

Aufbewahrungspflichten und Löschkonzept

Grundsatz

Personenbezogene Daten dürfen nur so lange gespeichert und verarbeitet werden, wie sie für den jeweils definierten Zweck benötigt werden. Wenn der Zweck nicht (mehr) besteht, müssen sie gelöscht werden, sofern dieser Löschung keine gesetzliche Aufbewahrungsfristen entgegenstehen. Eine unbegrenzte Aufbewahrung ist nicht zulässig.

Dies ergibt sich bereits aus dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchstabe c) DS-GVO:

Personenbezogene Daten müssen ... dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung); ...

Weitere Hinweise:

Art. 30 Absatz 1 Buchstabe f) DS-GVO Verzeichnis von Verarbeitungstätigkeiten

... Dieses Verzeichnis enthält sämtliche folgenden Angaben: ...

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

Im Verarbeitungsverzeichnis muss der Verantwortliche nach Möglichkeit auch die vorgesehenen (Regel-)fristen für die Löschung der verschiedenen Datenkategorien dokumentieren.

Die DS-GVO kennt keine allgemeine statische Regellöschfrist. Vielmehr verpflichtet sie, unverzüglich zu löschen (Art. 17 DS-GVO), sobald das Speicherinteresse entfällt, welche die Verarbeitung rechtfertigte, es sei denn, es greift eine Aufbewahrungspflicht oder eine sonstige Ausnahme von der Löschpflicht (Art.17 Abs. 3 DS-GVO). Die Speicherung muss also auf das unbedingt notwendige Maß beschränkt bleiben (EG 39, S. 8).

Weitere Hinweise:

Dass die DS-GVO keine festen Löschfristen vorsieht, befreit den Verantwortlichen nicht davon, im Einzelfall Löschfristen in einem Löschkonzept zu verankern.

Erwägungsgrund 39 gibt dem Verantwortlichen auf, Fristen für die Löschung oder zumindest für eine regelmäßige Überprüfung vorzusehen, damit die Daten nicht länger als unbedingt nötig gespeichert werden. Er muss also sein Löschkonzept dokumentieren.

Weiteres ergibt sich aus **Art. 25 Abs. 2 DS-GVO**:

Der Verantwortliche hat selbst durch geeignete Voreinstellungen die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um die Löschungsverpflichtung zu erfüllen.

Weitere Hinweise:

§ 75 BDSG Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(2) Der Verantwortliche hat personenbezogene Daten **unverzüglich** zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

Anmerkung: die maßgebliche Unverzüglichkeit ist grds. einzelfallabhängig zu bestimmen.

Das Löschkonzept

Aus den Vorgaben resultiert die Notwendigkeit eines Löschkonzeptes, welche auf der Basis der für die Datenverarbeitung der konkreten Einrichtung geltenden Aufbewahrungsvorschriften die Grundsätze der in einer Einrichtung praktizierten Löschungs routinen widerspiegelt. Darüber hinaus bedarf es entsprechender Dokumentationen, dass die Löschung personenbezogener Daten prozessual gewährleistet ist und auch tatsächlich durchgeführt wird.

Zentrale Punkte eines Löschkonzeptes sind:

1. Zusammenstellung der Verarbeitungsvorgänge und ihrer Datenarten sowie der gesetzlichen Aufbewahrungsfristen
 2. Festlegung der Löschrufen in Abhängigkeit von gesetzlichen Vorschriften und eigenen Zwecken
 3. Übergangsfristen zur endgültigen Löschung
 4. Praktische Durchführung der Löschung bzw. Vernichtung je nach Datenträger bzw. Speichermedium
 5. Protokollierung
 6. Festlegung von Verantwortlichkeiten
 7. Aussagen zum Recht auf Löschung durch Betroffene
-

Praktische Probleme mit der Rechtsvorgabe der Löschung:

1. Gesetzliche Vorschriften enthalten auslegungsbedürftige Rechtsbegriffe,
2. es fällt schwer, das Ende der Verwendung in den einzelnen Arbeitsprozessen und damit letztlich taggenaue Löschfristen festzulegen,
3. Es müssen Personen aus mehreren Fachbereichen beteiligt werden, um die relevanten Prozesse zu beschreiben und es gibt immer Schnittstellen,
4. Es wird befürchtet, dass durch die Löschung Abläufe gestört werden,
5. Es fällt schwer, sich von Datenbeständen zu trennen, weil die Daten „ja noch gebraucht“ werden könnten,
6. Es fällt schwer, die fachlichen Zusammenhänge zu überschauen, da oft Daten in mehreren Prozessen benutzt werden.

Lösung: Festlegung einer systematischen Vorgehensweise.

Die DIN 66398 aus Mai 2016 bietet ein Modell und Hilfestellungen.

