Löschkonzepte nach DIN 66398 und Aspekte für den Betriebsrat

Abstract zum Vortrag auf der Tagung
„Neue Technologien und Datenschutz – Konferenz für Mitarbeitervertretungen“
am 09. November 2021 in München

Dr. Volker Hammer
Secorvo Security Consulting GmbH

Version 1.0
Stand 09. November 2021

Motivation

Das Löschen personenbezogener Daten wird heute von der Datenschutz-Grundverordnung der EU (DSGVO) gefordert.[1] Zahlreiche Artikel der 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. Die Norm wurde in den internationalen Standard ISO/IEC 27555 übertragen und 2021 veröffentlicht. Inhaltlich gibt es in der Vorgehensweise keine Unterschiede.[2]

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.

1 Eine inhaltlich entsprechende verpflichtende Anforderung besteht seit 1990, vorher war es eine Kann-Bestimmung.

2 Hinweise zu Unterschieden gibt https://din-66398.de/inhalt/bezuege/bezuege_iso_27555.html.

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.

Aspekte der Mitbestimmung

Da viele Datenarten auch die personenbezogenen Daten von Beschäftigten betreffen, erscheint es sinnvoll, dass der Betriebsrat die Definition der Löschregeln begleitet.

In Betriebsvereinbarungen können zum Schutz der Beschäftigten auch Regeln zur Löschung der Beschäftigtendaten vereinbart werden. Diese Löschregeln sollten nach Möglichkeit aber in die Dokumentationsstruktur nach DIN 66398 eingebettet werden. Dadurch wird erreicht:

- Ein zentrales Nachschlagewerk weist alle Löschregeln der Organisation nach.
- Die Beschreibung der Löschregeln ist präzise, weil sich die Definition an einem bewährten Schema orientiert.
- Die Löschregeln können konsistent gepflegt werden, weil sie nur ein einer Stelle definiert werden.

Auf die vereinbarten Löschregeln wird dann aus der BV verwiesen. Sie sind dann als ausgelagerter Anhang zu verstehen. Damit dürfen sie auch nur mit Zustimmung des Betriebsrates verändert werden. Um dies sicherzustellen, erscheint es sinnvoll, eine Grundlagen-BV zum Löschkonzept zu schließen, in der der Änderungsprozess und die Mitwirkung der Betriebsrats geregelt wird. Ein eine solche Mitwirkung erscheint grundsätzlich für alle Datenarten sinnvoll, mit denen die Löschung von Beschäftigtendaten festgelegt wird, auch wenn sie nicht direkt in Betriebsvereinbarungen genannt werden.

Schließlich verwendet der Betriebsrat selbst personenbezogene Daten von Beschäftigten. Er muss sicherstellen, dass dafür Löschregeln (im Regelkatalog) definiert sind. Dies Löschregeln kann er anwenden, indem er eigenen Umsetzungsvorgaben im Sinne der DIN 66398 festlegt.

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, Editor der DIN 66398 „Leitlinie Löschkonzept“ und Co-Editor für den Standard ISO/IEC 27555. Ich unterstütze Unternehmen dabei, ihr Löschkonzept zu etablieren, am liebsten mit Hilfe zur Selbsthilfe.

Weiterführende Hinweise

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

Zum Thema Löschkonzept und Mitbestimmung:
Hammer, V. / Schuler, K. (2016): Löschen nach Regeln – die neue Norm hilft, CuA – Computer und Arbeit, 1/2016, 30 ff.;
Download: Secorvo.de > Publikationen > 2016
(auch cua-web.de)

Löschkonzepte nach DIN 66398 und Aspekte für den Betriebsrat

Konferenz „Neue Technologien und Datenschutz“
München, 09.11.2021

Dr. Volker Hammer

Löschen??

Was denn?

Personenbezogene Daten

sind alle Informationen,
die sich auf eine identifizierbare
natürliche Person beziehen

- Alle möglichen Merkmale zur Identifikation berücksichtigen!
- **Richtiges Anonymisieren** ist gleichwertig

Löschen??
Warum denn?

