DIN 66398 – Löschen nach Konzept

Abstract zum Vortrag

Dr. Volker Hammer
Secorvo Security Consulting GmbH

Version 1.0
Stand 29. November 2017

Motivation

Das Löschen personenbezogener Daten wird heute vom BDSG und ab Mai 2018 auch von der Datenschutz-Grundverordnung der EU gefordert. Zahlreiche Artikel der EU-DSGVO definieren Anforderungen an ein Löschkonzept und seine Umsetzung.

In der Praxis gibt es große Umsetzungsdefizite. Das hat zwei Ursachen: Die Löschregeln sind nicht definiert und es fehlen Löschmechanismen in Anwendungen. Der Beitrag motiviert, eine systematische Vorgehensweise für das Löschen zu festzulegen.

Seit April 2016 liegt mit der DIN 66398 eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ vor. Die Norm geht auf ein Industrieprojekt zum Löschen personenbezogener Daten zurück und stellt einen praxistauglichen, effizienten und systematischen Weg vor, wie Löschkonzepte in Organisationen etabliert werden können. Derzeit greifen Organisationen diese Vorgehensweise auf, um mit Blick auf die EU-DSGVO ihre Löschkonzepte aufzusetzen. Der Beitrag gibt einen Überblick über die Inhalte der Norm.

Inhalt der Norm

Die Norm bietet umfangreiche Hilfestellungen, um ein Löschkonzept zu erstellen und in Organisationen zu etablieren:

- Sie beschreibt Vorgehensweisen, durch die Löschregeln festgelegt werden.
- Sie schlägt vor, wie die Umsetzung der Löschregeln gesteuert werden kann.
- Sie empfiehlt eine Struktur für die Dokumente des Löschkonzepts.
- Schließlich gibt die Norm auch Empfehlungen, wie das Löschkonzept etabliert und fortgeschrieben werden kann.

Die größte Hürde für die Löschung personenbezogener Daten ist das Fehlen von Löschregeln. Ohne Löschregeln können keine Mechanismen implementiert werden. Kern der Norm ist deshalb eine Vorgehensweise, um **Löschregeln zu definieren.** Der Datenbestand der verantwortlichen Stelle wird dazu nach (datenschutzrechtlichen) Zwecken in Datenarten unterteilt. Mit Hilfe von Standardfristen und Typen von Startzeitpunkten für den Fristbeginn werden sogenannte Löschklassen gebildet. Die Datenarten können dann leicht in die Löschklassen eingeordnet werden. Daraus ergibt sich je Datenart eine Löschregel mit einem konkreten Startzeitpunkt und einer Regellöschfrist.

Die Löschregeln werden technikunabhängig formuliert. Die Übertragung für konkrete Systeme wird über **Umsetzungsvorgaben** gesteuert. Für diese werden in der Leitlinie die Inhalte beschrieben. Außerdem werden typischen Gruppen von Umsetzungsvorgaben vorgestellt.

Die Norm schlägt eine Struktur für die Dokumente des Löschkonzepts vor. Sie gibt auch Hinweise, wie besondere Situationen – wie beispielsweise Fehler in Datenbeständen – innerhalb eines Löschkonzepts behandelt werden können. Sie empfiehlt zudem, welche Verantwortlichkeiten für eine kontinuierliche Pflege des Löschkonzepts geregelt werden sollten.

Die DIN 66398 macht auch einen Vorschlag zur Organisation eines Projekts „Löschkonzept“, mit dem ein solches Konzept in der Organisation etabliert werden kann. Das Löschen von nicht mehr aufbewahrungspflichtigen oder obsoleten Daten soll als eine „übliche Anforderung“ an IT-Systeme verstanden und durch Regelprozesse umgesetzt werden.

Die Norm fasst Erfahrungen aus sieben Jahren Projektarbeit zusammen. Sie berücksichtigt Praxis-Probleme, ohne die ein umfassendes Löschkonzept nicht etabliert werden kann. Sie bietet ein praxistaugliches und systematisches Vorgehen für Löschkonzepte, weil sie:

- pragmatische Lösungen anbietet, die im datenschutzrechtlichen Rahmen das Löschkonzept so einfach wie möglich gestalten,
- bereits zu Beginn eines Projekts „Löschkonzept“ eine klare Strategie, einheitliche Begriffe und eine Übersicht über notwendige Verantwortlichkeiten und Prozesse anbietet, und damit Fehlschläge und lange Lernkurven vermeidet,
- sehr hohe Effizienz für die Erstellung der Löschregeln erlaubt,
- Unterschiede zwischen Produktion, Archiven und Backups klarstellt und Strategien für deren Behandlung im Löschkonzept vorschlägt,
- Vorschläge anbietet, wie beispielsweise Beweismittel für Rechtsstreite, technische Störungen oder andere Ausnahmefälle behandelt werden können, und
- eine Integration der Dokumentation zum Löschkonzept in vorhandene Dokumente und der zugehörigen Prozesse in bestehende Prozesse der Organisation empfiehlt, soweit dies möglich ist.