Checkliste: Wann müssen Daten gelöscht bzw. vernichtet werden?

Datenträger und Papierunterlagen, die personenbezogene Daten enthalten, müssen gelöscht bzw. vernichtet werden, wenn sie nicht mehr für den **ursprünglichen Zweck** verwendet werden. Eine längere Aufbewahrung darf nur erfolgen, wenn Gesetze oder Rechtsvorschriften dies fordern.

1. Ist der ursprüngliche Zweck der Datenverarbeitung entfallen?

nein: Die Daten sind nach der Zweckbestimmung weiter aufzubewahren.

ja: weiter mit Schritt 2

2. Liegt eine gesetzliche oder sonst verbindliche Aufbewahrungspflicht vor?

nein: Die Daten müssen kurzfristig gelöscht werden.

ja: weiter mit Schritt 3

3. Wann läuft die Aufbewahrungspflicht aus?

Die Aufbewahrungsfrist ist in der Regel in Jahren angegeben.

Fristbeginn: z. B. mit der Abwicklung eines Vertrages/Vorgangs

Fristende: z. B. festgesetzt für das Jahr des Ablaufs der Frist generell am 31.12.

Frist ist abgelaufen: die Daten müssen kurzfristig gelöscht werden.

Frist ist nicht abgelaufen: die Daten müssen bis zum Ende der Frist aufbewahrt werden.

Beispiele relevanter Fristen, die sich aus Rechtsregeln ergeben

§ 147 Absatz 3 Abgabenordnung: 10 Jahre bzw. 6 Jahre

Verjährungsfristen nach dem BGB gemäß §§ 195 ff. BGB (Regelverjährung 3 Jahre)

Die Aufbewahrung legitimiert sich durch den ihr zugrundeliegenden zulässigen Zweck.

Zentral ist der Zweck der ursprünglichen Verarbeitung. Es sind im Laufe der Zeit Zweckänderungen möglich, die – sachlich zulässig begründet – zu einer weiteren Aufbewahrung führen können.

Das Löschkonzept – DIN 66398 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten (Mai 2016)

Die DIN schlägt ein Modell zur Entwicklung und Etablierung eines Löschkonzepts vor. Sie

- beschreibt Vorgehensweisen, durch die Löschrregeln festgelegt werden,
- schlägt Möglichkeiten der Steuerung der Umsetzung der Löschrregeln vor,
- empfiehlt eine Struktur für die Dokumentation,
- empfiehlt Schritte zur Etablierung und Fortentwicklung des Löschkonzepts.

Die DIN legt **nicht** konkrete Löschrregeln, Löschrfristen oder technische Mechanismen fest!

Welche datenschutzrechtlichen Vorschriften einschlägig sind, hängt jeweils von den Zwecken der Verarbeitung im Einzelnen ab.

Die Erarbeitung eines Löschkonzepts kann **organisationsübergreifende Synergieeffekte erschließen**, da zwangsläufig Akteure aus den unterschiedlichsten Bereichen bei der Erstellung und Nutzung zusammenarbeiten müssen.

Das Löschkonzept – DIN 66398 Leitlinie - wesentliche Inhalte:

Definition von Begriffen, u. a.:

Anonymisierung: Verändern pbD derart, dass die hinter den Einzelangaben stehende Person nicht bzw. nicht mehr identifiziert werden kann (**nicht in der DSGVO definiert**)

Pseudonymisierung: Verarbeitung pbD derart, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden, **Art. 4 Nr. 5 DSGVO**.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Aufbewahrungsfrist: Zeitraum, innerhalb dessen die Objekte einer Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein müssen.

Datenart: Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird.

