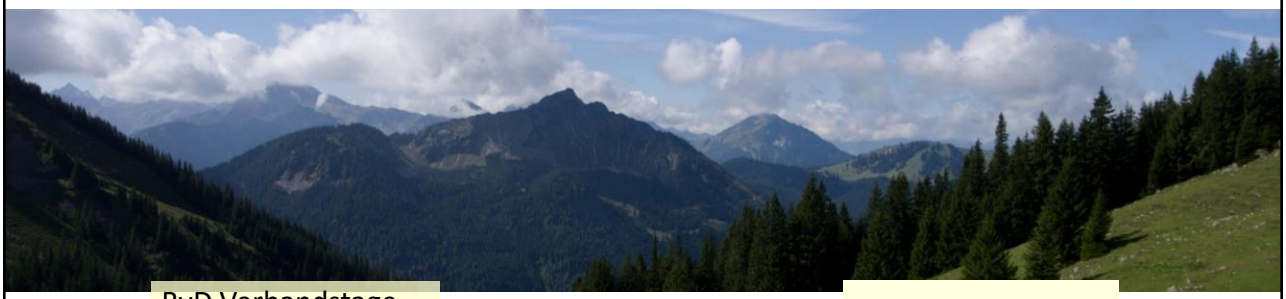
DIN 66398
Die Basis für Löschkonzepte



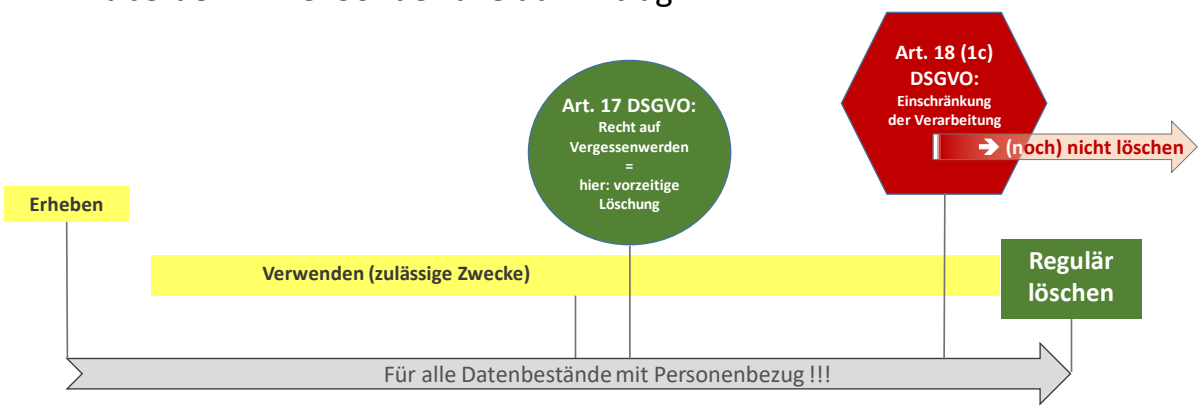
BvD Verbandstage
Berlin, 10.05.2023

Dr. Volker Hammer
Löschprojekte.de

Der Rahmen: Grundsätze in der DSGVO
Art. 5 (1e) **Speicherbegrenzung für personenbezogene Daten**

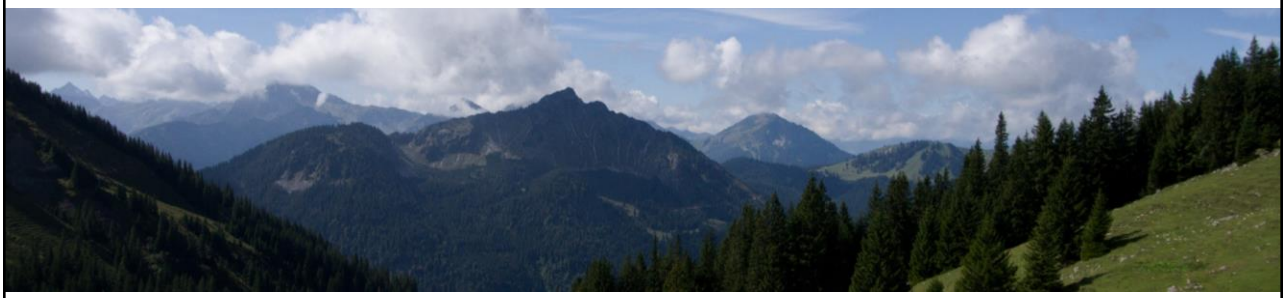
- Zulässige Zwecke

Außerdem: zwei Sonderfälle auf Antrag



Schöne Aussichten? Herausforderungen!

