Löschen? Löschen. Löschen!

Abstract und Folien
zum Vortrag am 22.05.2017 auf dem Entwicklertag in Karlsruhe

Dr. Volker Hammer
Secorvo Security Consulting GmbH

Version 1.2
Stand 22. Mai 2017

1 Zusammenfassung

Das Löschen personenbezogener Daten wird heute vom BDSG und ab 2018 auch von der Datenschutz-Grundverordnung der EU gefordert. 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, Löschen als eine wichtige Anforderung aufzugreifen, und bereits zu Beginn von Entwicklungsprojekten zu berücksichtigen. Entwickler sollten deshalb für die Fragestellung sensibilisiert sein.

Die DIN 66398, die durch mehrjährige Praxiserfahrungen des Referenten geprägt ist, gibt konkrete Hilfestellungen bei Löschprojekten: Sie schlägt vor, wie Löschkonzepte etabliert werden sollten und bietet eine effiziente Vorgehensweise zur Ableitung von Löschregeln. Löschprojekte können außerdem positive Wirkungen nach sich ziehen, die weit über die Datenschutz-Anforderungen hinausgehen.

Um **Löschregeln** zu definieren, kann die Vorgehensweise der im April 2016 erschienen DIN 66398 verwendet werden: Mit Hilfe von Standardfristen und Typen von Startzeitpunkten werden Löschklassen gebildet. Abgegrenzte Arten personenbezogener Daten können dann leicht in die Löschklassen eingeordnet werden. Daraus ergeben sich die Löschregeln mit je einem Startzeitpunkt und einer Regellöschfrist. Diese Löschregeln sind die Grundlage für die Implementierung von Löschmechanismen. Dazu werden für verschiedene Bereiche sogenannte Umsetzungsvorgaben entwickelt.

Mechanismen zur Löschung können sehr unterschiedlich implementiert werden. Entwurfsentscheidungen sind z.B. abhängig vom Verarbeitungsprozess, der Einbettung des Systems in die IT-Landschaft oder Datenvolumen. Beispiele für Implementierungsansätze sind:

- Transport-Files, Log-Files etc.: dateibasiertes Löschen
- Massendatenverarbeitung: partitionieren von Tabellen nach Zeitscheiben und „Drop Table“
- Datensätze in Datenbanken: (SQL-)Statements auf Tabellen
- Attribut-Ebene: Überschreiben von Werten
- Objektorientierte Ansätze z.B.: Die Klasse „kennt“ die Regellöschfrist; über weitere Attribute kann der Startzeitpunkt und ein „aussetzen-Flag“ gesetzt werden. Über Methoden könnten die löschfälligen Datensätze identifiziert und dann auch gelöscht werden.
- Archivieren und Löschen der Archivdateien, bspw. in SAP

Allgemeine Anforderungen an Löschmechanismen:

- Die Löschfrist sollte konfigurierbar sein

- Der Mechanismus muss insgesamt ausgesetzt werden können.
- Je nach Datenart kann es notwendig sein, einzelne Datenobjekte zeitweise aus der Löschung auszunehmen
- Es sollte „sicher“ gelöscht werden.
- Löschläufe sollten dokumentiert werden (z.B. Parameter des Laufs, Anzahl gelöschter Datensätze, Erfolgs-/Fehlermeldungen)

Die Vorgehensweise kann auch für nicht-personenbezogene Daten angewandt werden.
Nutzen – neben der datenschutzgerechten Gestaltung von Prozessen – kann sich u.a. ergeben, weil

- Geschäftsprozesse präzisiert werden
- Systeme und IT-Prozesse entkoppelt werden
- Vorgaben für die Datenhaltung getroffen werden
- überflüssige Daten aufgeräumt und Redundanzen abgebaut werden. Dadurch sinken Kosten für den IT-Betrieb und für Migrationen.

Biografie

Dr. Volker Hammer, Dipl. Informatiker, bis 1998 interdisziplinäre Arbeiten zur rechtsgemäßen und verletzlichkeitsreduzierenden Gestaltung. 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“

2 Folien

Löschen? Löschen. Löschen!