Der Beitrag weist außerdem auf zahlreiche positive Nebeneffekte hin, die sich aus der Etablierung eines Löschkonzepts für eine Organisation ergeben können.

Biografie

Dr. Volker Hammer, Dipl. Informatiker, bis 1998 interdisziplinäre Arbeiten zur rechtsgemäßen und verletzlichkeitsreduzierenden Gestaltung bei der Projektgruppe verfassungsverträgliche Technikgestaltung e.V. - provet. Seitdem Mitarbeiter der Secorvo Security Consulting GmbH mit Arbeitsschwerpunkten in Datenschutz und Informationssicherheit. Unter anderem Leiter des Projekts Löschkonzept für die Toll Collect GmbH und Editor der DIN 66398 „Leitlinie Löschkonzept“

Weiterführende Hinweise

Weiterführende Hinweise und Literatur zur DIN 66398 finden Sie unter www.DIN-66398.de

DIN 66398 – Löschen nach Konzept

6. DFN-Konferenz Datenschutz
Hamburg, 28.11.2017

Dr. Volker Hammer

Löschen: Warum denn?

DSGVO – Löschen: generelles Löschen

Regelungsbereich	Fundstellen
Generelles Löschgebot	Artikel 5 (1) d Richtigkeit; (1) e Speicherbegrenzung i.V.m. Artikel 6 Rechtmäßigkeit (1) Zulässige Zwecke, (4) Kriterien für Zweckänderung Artikel 5 (1) c Datenminimierung
technisch-organisatorische Maßnahmen, Aufwand	Artikel 24, Artikel 25 Technikgestaltung und Voreinstellungen Artikel 32 Sicherheit der Verarbeitung (auch unbefugten Zugang ausschließen) Aber: angemessene Mittel, Stand der Technik
Festlegung/Dokumentation von Fristen im Verzeichnis	Artikel 30

DSGVO – Löschen: Informationspflichten, Betroffenenrechte

Regelungsbereich	Fundstellen
Informationspflichten: Fristen	Artikel 13: Erhebung; Artikel 14: andere Quellen; Artikel 15: Auskunft
Löschen auf Antrag	Artikel 17 (u.a. i.V.m Artikel 21 Widerspruchsrecht); Aber Artikel 18: (1) b: Betroffene Person lehnt Löschen ab und fordert Sperren
Durchsetzung durch Aufsichtsbehörde	Artikel 58
Mitteilungspflichten über Löschung	Artikel 19 an Empfänger und Artikel 17 (2) Mitteilungspflicht an „andere Verwender (?)“ (angemessener Aufwand)

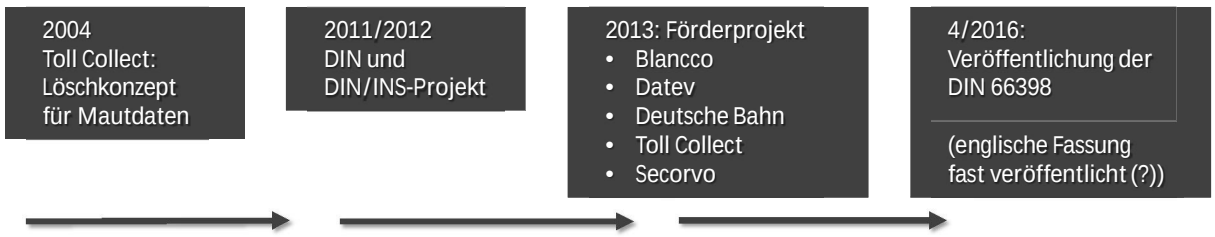
DSGVO – Löschen: Weitere Aspekte

Regelungsbereich	Fundstellen
Dokumentationserfordernisse	Artikel 5: generell; Artikel 24, Artikel 25 und Artikel 32: angemessene technisch-organisatorische Maßnahmen
	ggf. Artikel 33 bei Vorfällen
Auftragsverarbeiter	Artikel 28 (3): Löschen entsprechend Vorgaben des Verantwortlichen und am Ende des Vertrages
Überwachung und Weiterentwicklung Löschkonzept	Artikel 24, Artikel 25 und Artikel 32: angemessene technisch-organisatorische Maßnahmen; ggf. Artikel 33 bei Vorfällen
Sekundärmotivationen	Artikel 83

Löschen??
Wie denn?