- Berge über Berge von Daten! = **Was liegt eigentlich wo?**
- „Wir könnten ‚sie' doch noch mal brauchen!?" = **Unsicherheit!**
- Wie sollen wir löschen? = **Ohne Regeln keine Löschung!**
- Konkrete Maßnahmen? = **Viele Umsetzungsaufgaben!**

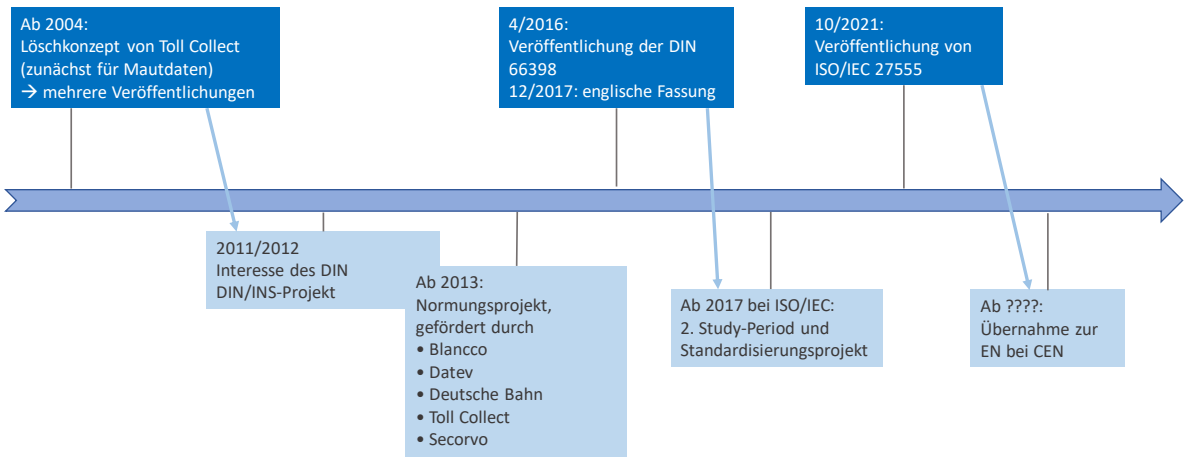


Wie löst eine Organisation diese Aufgabe dauerhaft?

Vorschlag zur Vorgehensweise

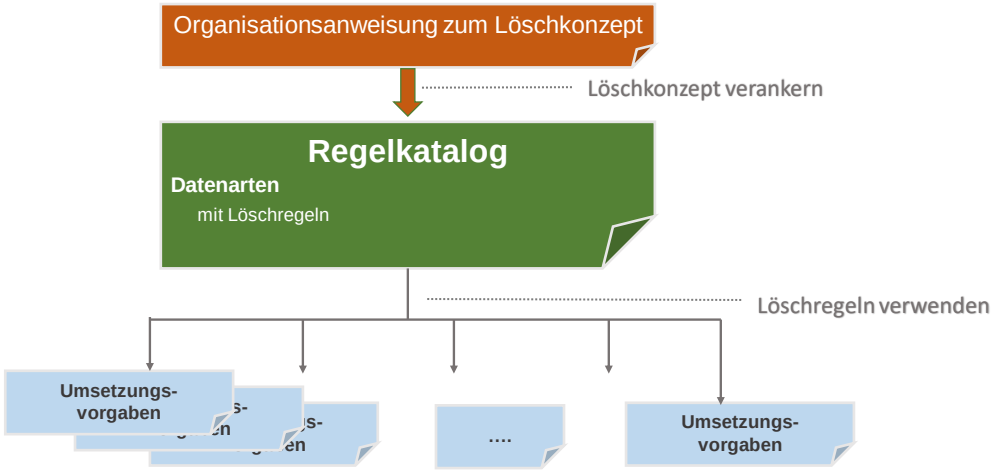
DIN 66398
„Leitlinie Löschkonzept“

Wie kam es zur Norm?