Entwicklertag
Karlsruhe, 22.05.2017

Dr. Volker Hammer

secorvo
security consulting

Löschen??

Was denn?

Löschen??
Warum denn?

Löschen? Warum denn?

- Datenschutz fordert: Löschen personenbezogener Daten
  - sobald für zulässige Zwecke nicht mehr erforderlich
- Auch nach EU-DSGRVO
- Gilt ab Mai 2018
- Artikel 83 EU-DSGVO: „wirksame“ Geldbußen
  - Bis zum Maximum von € 20 Mio und 4% weltweitem Jahresumsatz (u.a. Verstöße gegen Prinzipien)
  - Bis zum Maximum von € 10 Mio und 2% weltweitem Jahresumsatz (u.a. Verstöße Umsetzung)
- Überraschender „Zusatznutzen“

Löschen.
Wie denn?

DIN 66398

Leitlinie Löschkonzept

2004
Toll Collect:
Löschkonzept
für Mautdaten

2011/2012
DIN und
DIN/INS-Projekt

2013: Förderprojekt
- Blancco
- Datev
- Deutsche Bahn
- Toll Collect
- Secorvo

4/2016:
Veröffentlichung der
DIN 66398

(englische Fassung in
Arbeit)

Kernelemente der DIN 66398

Inhalte der DIN 66398

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

- Schlüssel zum Erfolg: Einfachheit!!!