DIN 66398

Leitlinie Löschkonzept



Inhalte der DIN 66398

- Elemente eines Löschkonzepts
- Dokumentationsstruktur
- Begriffe
- Vorgehensweise zur Bildung von Löschregeln
- Inhalt von Umsetzungsvorgaben
- Notwendige Verantwortlichkeiten

- Einfachheit ist der Schlüssel zum Erfolg!

Dokumentationsstruktur

Katalog der Löschregeln

Umsetzungs-vorgaben

Umsetzungs-vorgaben

Umsetzungs-vorgaben

Umsetzungs-vorgaben

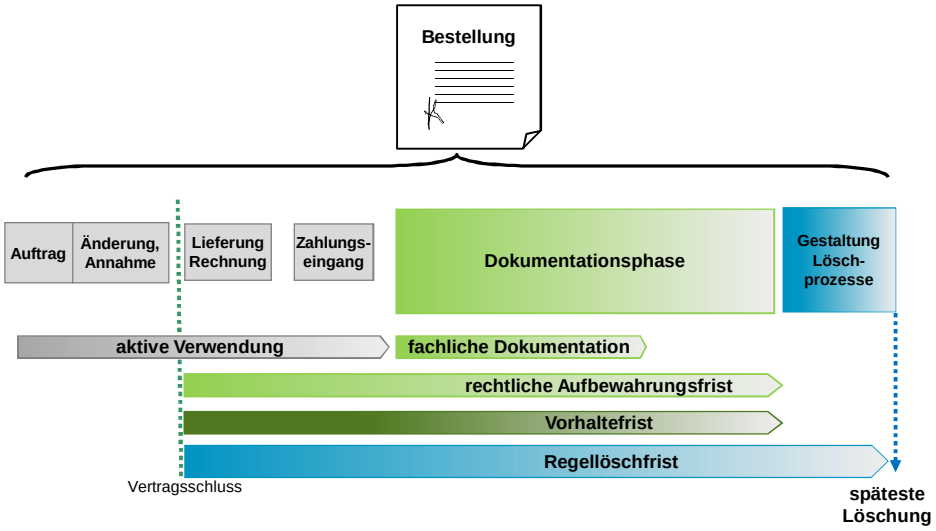
Datenart

Technikunabhängig!

Löschregel

= Frist und Startzeitpunkt
Eine Datenart è eine Löschregel!

Begriffe für die Fristableitung

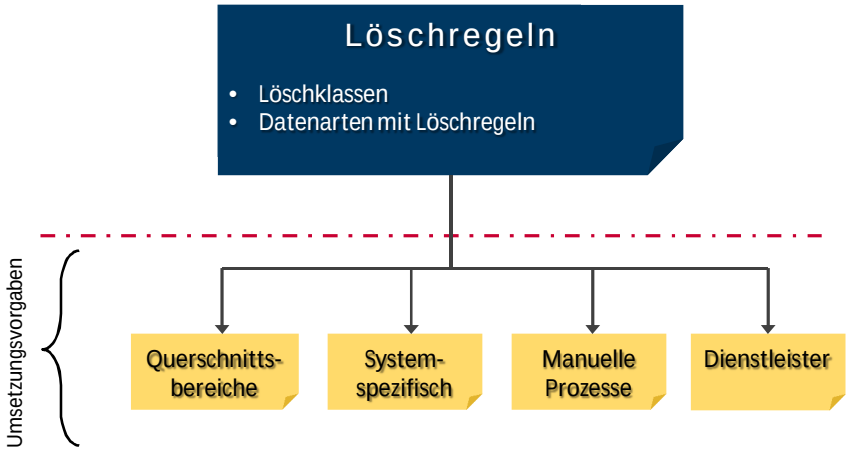


Matrix der Löschklassen

Startzeitpunkte	Sofort	42 T	120 T	1J	4J	7J	12J
Erh			Maut-daten	Mautd. mit bes. Analyse-bedarf			
EdV	Web-Logs, nmF	Kurzzeit-Doku, Betriebs-Logs	Voll erstattete Reklama-tionen	Vorgänge ohne Doku-pflicht	Rekla- und Forde-rungsd.	Handels-briefe	Buch-haltungs-daten
EBB				ergänzende Stamm-daten		Verträge	Kernstamm-daten.