Kernelemente der DIN 66398

Dokumentationsstruktur



9

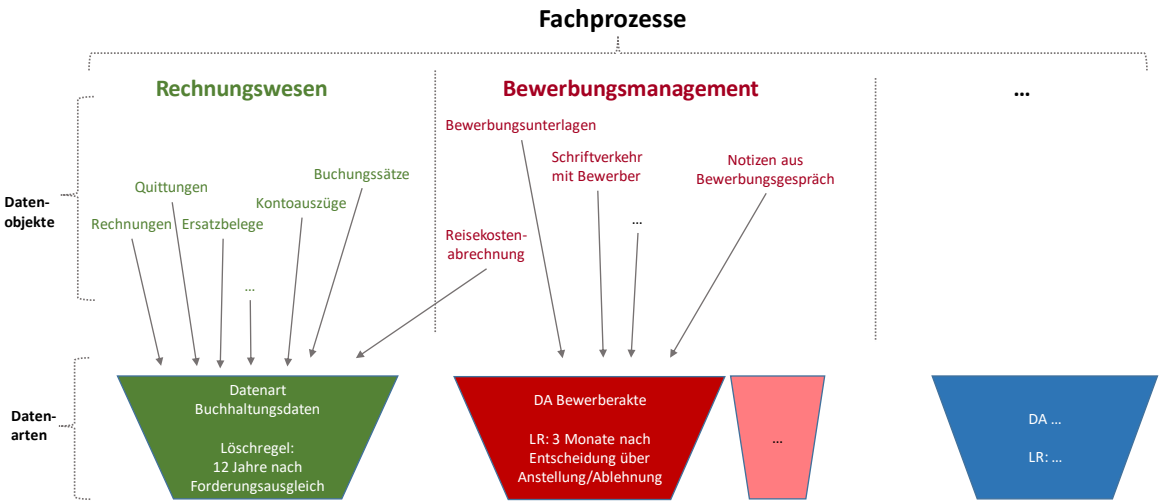
Datenart

„Sammelt“ Datenobjekte mit **einheitlichem datenschutz-rechtlichen Zweck**

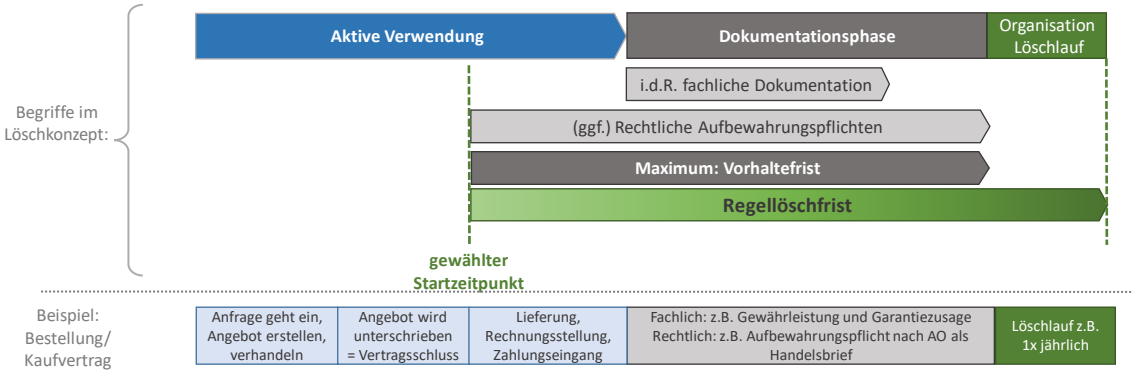
Eine Datenart → eine Löschregel = Frist & Startzeitpunkt