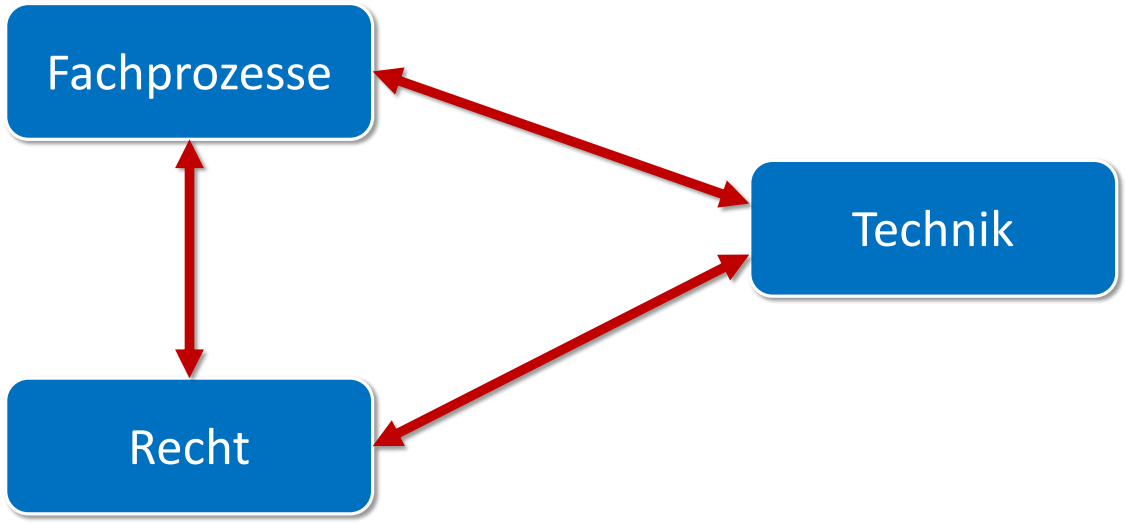
EU Datenschutz-Grundverordnung (DSGVO)

- Generelles Löschen gefordert nach Artikel 5 DSGVO
  - Zulässigkeit, Datenminimierung, Speicherbegrenzung
- Löschen im Einzelfall auf Antrag: Artikel 17 DSGVO
  - Recht auf Vergessenwerden, unter bestimmten Bedingungen
- Recht auf Sperren (= auch „nicht Löschen“): Artikel 18 DSGVO
- Informations-, Dokumentations-, Mitteilungs- und Nachweispflichten
  - Artikel 5 (2), 12, 13 bis 15, 16, 19, 24, 30, 32, ... DSGVO

- Artikel 83 EU-DSGVO: „wirksame“, „abschreckende“ Geldbußen

Löschen??
Wie denn?

Technikgestaltung „Löschen“



DIN 66398

Leitlinie Löschkonzept

2004
Toll Collect: Löschkonzept für Mautdaten

2011/2012
DIN und DIN/INS-Projekt

2013:
Normungsprojekt durch Förderunternehmen
- Blancco
- Datev
- Deutsche Bahn
- Toll Collect
- Secorvo