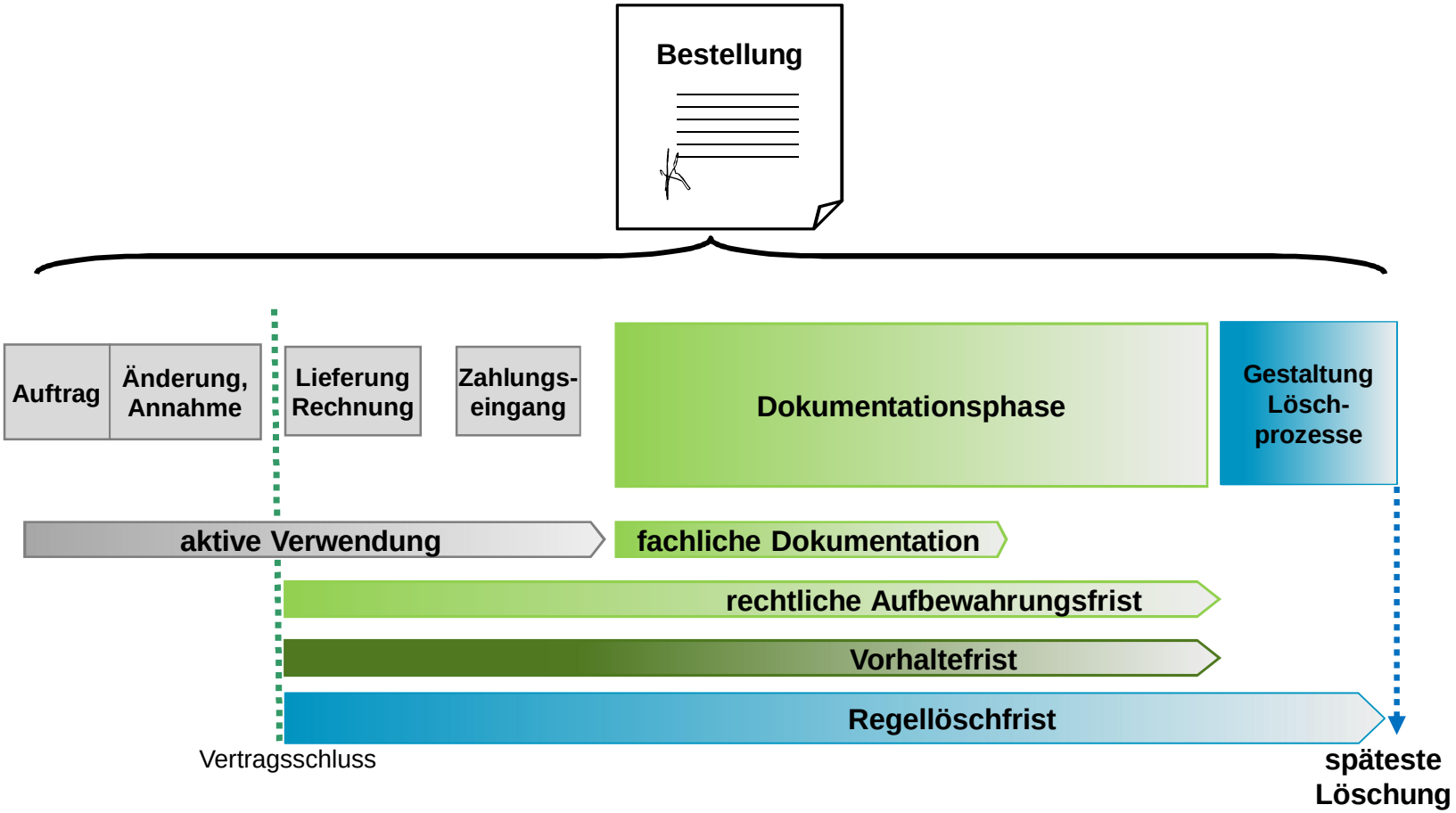
Datenart

Löschregel

= Frist und Startzeitpunkt

Eine Datenart è eine Löschregel!

Begriffe für die Fristableitung



Matrix der Löschklassen

Standardlöschfristen

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

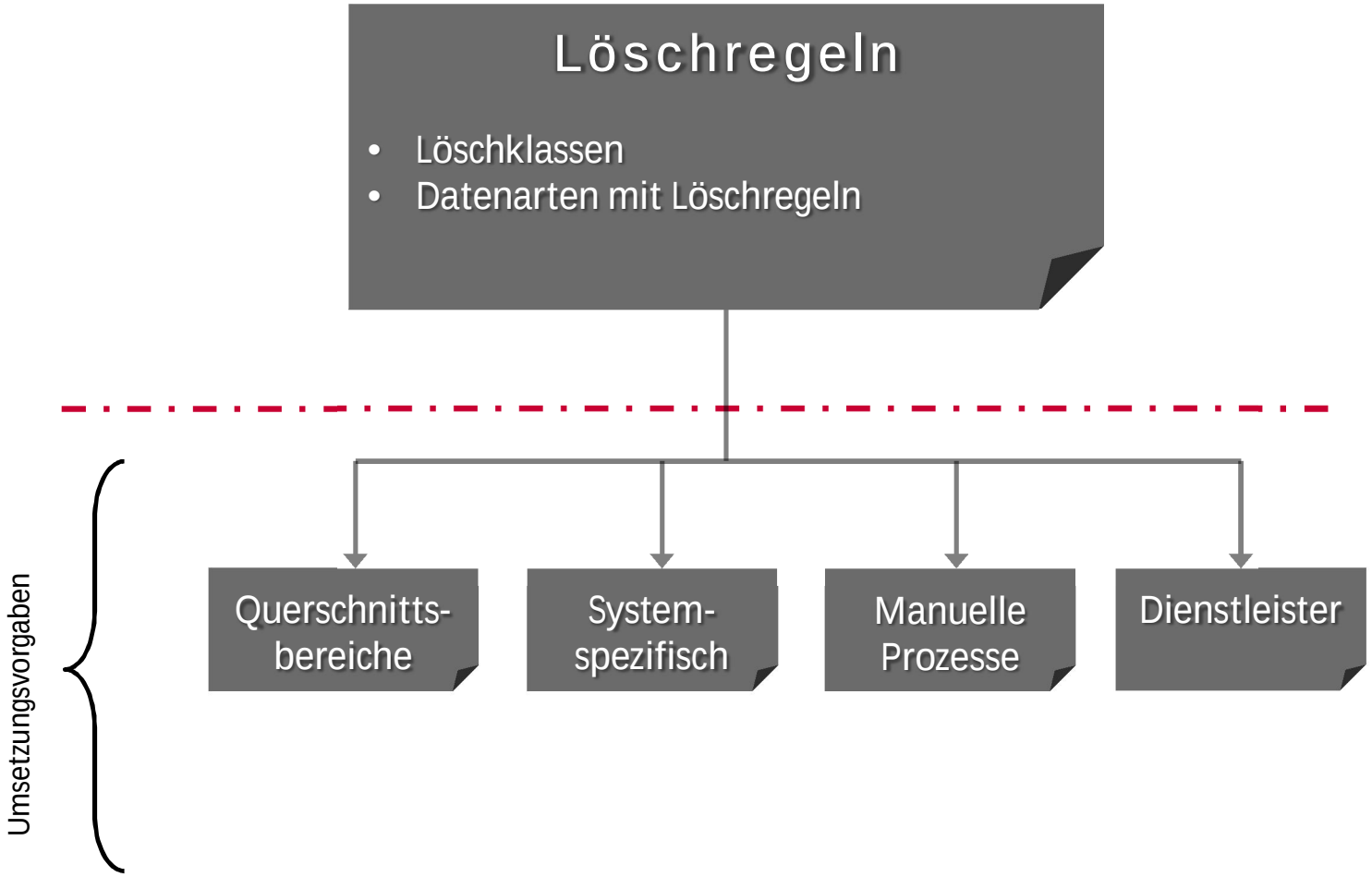
(Legende: Fist gelb unterlegt = allgemeine Gesetze, blau unterlegt = spezifische Gesetze, grün unterlegt = frei gewählt