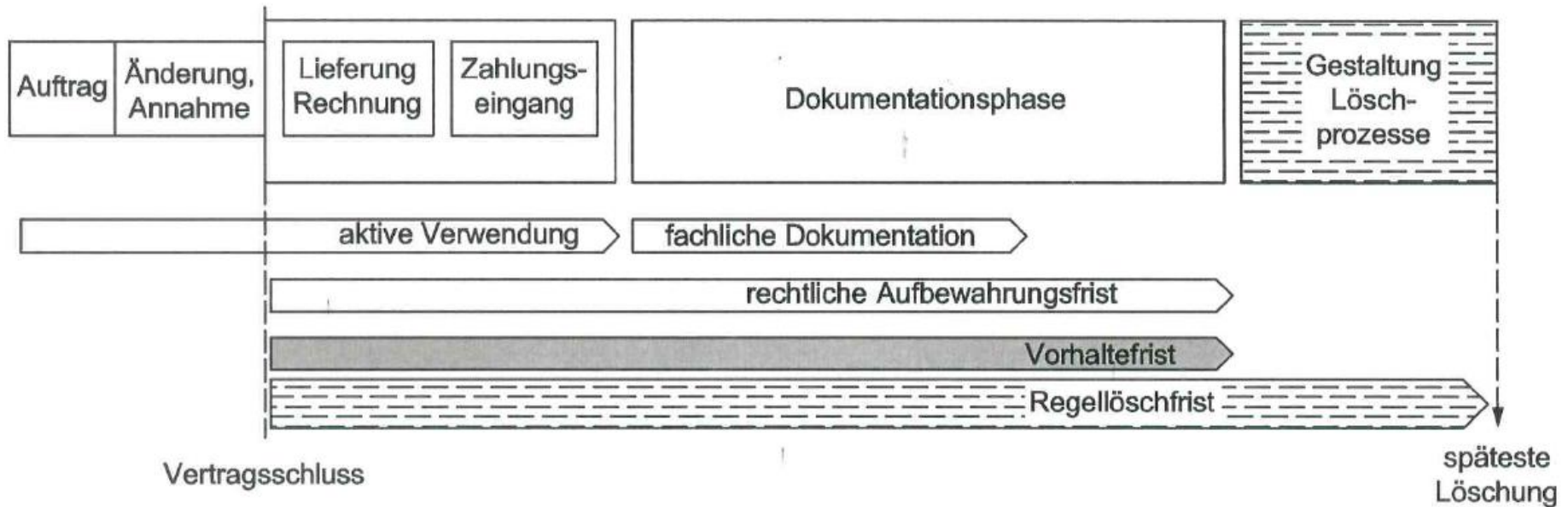
Löschfrist: Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden sollte = Oberbegriff aller Löschrufen.

Regellöschfrist: maximaler Zeitraum, nach dessen Ablauf eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle gelöscht werden sollte.

Standardlöschfrist: vereinheitlichte Löschrufen für die verantwortliche Stelle.

Vorhaltefrist: Zeitraum, innerhalb dessen die Objekte einer Datenart aufgrund der fachlichen Verwendung mindestens verfügbar sein müssen.

Schaubild, „Wiedergegeben mit Erlaubnis von DIN Deutsches Institut für Normung e. V. Maßgebend für das Anwenden der DIN-Norm ist deren Fassung mit dem neuesten Ausgabedatum.“



Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Vorgaben zur Löschung ergeben sich aus den einschlägigen **datenschutzrechtlichen Vorschriften** und aus **weiteren rechtlich bindenden Vorgaben**.

Neben Gesetzen können dies auch z. B. Betriebsvereinbarungen oder Verträge sein. Löschrufen können **vertraglich vereinbart** werden, wenn sie sich im Rahmen des Datenschutzrechts halten, wenn also keine rechtlichen Regelungen dagegen stehen.

Auf die vorhandenen verbindlichen Regelungen muss primär zurückgegriffen werden. Diese bilden den Orientierungsrahmen für die zu erstellenden Löschrufen und reduzieren die Komplexität. Sind solche expliziten Regelungen nicht vorhanden oder zumindest ableitbar, ist eine freie Setzung nach Maßgabe der Verarbeitungszwecke zulässig.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Keine Löschung ohne Regeln

Eine **Löschregel** definiert, **welche Daten** zu **welchem Zeitpunkt** gelöscht werden.
Sie besteht also aus 2 Angaben:

- der Regellöschfrist und
- dem Startzeitpunkt, ab dem die Regellöschfrist läuft.

Mit der Löschregel ist eine geeignete Kombination von Regellöschfrist und Startzeitpunkt zu bestimmen.

Dazu schlägt die DIN die Verwendung von **Löschklassen** vor.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Für jede Datenart eine Löschregel.

Jeder Teil des Datenbestandes, der für einen **einheitlichen fachlichen Zweck** verwendet wird, bildet eine **Datenart**, unabhängig davon, wo die Daten im Einzelnen gespeichert sind. Aus den unterschiedlichen Zwecken, für die die Datenarten verwendet werden, können sich unterschiedliche Regeln für die Löschung ergeben.

Es wird empfohlen, jede Datenart entsprechend ihres Zweckes eindeutig zu benennen (z. B. Abrechnungsdaten, Einzelverbindungsachse, Stammdaten usw.).