4/2016:
Veröffentlichung der DIN 66398

12/2017:
englische Fassung

Ab Herbst 2018 bei ISO
Standardisierungsprojekt

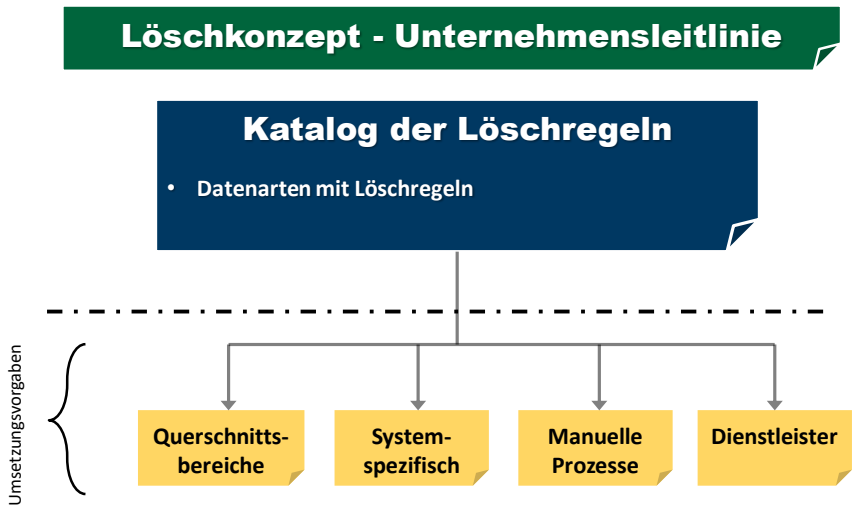
10/2021: Publikation ISO/IEC 27555

Die Elemente der DIN 66398

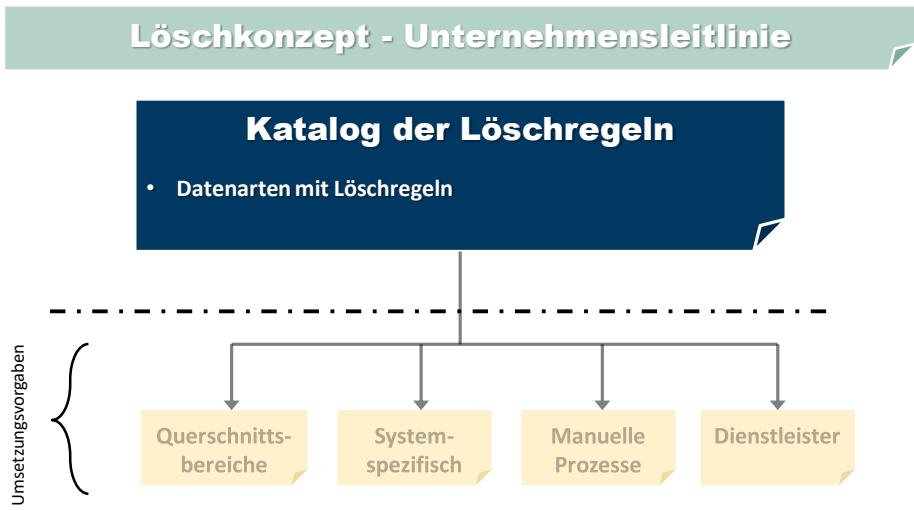
- Dokumentationsstruktur eines Löschkonzepts
- Begriffe
- Vorgehensweise zur Bildung von Löschregeln
- Inhalt von Umsetzungsvorgaben
- Notwendige Verantwortlichkeiten

- Einfachheit ist der Schlüssel zum Erfolg

Dokumentationsstruktur



Dokumentationsstruktur



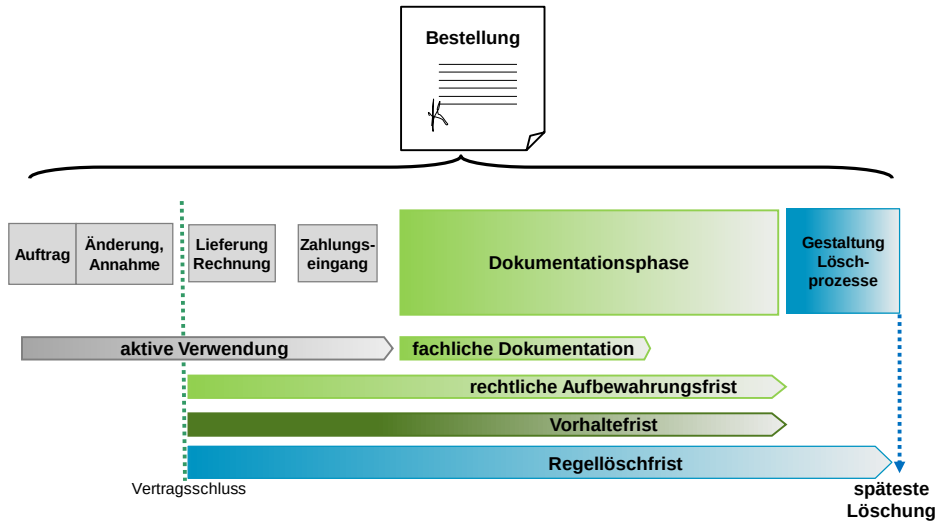
Datenart

Datenschutzrechtlich einheitliche Zwecke
Technikunabhängig!

Löschregel

= Frist und Startzeitpunkt
Eine Datenart ➔ eine Löschregel!