Löschklassen am Beispiel von Toll Collect
(Legende: Fist gelb unterlegt = allgemeine Gesetze, blau unterlegt = spezifische Gesetze, grün unterlegt = frei gewählt
Erh: ab Erhebung; EdV: Ende eines Vorgangs; EBB: Ende der Beziehung zum Betroffenen)

Dokumentationsstruktur



Inhalte von Umsetzungsvorgaben

- Datenarten à Regeln aus dem Katalog
- Jeweils konkrete Frist
- Mechanismen(-stärke)
- Welcher Mechanismus ist wie zu konfigurieren? Wie wird er gestartet?
- Löschläufe dokumentieren
  - (z.B. Parameter des Laufs, Anzahl gelöschter Datensätze, Erfolgs-/Fehlermeldungen)

- Hilfreich:
  - Frist konfigurierbar,
  - muss insgesamt ausgesetzt werden können
  - ggf. einzelne Datenobjekte aus der Löschung ausnehmen

Produktion, Archiv und Backup

Besondere Abläufe: spätere Löschung

- Vorbehalt der Freigabe des Löschlaufs
- Wechsel zwischen Datenarten, z.B. für
  - Rechtsstreit: Beweismittel
  - Verdichtung, „Anonymisierung“ è u.U. längere Fristen?
- Aussetzen der Löschung ist zeitweise möglich, z.B.
  - bei Störfällen
  - mit dem bDSB abgestimmte einmalige Auswertung
  - ...

Löschen, Sperren, Anonymisieren

Nutzen für den Datenschutz

- Lösch-Compliance
  - Definition der Löschregeln (Verzeichnis)
  - Löschen wird umgesetzt
  - Dokumentierte Lösch-Maßnahmen
- Allgemeine Compliance
  - Rechtsgrundlagen/Zulässigkeit von Prozessen werden überprüft
- Datenschutz-Prozesse
  - Bessere Dokumentation von Verantwortlichen, Systemen und Geschäftsprozesse
  - Arbeitsgrundlage für Auskunft und Löschanfragen
- Datenschutz verankern
  - Geschäftsprozesse mitgestalten
  - IT-Prozesse und Changes begleiten
  - Integration in (andere) Regelprozesse
  - Chance auf bessere Datenschutz-Kultur

Mehr Nutzen durch ein Löschkonzept

- Datenschutz
  - Compliance
  - Arbeitsgrundlagen für DS-Prozesse
  - Verankerung DS in der Organisation
- Fachabteilungen
  - Geschäftsprozesse präzisieren
  - Datenschiefstände beseitigen
  - Vorgaben für Datenhaltung, gute Büroorganisation
- IT: Entwicklung und Betrieb
  - Altsysteme abschalten
  - einfachere Projekte: Ballast/Migration wird reduziert
  - Daten reduzieren und konsolidieren: Stabilität und Performanz
- IT-Sicherheit
  - Synergieeffekte/Zusammenarbeit
  - bessere Übersicht über Datenbestände
  - Verringerung der Angriffsfläche
  - nicht-pbD löschen?

Quellenangaben

- Bilder Titelfolie, Agenda, etc.: Wolfram Sieber/Fotoskop.de
- Bild Schlussfolie (Visitenkarte): harmonicdesign/Bigstock.com
- Grafiken zur „Dokumentationsstruktur“, „Begriffe Fristableitungen“, „Matrix der Löschklassen“ in Anlehnung an
  - DIN 66398 (Beuth Verlag) und
  - Leitlinie Löschkonzept (Secorvo.de > Publikationen > 2012)

Materialien

- DIN 66398: Beuth-Verlag
- Leitlinie Löschkonzept (Vordokument zur Norm): Secorvo.de > Publikationen > 2012
- Hammer, V: DIN 66398, DuD 8/2016 (gibt einen Überblick) Secorvo.de > Publikationen > 2016
- Weitere Informationen auch unter: www.DIN-66398.de