Technik-unabhängig definiert

Definition von Datenarten: Datenobjekte sortieren

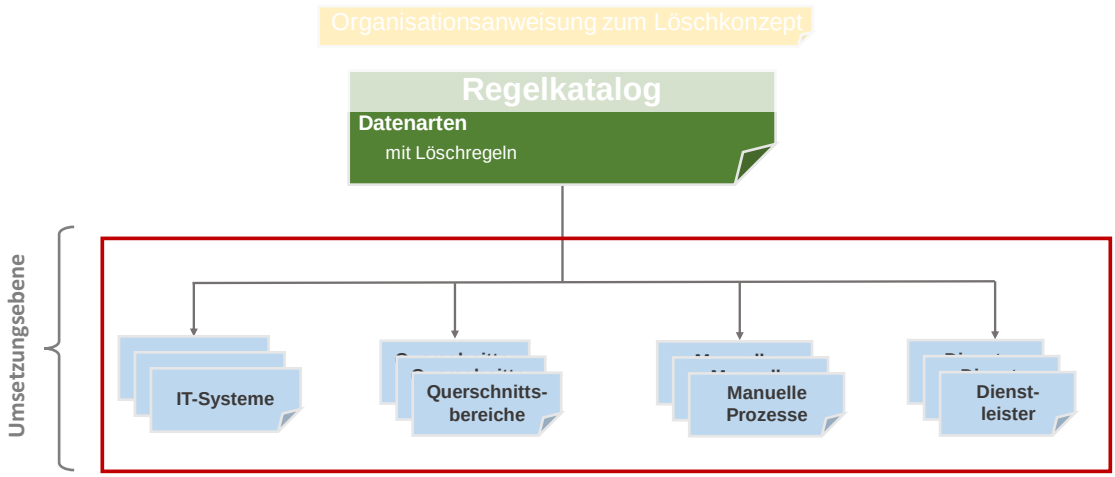


Löschregeln bestimmen:
Begriffe im Lebenszyklus von Datenobjekten



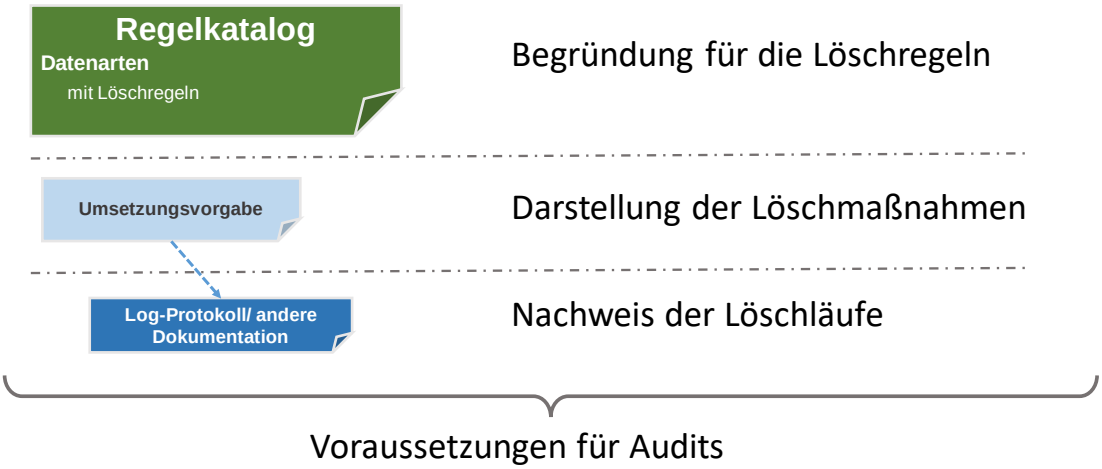
Regeln alleine …
löschen nichts →Umsetzungsebene

Aufgabenbereiche für die Umsetzung nach DIN 66398

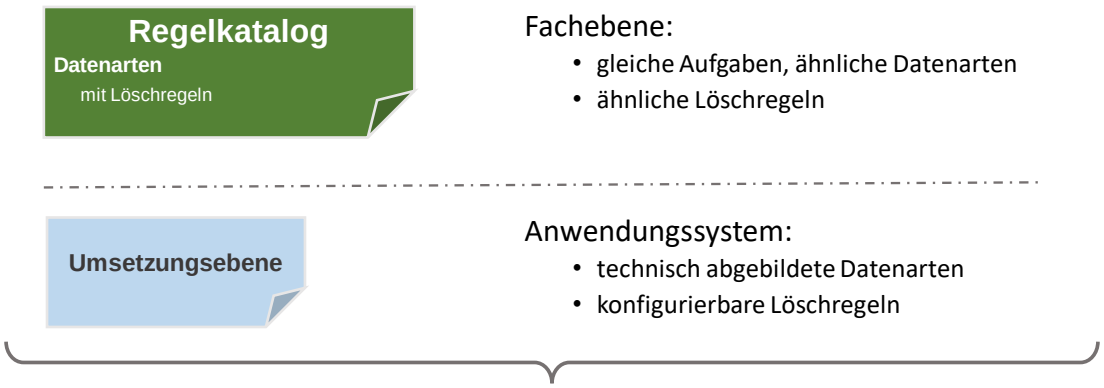


Was hilft die Norm?

