DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

Aufbewahrungspflichten und Löschkonzept

Rechtlicher Rahmen und wesentliche Inhalte

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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 gesetzlichen Aufbewahrungsfristen entgegenstehen (z. B. aus dem Steuerrecht).

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 u. a. 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.

Exkurs: technische und organisatorische Maßnahmen

Art. 25 Absatz 1 DS-GVO:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

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 der Erstellung eines Löschkonzeptes, welche die Grundsätze der in einer Einrichtung praktizierten Löschungsroutinen 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 Datenarten und der gesetzlichen Aufbewahrungsfristen
2. Festlegung der Löschfristen 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. Recht auf Löschung durch Betroffene

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

Praktische Probleme mit der Rechtsvorgabe der Löschung:

1. Es müssen unbestimmte Rechtsbegriffe ausgelegt werden, um selbst Regeln festzulegen,
2. es gibt eine Vielzahl von Rechtsvorschriften aus unterschiedlichen Bereichen,
3. es fällt schwer, das Ende der Verwendung in Prozessen und damit taggenaue Löschfristen festzulegen,
4. es müssen Personen aus mehreren Fachbereichen beteiligt werden, um die Prozesse zu beschreiben,
5. es wird befürchtet, dass durch die Löschung andere Abläufe gestört werden,
6. es fällt schwer, sich von Datenbeständen zu trennen, weil vage erwartet wird, dass die Daten „ja noch gebraucht“ werden könnten,
7. 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 hierfür 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.

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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

Die DIN definiert ein Vorgehensmodell zur Entwicklung und Etablierung eines Löschkonzepts und

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

Die DIN legt nicht konkrete Löschregeln, Löschfristen 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 DS-GVO 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 DS-GVO.

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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 Löschfristen.

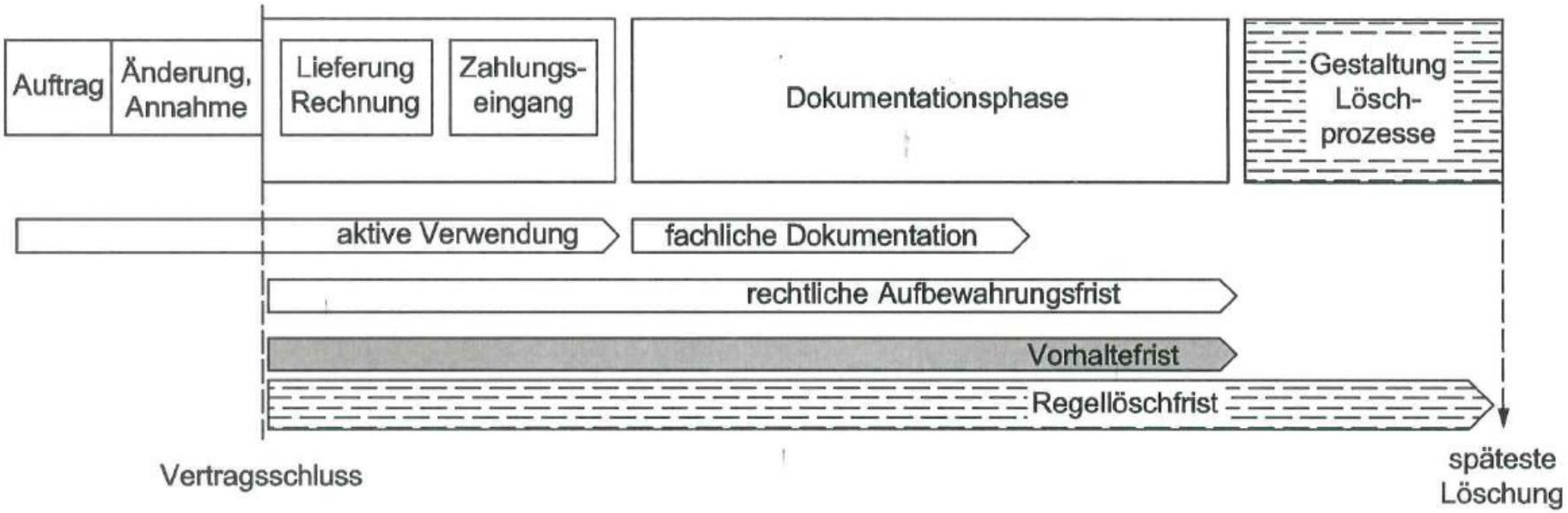
Regellöschfrist: maximaler Zeitraum, nach dessen Ablauf eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle gelöscht werden sollte.

Standardlöschfrist: vereinheitlichte Löschfristen 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. Löschfristen können vertraglich vereinbart werden, wenn sie sich im Rahmen des Datenschutzrechts halten.

Auf explizite verbindliche Regelungen muss primär zurückgegriffen werden. Diese finden Eingang in die zu erstellenden Löschregeln und reduzieren die Komplexität.

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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.

Zentral ist, mit der Löschregel eine geeignete Kombination von Regellöschfrist und Startzeitpunkt zu bestimmen.

Dazu schlägt die DIN die Verwendung von Löschklassen vor.

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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.
Im Sinne einer klaren Kommunikation ist es sinnvoll, jede Datenart eindeutig zu benennen (z. B. Abrechnungsdaten, Einzelverbindungsnachweise, 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, für die sich Fristen unmittelbar aus Rechtsvorschriften ergeben.

- Wenn für Datenarten die 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 danach noch nicht erfasste Datenarten kann einerseits der 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 zudem 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.

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

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

Wesentliche Inhalte der DIN

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

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 für eine längere Verwendung:

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

Differenzierte Handhabung nach Archivfunktion und Sicherungskopiefunktion erforderlich.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Löschen in Sondersituationen

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

- das Löschen von unberechtigt erhobenen Daten,
- das Löschen nach berechtigtem Löschbegehren des Betroffenen,
- das Löschen beim Rückbau von Systemen, oder
- das Löschen von Daten im Fall eines Betriebsübergangs oder einer Betriebsaufspaltung.

Das Löschkonzept – DIN 66398 - wesentliche Inhalte:

Wesentliche Kriterien für die **Umsetzung** des Löschkonzeptes:

- Festlegung von Umsetzungsvorgaben für IT-Systeme oder andere Datenbestände,

- Welche Löschregel gilt für welche Datenart? Gibt es technische Bedingungen für die Auslösung des Fristlaufs?

- Durch welchen Mechanismus wird die Löschung durchgeführt? Wer ist verantwortlich für den Einsatz des richtigen Mechanismus zur Löschung? Welche Kriterien sind anzuwenden, um die zu löschenden Daten von anderen Daten zu trennen?

- Welche Nachweise sind geeignet für die Dokumentation der erfolgten Löschung?

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

Einige wichtige gesetzliche Aufbewahrungsfristen (Jahresfristenende: 31.12.)

Art der Unterlagen	Aufbewahrungsdauer	X = es gibt Sonderfälle	Rechtsgrundlage	Bemerkungen
Arbeitnehmerüberlassung, Unterlagen Entleiher	3 Jahre		§ 7 Absatz 2 AÜG	
Arbeitszeitnachweise (allgemein)	2 Jahre		§ 16 Abs. 2 ArbZG	
Bewerbungsunterlagen	Empfehlung: 6-9 Monate		§ 15 Abs. 4 AGG, § 61 Abs. 1 ArbGG	Variable Klagefristen
Lohnunterlagen	Bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres		§ 28f Abs. 1 SGB IV	nach Sozialversicherung
Gesundheitszeugnis nach IfSG	Bis Ausscheiden des Arbeitnehmers		§ 43 Abs. 5 IfSG	