Begriffe für die Fristableitung



Matrix der Löschklassen

Standardlöschfristen

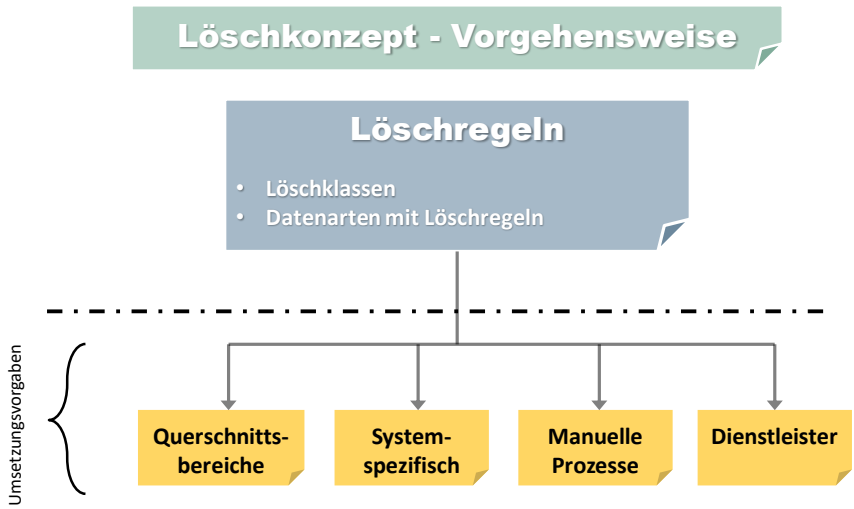
Startzeitpunkte	Sofort	42 T	120 T	1J	4J	7J	12J
Erh			Maut-daten	Mautd. mit bes. Analyse-bedarf			
EdV	Web-Logs, nmF	Kurzzeit-Doku, Betriebs-Logs	Voll erstattete Reklama-tionen	Vorgänge ohne Doku-pflicht	Rekla- und Forde-rungsd.	Handels-briefe	Buch-haltungs-daten
EBB				ergänzende Stamm-daten		Verträge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

Umsetzungsvorgaben

Umsetzungsvorgaben in der Dokumentationsstruktur



Geltungsbereiche: Produktion, Archiv und Backup

- Löschregeln gelten auch in Archiven
- Löschregeln gelten auch für Datenabzüge/Datenträger (Ausnahmegenehmigungen???)
- Backups werden gesondert behandelt
- Testsysteme, Entwicklung ???
  ➔ keine Produktivdaten (oder Ausnahme/spezielle Regelung)

Besondere Abläufe: spätere Löschung

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

Aufgaben des Betriebsrats bezüglich „Löschen“

- Betriebsrat trägt (auch) Sorge für Schutzrechte der Beschäftigten
  - Löschverpflichtung für Verantwortliche ist Teil des Datenschutzrechts
    - ➔ Kann vom Betriebsrat für die Beschäftigtendaten eingefordert werden
- Löschen in IT-Systemen kann mindestens beeinflussen
    - Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb
    - Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen
  - ➔ Mitbestimmungspflichtig nach § 87 BetrVG,
    BR sollte mitwirken an Löschregeln (und Umsetzung)
- Verhältnis Betriebsvereinbarungen und Regelkatalog
- Datenbestände beim Betriebsrat fallen unter die Löschpflicht
  - ➔ Löschregeln für den Betriebsrat

Mitwirken am Regelkatalog

Phase Regelkatalog: Was tut der Betriebsrat?

- Im Unternehmen ein eigenes Projekt
  - Wie wird der Regelkatalog erstellt?
  - BR kann sich einklinken in die wichtigen Datenarten
- Mitwirken an der Definition von Datenarten und Löschregeln
- Review des Regelkatalogs vor der Freigabe
  - (mindestens) die wichtigen Datenarten prüfen

Balance zwischen Differenzierung und wenigen Datenarten

- Empfehlung der DIN:
  - Einfache Datenarten
  - Einfache Löschregeln
  - So wenig Datenarten wie möglich, so viele wie nötig

- Warum?
  - Auch mit der DIN 66398 ist das Löschkonzept sehr aufwändig
  - Die Beteiligten müssen die Löschregeln umsetzen können
  - Weniger Datenarten erleichtern das Verständnis und die Umsetzung

Beschäftigtendaten in anderen Datenbeständen

Beispiel Kundenbetreuung: Datensatz in einer Datenbank

Allgemeine Korrespondenz
(Betroffener = z.B. Mieter)

Ansprechpartnerin: Fr. Müller

Created by: Mitarbeiter X, Datum
(Betroffener = Beschäftigter)