… für die Rechenschaftspflicht?



… Übertragbarkeit zwischen Organisationen …



Übertragbarkeit von Bausteinen durch
- einheitliche Vorgehensweise (Trennung Regelkatalog und Umsetzung)
- gleiche Begriffe

Und sonst ...

Mehr Vorschläge in der DIN 66398 zu ...

- Inhalten von Umsetzungsvorgaben
- Speziellen Umsetzungsaufgaben ...
  - Produktion, Archiv, Backup,
  - verzögerte Löschung (Rechtsstreit, Art. 18-Anfrage, andere Fälle)
  - Integration in Projektprozesse
  - ...
- „Schnelle Löschregeln“ mit der Matrix der Löschklassen
- Verantwortlichkeiten und Pflege für das Löschkonzept

19

Positive Effekte des Löschprojekts in der Organisation

… den Datenschutz

- Compliance
- Arbeitsgrundlagen für DS-Prozesse
- Verankerung DS in der Organisation

… die Fachprozesse

- Abläufe prüfen, präzisieren, dokumentieren
- Daten konsolidieren, aufräumen
- Gute Büroorganisation

… die IT

- Altsysteme abschalten
- Ballast/Migration in Entwicklungsprojekten wird reduziert
- Weniger Daten: bessere Stabilität, höhere Performanz, schnellere Backups

… die Informationssicherheit

- Synergieeffekte/Zusammenarbeit
- Bessere Übersicht über Datenbestände
- Verringerung der Angriffsfläche
- Nicht-pbD löschen?

Copyright, Kontakt, Nachweise, Materialien

Dr. Volker Hammer
Löschprojekte.de

Dr. Volker Hammer, Löschprojekte.de,
Röderweg 27, 64625 Bensheim;
mail@loeschprojekte.de
www.loeschprojekte.de

Nachweise

- Grafiken zur „Dokumentationsstruktur“, „Begriffe Fristableitungen“ und „Matrix der Löschklassen“ in Anlehnung an DIN 66398 (Beuth Verlag) und Leitlinie Löschkonzept (Secorvo)

Materialien

- DIN 66398 (2016): Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Berlin 2016, Beuth Verlag
- ISO/IEC 27555:2021: Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion (ebenfalls beim Beuth Verlag erhältlich)
- Weitere Informationen zur Norm und Themen im Umfeld unter: www.DIN-66398.de, dort auch Hinweise auf weitere Materialien
- Hammer, V., Schuler, K.: Leitlinie Löschkonzept (Vordokument zur Norm): Download: www.Secorvo.de > Publikationen > 2012
- Hammer, V: DIN 66398, DuD 8/2016 (gibt einen Überblick über die Norm) Download: www.Secorvo.de > Publikationen > 2016

DIN 66398 – die Basis für Löschkonzepte

Abstract zum Vortrag auf den BvD-Verbandstagen am 10. Mai 2023 in Berlin

Version 1.0, Stand: 08.05.2023

1 Motivation

Das Löschen personenbezogener Daten wird heute von der Datenschutz-Grundverordnung der EU (DSGVO) gefordert.[1] Auch die Informations- und Dokumentationspflichten der DSGVO setzen ein durchgängiges Konzept zum Löschen personenbezogener Daten voraus.

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

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]

Dieses Abstract gibt einen kurzen Überblick über die Inhalte der Norm und des Vortrags.

2 Inhalt der Norm

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

- Sie empfiehlt Begriffe, durch die eine einheitliche Kommunikation der Beteiligten zu Löschkonzepten gewährleistet wird.
- 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, nach der zwischen Löschregeln einerseits und ihrer Umsetzung andererseits getrennt werden soll.
- Schließlich gibt die Norm auch Empfehlungen, wie das erste Löschprojekt in der Organisation aufgesetzt und das Löschkonzept anschließend fortgeschrieben werden kann.

Die größte Hürde für die Löschung personenbezogener Daten ist das Fehlen von Löschregeln. Ohne Löschregeln können keine Maßnahmen zur Löschung 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. Für jede Datenart wird eine Löschregel mit einem konkreten Startzeitpunkt und einer Regellöschfrist definiert. Mit Hilfe von Standardfristen und Typen von Startzeitpunkten für den Fristbeginn können sogenannte Löschklassen gebildet werden. Eine »Matrix der Löschklassen«

---

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

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

kann als Hilfsmittel eingesetzt werden, um für Datenarten auf einfache Weise Löschregeln zu finden. Die Datenarten mit ihren Löschregeln werden technikunabhängig definiert. Alle Datenarten einer Organisation bilden einen »Katalog der Löschregeln«.

Löschmaßnahmen in konkreten IT-Systemen, manuellen Prozessen oder gegenüber Auftragsverarbeitern werden nach dem Vorschlag der Norm über sogenannte **Umsetzungsvorgaben** gesteuert. In den Umsetzungsvorgabe werden Löschregeln aus dem Katalog verwendet und für den jeweiligen Datenbestand die technischen Details für die Löschung identifiziert und festgelegt. Die DIN 66398 beschreibt, welche Inhalte in Umsetzungsvorgaben dargestellt werden sollen.

Die Norm 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 initialen Löschprojekts, mit dem ein solches Konzept in der Organisation etabliert werden kann. Letztlich soll Löschen von personenbezogenen Daten 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.

3 Wo hilft die Norm?

Unterstützung für das Löschprojekt: Ihren wichtigsten Nutzen entfaltet die Norm dadurch, dass sie für das sehr komplexe Thema »Löschprojekt« eine Vorgehensweise beschreibt, in der handhabbare Arbeitspakete abgegrenzt werden können. Außerdem stellt sie bewährte Begriffe bereit, mit denen die Beteiligten präzise kommunizieren können. Schließlich trägt die Trennung von Definition der Datenarten einerseits und Umsetzung von Löschmaßnahmen anderseits wesentlich dazu bei, dass innerhalb der Organisation konsistente Löschregeln definiert und in verschiedenen Kontexten und beim Wechsel von Techniksystemen weiterverwendet werden können.

Übertragbarkeit zwischen Organisationen: Fachbereiche mit ähnlichen Aufgaben verwenden ähnliche Datenbestände. Es liegt nahe, dass dann auch die Datenarten ähnlich definiert werden könnten. Erste praktische Erfahrungen zeigen in solchen Kontexten, dass Datenarten gut zwischen Organisationen übertragen und angepasst werden können. Ähnliches gilt für die

Löschmaßnahmen in IT-Systemen: Wenn sie entsprechend des Strukturvorschlags der Norm »gebaut« werden und die typischen Datenarten eines fachlichen Kontextes abbilden, sollten auch die technischen Lösungen gut übertragbar sein. Produkte, die solche Anforderungen erfüllen, dürften einen Marktvorteil haben.

4 Biografie

Dr. Volker Hammer, Diplom Informatiker, bis 1998 interdisziplinäre Arbeiten zur rechtsgemäßen und verletzlichkeitsreduzierenden Gestaltung bei der Projektgruppe verfassungsverträgliche Technikgestaltung e.V. – provet. Von 1998 bis 2022 Mitarbeiter der Secorvo Security Consulting GmbH mit Arbeitsschwerpunkten in Datenschutz und Informationssicherheit. Inzwischen freiberuflich tätig (www.loeschprojekte.de).

Seit 2004 unterstütze ich Unternehmen dabei, ihr Löschkonzept zu etablieren, unter anderem als Leiter des Projekts »Löschkonzept« für die Toll Collect GmbH. Das Ziel meiner Projekte ist Hilfe zur Selbsthilfe. An der der DIN 66398 durfte ich als Editor mitwirken, am inhaltlich gleichen Standard ISO/IEC 27555 als Co-Editor. In zahlreichen Aufsätzen habe ich, teilweise mit Co-Autoren, Hintergründe, Details und Vertiefungen zur Norm publiziert.

5 Weiterführende Hinweise

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

mail@loeschprojekte.de
https://www.loeschprojekte.de/