Kriterien für die Gestaltung von Datenarten können sich ergeben aus

- unterschiedlichen Personengruppen (Mitarbeiter, Kunden, Externe),
 - die jeweilige Rechtsgrundlage für die Datenverarbeitung,
 - unterschiedliche fachliche Verwendungszwecke,
 - Datenbestände unterschiedlicher Sensitivität.
-

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Nach der Auswahl typischer Datenarten werden Schritte vorgeschlagen, um vereinheitlichende Standardlöschfristen zu beschreiben:

- Datenarten, deren Löschung sich **unmittelbar aus Rechtsvorschriften** ergibt.
 - Wenn für Datenarten **Fristen unzureichend** sind (z. B. wegen der besonderen Sensibilität oder ungenauer Rechtsvorschriften), werden **Prozessanalysen** durchgeführt und eruiert, wie lange ein Geschäftsprozess in der Regel bzw. maximal dauert und welche Schritte er beinhaltet.
 - Für auf diese Weise noch nicht erfasste Datenarten kann einerseits der **spezifische Zweck** verhindern, dass sie zu einer früheren Standardlöschfrist gelöscht werden. Andererseits kann die nächst längere Standardlöschfrist zu lang und damit nicht mehr vertretbar sein.
 - Da eigene fachliche Zwecke eine Aufbewahrung nach dem Ende der aktiven Verwendung rechtfertigen, können für diese verbleibenden Datenarten Standardlöschfristen frei gewählt werden. Die fachlichen Zwecke prägen die Regellöschfrist.
-

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Neben der Fristlänge sind die **Startzeitpunkte** für die Löschfrist Teil der Löschregel. Es gibt im Wesentlichen 3 Typen:

- Zeitpunkt der Erhebung
- das Ende eines – zu definierenden - Vorgangs oder
- das Ende der Beziehung zum Betroffenen.

Löschklassen werden nun gebildet aus den festgelegten **Standardlöschfristen** und den Typen der jeweiligen **Startzeitpunkte**.

Löschklasse = Zuordnung einer Datenart zur Kombination aus Standardlöschfrist und Startzeitpunkt.

Sind Jahresfristen angegeben, **enden** diese in der Regel zum 31.12. eines Kalenderjahres.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Abb. 1 | Matrix von Löschklassen am Beispiel von Toll Collect.⁷

		Standardlöschfristen						
		Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Startzeitpunkte	ab Erhebung			Mautdaten	Mautdaten mit besonderem Analysebedarf			
	Ende des Vorgangs	Web-Logs, nmF	Kurzzeit-Doku, Betriebs-Logs	Voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Reklamations- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
	Ende der Beziehung zum Betroffenen				ergänzende Stammdaten		Verträge	Kernstammdaten

Die gesetzlich motivierten Fristen von 4, 7 und 12 Jahren entstehen, weil die Rechtsvorschriften die Frist erst ab einer Jahresgrenze definieren. Das laufende Kalenderjahr wurde in diesen Fällen zur Standardlöschfrist hinzugerechnet.

Legende

allgemeine Gesetze	spezielle Gesetze	frei gewählt
--------------------	-------------------	--------------

Quelle: Aufsatz von Volker Hammer, DIN 66398 – Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 2016, Heft 8, S. 528, 530.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Sonderfälle bzw. Ausnahmen für eine längere Verwendung:

Handhabung durch Zuordnung dieser Daten zu einer eigenen Datenart, soweit datenschutzrechtlich zulässig oder bei Störfällen zeitweise Aussetzung der Löschung.

Nur dann, wenn **im Einzelfall ein (anderer) Nutzungszweck absehbar** ist (z. B. Beweissicherung im eigenen Interesse hinsichtlich eines Gerichtsverfahrens), ist zulässigerweise eine neue Datenart gegeben.

Differenzierte Handhabung nach **Archivfunktion** und **Sicherungskopiefunktion** erforderlich.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Löschen in Sondersituationen

Nicht nach den allgemeinen Löschrregeln zu löschen ist z. B. in folgenden Situationen:

- das Löschen von unzulässig erhobenen Daten,
 - das Löschen nach berechtigtem Löschrbegehren des Betroffenen (Recht auf Vergessen)
 - das Löschen von Daten im Fall eines Betriebsübergangs oder einer Betriebsaufspaltung.
-

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Mögliche **weitere Kriterien für die Umsetzung** des Löschkonzeptes:

- Differenzierte Festlegung von Umsetzungsvorgaben für IT-Systeme oder andere Datenbestände,
 - Gibt es besondere **technische Anforderungen**?
 - Durch welchen **Mechanismus** wird die Löschung durchgeführt? Wer ist verantwortlich?
 - Welche Kriterien sind anzuwenden, um die zu löschenden Daten von anderen Daten zu trennen?
 - Welche Nachweise sind geeignet dafür, dass die Löschung tatsächlich durchgeführt wurde?
-

Herzlichen Dank für Ihre Aufmerksamkeit!

Paritätischer Wohlfahrtsverband
Landesverband Rheinland-Pfalz/Saarland e. V.
Feldmannstraße 92
66119 Saarbrücken
Elke.Nicolay@paritaet-rps.org