- In vielen Datenbeständen sind neben den Nutzdaten (gelb)
  - auch Informationen zu verantwortlichen Mitarbeiter.innen (blau)
  - und Bearbeiterdaten (blau unterlegt) enthalten
- Verantwortlichen Mitarbeiter.innen sind Betroffene
  - Typischerweise Teil der Nutzdaten → gleiche Löschregel
- Die Bearbeiter sind auch Betroffene

Fragestellungen zu Bearbeiterdaten

- Zu welchem Zweck werden die Bearbeiterdaten verwendet?
  - Sind sie als Teil des Datensatzes aufzufassen?
  - Sind für die Bearbeiterdaten andere Löschregeln zu definieren als für die Nutzdaten?
- Wie können die Beschäftigten vor Missbrauch geschützt werden?
  - Genereller Ausschluss von Leitungs- und Verhaltenskontrolle?
    - Ausnahmen: Für jeden Datenbestand/ jede Anwendung konkrete Zwecke für die Leistungs-/ Verhaltenskontrolle definieren

Betriebsvereinbarungen und Löschregeln

Empfehlung: Löschregeln für Beschäftigtendaten ausschließlich im Regelkatalog

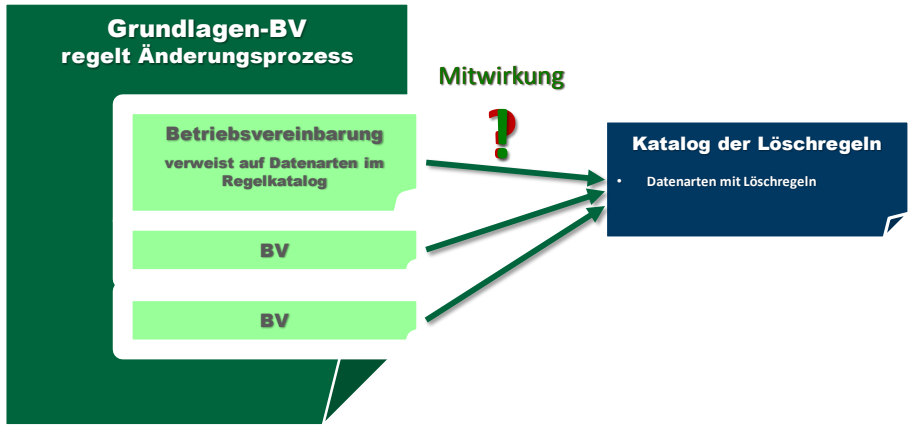
- DIN 66398: Regelkatalog ist DAS zentrale Dokument für Löschregel
  - Eine Stelle zum nachschlagen

➔ Auch Löschregeln für Beschäftigtendaten sollen möglichst im Regelkatalog definiert werden

  - Nur so wird Konsistenz und Übersichtlichkeit erreicht

Änderung vereinbarter Datenarten?

- Betriebsvereinbarungen verweisen auf den Regelkatalog



- BR muss an der Änderung solcher Datenarten und Löschregeln mitwirken

Änderungsverfahren für Löschregeln, z.B.:

- Eine Organisationseinheit ist verantwortlich für die Pflege des Regelkatalogs
- Änderungen werden dort beantragt
  - Beschäftigtendaten betroffen?
    - Information des Betriebsrats
    - Betriebsrat kann mitwirken
  - Für die Freigabe der Änderungen
    - Betriebsrat wird beteiligt und hat im Rahmen der Mitbestimmungsrechte Einfluss
- Verfahren kann in einer Grundlagen-BV zum Löschen vereinbart werden

Eigenen Daten des Betriebsrats

Personenbezogen Datenbestände des BR, z.B.

- Wahlakten Mitbestimmungsgremien
- Merkmale von Beschäftigten beim BR
  - wie erweiterte Stammdaten Beschäftigte
- Personalplanungsdaten
- Niederschriften von Mitbestimmungsgremien
- Betriebsvereinbarungen:
  „Dokumente der Wissensbasis und Unternehmensorganisation“

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) Download: Secorvo.de > Publikationen > 2016
- Hammer, V. / Schuler, K. (2016): Löschen nach Regeln – die neue Norm hilft, CuA – Computer und Arbeit, 1/2016, 30 ff.; auch cua-web.de Download: Secorvo.de > Publikationen > 2016
- Weitere Informationen auch unter: www.DIN-66398.de
- ISO/IEC 27555:2021: Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion