit. e DSGVO: Speicherbegrenzung**

„Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (…).“

Das bedeutet, dass die Daten nach dem Wegfall des ursprünglichen Speicherzwecks gelöscht werden müssen, weil der Grund für die Verarbeitung entfallen ist.

Artikel 17 DSGVO – Recht auf Löschung („Recht auf Vergessenwerden“)

Grundsätzlich können Betroffene verlangen, dass die über sie gespeicherten personenbezogenen Daten auch wieder gelöscht werden. Das gilt z.B. dann, wenn:

- der **Zweck entfallen** ist.

  ➡ Der ursprüngliche „Grund“ für die Speicherung ist nicht mehr gegeben.

- die **Einwilligung widerrufen** wurde,

  ➡ Die erteilte Einwilligung des Betroffenen kann jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft widerrufen werden. **Bsp.:** Der Mitarbeiter hat ursprünglich in die Nutzung seiner Bilder für betriebliche Zwecke eingewilligt.

- eine **unrechtmäßige Verarbeitung** vorliegt.

  ➡ Die Speicherung der personenbezogenen Daten bei der betroffenen Person ist zu Unrecht erfolgt.

Beispiel: Der Bewerber wurde abgelehnt und die Daten zu seiner Bewerbung wurden trotzdem nicht gelöscht. (Der Zweck ist entfallen, denn der Bewerbungsprozess ist beendet und damit auch die Zweckbindung gemäß Art. 5 I lit. b DSGVO.) Auch ein berechtigtes Interesse gemäß Art. 6 I lit f DSGVO würde hier nur ausnahmsweise greifen, wenn z.B. eine Klage droht. **Aber:** Die „vorsorgliche“ Speicherung ist hier nicht gerechtfertigt. Deshalb sollten die Daten abgelehnter Bewerber **nach sechs Monaten gelöscht** werden.

Klagerisiko AGG nach 6 Monaten entfallen. **-> siehe Hinweise in der Beratungspraxis.**

Artikel 30 DSGVO – Verzeichnis von Verarbeitungstätigkeiten

Jedes Verzeichnis muss Angaben zur vorgesehenen Frist für die Löschung enthalten (Art. 30 I lit. f DSGVO).

Verarbeitungsverzeichnisse müssen immer dann angelegt werden, wenn personenbezogene Daten im Unternehmen verarbeitet werden (Lohn- und Gehaltsabrechnung, ERP-System, Onlineshop, Newsletter-Versand u.a.).

➔ Verstöße gegen diese Anlagepflicht können gemäß Art. 83 IV lit. a DSGVO mit einem Bußgeld von bis zu 10 Millionen € oder 2 % des weltweiten Jahresumsatzes geahndet werden (je nachdem, was höher ausfällt).

§ 35 BDSG (neu) – Löschung im nationalen Recht

- Ergänzende Regelungen für Deutschland, z. B. bei Ausnahmen zur Löschverpflichtung.

Beispiel: Ein Unternehmen speichert personenbezogene Daten täglich auf Datensicherungsbändern. Der Betroffene fordert das Unternehmen zur Löschung seiner Daten gemäß Art. 17 DSGVO auf. Die Daten sind im Produktivsystem bereits gelöscht, befinden sich aber z.B. noch auf alten offline-Backups.

Lösung: Wenn die Daten im Produktivsystem bereits gelöscht sind, wäre es u.U. technisch aufwendig und unverhältnismäßig alte Bänder zu durchsuchen und selektiv zu löschen. Das Unternehmen kann sich daher darauf berufen die Daten nicht zu löschen, muss eine weitere Verarbeitung allerdings einschränken. Das funktioniert z.B. dann, wenn entsprechende technische und organisatorische Maßnahmen vorliegen, die eine Wiederverarbeitung aus diesen alten Backups ausschließt.

3. Risiken bei fehlender Datenlöschung

- Bußgelder: z. B. Deutsche Wohnen SE – 14,5 Mio. € wegen mangelhafter Löschkonzepte und Aufbewahrung von „Altdaten“.
- Haftung der Geschäftsführung und der Unternehmen selbst.
- Reputationsverlust und Vertrauensverlust bei Kunden.
- Technische Risiken: Höheres Risiko mit Blick auf die Menge der betroffenen Daten bei Alt- und Schattendaten.

- **Deutsche Wohnen (2019): Bußgeld i.H.v. 14,5 Million €**

Begründung: Systematisches Versäumnis ein datenschutzkonformes Löschkonzept umzusetzen (Verstoß gegen Art. 5 I lit. e DSGVO, Art. 25 DSGVO, Art. 5 II DSGVO).

Die Deutsche Wohnen hatte in Ihrem Archiv langfristig personenbezogene Daten gespeichert, ohne zu prüfen, ob diese noch benötigt werden. Betroffen waren: **Mieterdaten wie Gehaltsnachweise, Arbeitsverträge, Versicherungsdaten etc**. Die Daten wurden jahrelang gespeichert, obwohl der Speicherzweck längst entfallen war (auch Daten zu ehemaligen Mietverhältnissen). Letztlich entschied der BGH 2023 in dieser Sache zudem noch, dass Bußgeldbescheide **auch gegen Unternehmen** und nicht nur natürlich Personen ergehen können. **-> Praxisrelevanz!**

- **Hamburgische Datenaufsicht gegen „marktstarke“ Inkassounternehmen: Bußgeld 900.000 €**

Sachverhalt: Im November 2024 führte der Hamburgische Datenschutzbeauftragte sog. Schwerpunktprüfungen bei Inkassounternehmen durch. Bei den geprüften Unternehmen wurde festgestellt, dass hunderttausende personenbezogene Datensätze -hauptsächlich Schuldner-Daten - deutlich über die zulässige Aufbewahrungsfrist hinaus gespeichert waren. Teilweise bis zu fünf Jahre wurde ohne rechtliche Grundlage gespeichert.

Begründung: Verstoß gegen den Grundsatz der Speicherbegrenzung nach Art. 5 Abs. lit e DSGVO sowie gegen die allgemeine Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO). Bußgeld orientiert sich an der Menge der Daten und deren Sensibilität. Das Urteil ist mittlerweile rechtskräftig.

2: Löschkonzept erstellen – Handlungsempfehlungen für Unternehmen

AGAD
Partner im Wettbewerb.

1. Ziel und Zweck eines Löschkonzepts

- Definition:
  Ein Löschkonzept legt fest, wann und wie personenbezogene Daten im Unternehmen sicher gelöscht werden.

- Dient dazu, gesetzliche Anforderungen umzusetzen und Datenschutz-Risiken – z.B. durch Verlust – zu minimieren.

- Zielgruppen: Geschäftsführung, IT-Abteilung, Fachabteilungen.

Ein Löschkonzept sollte daher folgende Punkte umfassen:

- 1. Geltungsbereich und Zielsetzung der Datenlöschung
- 2. Rechtliche Grundlagen
- 3. Datenarten und Verarbeitungstätigkeiten
- 4. Speicherfristen und Löschfristen
- 5. Löschklassen (z. B. sofort löschen, nach 3 Jahren, dauerhaft archivieren)
- 6. Löschprozesse (organisatorisch und technisch)
- 7. Verantwortlichkeiten
- 8. Kontroll- und Dokumentationspflichten
- 9. Notfall- und Ausnahmeregelungen

Schritt 1: Dateninventur

- Ausgangspunkt: Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Welche Daten werden erhoben, verarbeitet und gespeichert?
- Welche Speicherorte gibt es? (z. B. lokale Server, Cloud, E-Mails)

Schritt 2: Kategorisierung und Zweckbindung

- Wozu dienen die Daten? (z.B. Personalverwaltung, Kundenbetreuung)
- Wann entfällt der Zweck? Bsp. siehe oben.

Schritt 3: Definition von Speicher- und Löschfristen

➔ **Orientierung an:**

gesetzlichen Aufbewahrungsfristen (z. B. HGB, AO, etc.)/internen Erfordernissen (z. B. Garantiezeiten, Rückfragen)

Eine Übersicht zu den gängigsten Aufbewahrungsfristen können wir Ihnen gern zur Verfügung stellen.

Bildung von Löschgruppen, unter die man unterschiedlichste Löschfristen fassen kann

Beispiel

- LG1 – Bewerbung abgelehnt → Löschung nach 6 Monaten
- LG2 – Vertragsunterlagen → 8 Jahre Aufbewahrungspflicht
- LG3 – Newsletter-Abonnenten → Löschung 2 Jahre nach Abmeldung

Schritt 4: Technische Umsetzung

- Implementierung automatisierter Löschroutinen (in CRM-Systemen/Mailprogramm z.B. für den Bewerbungsordner nach sechs Monaten s. o.). Dafür ist es unabdingbar, dass Bewerbungen nur zentralisiert eingehen und nicht im Unternehmen weitergeleitet werden. Anderenfalls ist keine zuverlässige Anknüpfung an die Erfordernisse der notwendigen Löschung möglich.