Erh: ab Erhebung; EdV: Ende eines Vorgangs; EBB: Ende der Beziehung zum Betroffenen)

Umsetzung/Mechanismen

Umsetzungsvorgaben

Dokumentationsstruktur



Anforderung für Anwendungen

- „Technische“ Löschregeln für Datenarten im System
- Die Löschfrist sollte konfigurierbar sein
- Mechanismus muss insgesamt ausgesetzt werden können.
- Ggf. einzelne Datenobjekte aus der Löschung ausnehmen
- Es sollte „sicher“ gelöscht werden.
- Löschläufe dokumentieren
  - (z.B. Parameter des Laufs, Anzahl gelöschter Datensätze, Erfolgs-/Fehlermeldungen)

Ideen für Mechanismen

- Transport-Files, Log-Files etc: dateibasiertes Löschen
- Massendatenverarbeitung: partitionieren, „Drop Table“
- Datensätze in Datenbanken: (SQL-)Statements auf Tabellen
- Attribut-Ebene: Überschreiben von Werten
- Objektorientierte Ansätze z.B.:
  - Die Klasse „kennt“ die Regellöschfrist;
  - Weitere Attribute: Startzeitpunkt und „Aussetzen-Flag“
  - Methoden zum Identifizieren und Löschen von Datensätzen.
- Archivieren und Löschen der Archivdateien, bspw. in SAP
- Steuerung der Löschung durch einen Löschvorrat (z.B. DMS)


Kosten? Nutzen!

Nutzen

- Datenschutz einhalten
- Geschäftsprozesse präzisieren
- Vorgaben für die Datenhaltung treffen
  è “gute Büroorganisation“
- Systeme und IT-Prozesse entkoppeln
- Überflüssige Daten aufräumen, Redundanzen abbauen
  è Vorteile für IT-Betrieb und Migrationen
- Verbesserungen für die Informationssicherheit
  è Transparenz über Datenbestände, Angriffsfläche reduzieren

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


TOP
CONSULTANT
IT-Berater
2015
secorvo
security consulting
Ettlinger Str. 12-14
76137 Karlsruhe
Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de