- Einsatz von Tools (z. B. Datenklassifizierungs- und Bereinigungssoftware)

Schritt 5: Dokumentation und Kontrolle

Gem. Art. 5 II DSGVO gilt das Prinzip der Rechenschaftspflicht: Unternehmen müssen nachweisen können, dass sie DSGVO-konform handeln.

Daher müssen Löschentscheidungen dokumentiert und überprüfbar sein.

Dazu bietet sich eine Checkliste mit z. B. folgenden Inhalten an (für jedes Unternehmen individuell):

Prüffragen zu jedem Projektschritt:

- Sind alle Datenarten und Speicherorte erfasst? (An welchen Stellen im Unternehmen werden Daten erfasst?) -> Problem: wenn es kein einheitliches Vorgehen für die Datenerfassung gibt. -> z.B.: das Vorgehen bei der Datenerfassung ist nicht bei allen Kunden gleich.
- Sind die Rechtsgrundlagen für die Datenverarbeitung bekannt? (Einwilligung oder Rechtsgrundlage?)

- Sind die Löschfristen dokumentiert worden? (Ist von vorneherein klar, wann die abgelegten Daten zu löschen sind? Siehe oben)
- Gibt es dokumentierte Verantwortlichkeiten? (Wer kann, soll und muss die Daten löschen?)
- Gibt es technische Löschprozesse oder manuelle Verfahren? („Sieht“ die eingesetzte Software überhaupt eine Löschung vor? -Vor allem bei „Altsystemen“ problematisch). Hier ist gegebenenfalls eine manuelle Löschung erforderlich.
- Bitte beachten: Technische Probleme oder ein damit verbundener hoher Aufwand befreien grundsätzlich nicht von der Löschverpflichtung!
- Optional mit Ampel- oder Bewertungslogik („erfüllt“/„teilweise/nicht erfüllt“).

Schritt 6: Schulung und Sensibilisierung

- Mitarbeiterschulung für den Umgang mit personenbezogenen Daten und Löschfristen (Schnittmenge zum **Themenbereich Berechtigungskonzept**: Mitarbeiter dürfen nur die Daten zugänglich gemacht werden, die sie für ihre unmittelbare Tätigkeit/Arbeitserbringung benötigen. Ein „weites“ Berechtigungskonzept aus reinen Praktikabilitätsgründen ist nicht zulässig.)

- Einbindung der Fachabteilungen z.B. über Kurzleitfäden oder One-Pager für Fachabteilungen (HR, Vertrieb, Buchhaltung), welche Daten überhaupt mit Blick auf die spätere Löschverpflichtung sinnvollerweise verarbeitet werden sollten.

- E-Learning-Module zum Thema Speicherbegrenzung und Löschpflicht

- Präsentationen für Schulungen (inkl. Fallbeispielen)
- Verhaltensregeln bei Datenanfragen von Betroffenen (es muss sichergestellt sein, dass z.B. bei einem Auskunftsersuchen gemäß Art. 15 DSGVO die Übermittlung nur gegenüber dem Berechtigten erfolgt).
- Eine „Zugänglichmachung“ für Dritte (auch für Personen innerhalb des Unternehmens) ist in den meisten Fällen nicht zulässig (Ausnahme: GF und „echte“ leitende Angestellte).
  (-Anderenfalls kann es zu einem meldepflichtigen Datenschutzvorfall kommen-.)

4. Tipps zur Umsetzung im Unternehmen

- Projektgruppe bilden: Geschäftsführung, IT, Fachabteilungen (Datenschutzbeauftragter)
- Praxisorientiert arbeiten: mit Pilotprojekten (z. B. HR-Daten beginnen)
- Regelmäßige Aktualisierung: Fristen ändern sich, Prozesse auch
- Technische und organisatorische Maßnahmen kombinieren

5. Fazit

➔ Ein Löschkonzept ist kein Luxus, sondern Pflicht.

➔ Ein Löschkonzept muss allerdings für jedes Unternehmen individuell entworfen werden. Einmal erstellt, kann es ohne weiteren Aufwand an neue Erfordernisse angepasst werden.

➔ Löschkonzepte schützen Unternehmen vor Sanktionen (s.o. Urteile), erhöhen die IT-Sicherheit und schaffen Vertrauen.

➔ Mit einem strukturierten Vorgehen lässt sich ein praxistaugliches Löschkonzept auch in kleinen und mittleren Unternehmen problemlos umsetzen.

Zeit für Fragen!?

Herzlichen Dank
für Ihre Aufmerksamkeit!

AGAD Service GmbH
Christopher Pröpper
Waldring 43-47
44789 Bochum
proepper@agad.de
Tel.: 0234/282533 20

AGAD
Partner im Wettbewerb.