

TeleTrust "IT-Sicherheitsrechtstag 2022"

Berlin, 21.09.2022

Löschen von personenbezogenen Daten; aber wie?

Entwicklung eines generischen Löschkonzeptes auf Basis der DIN 66398

Thomas H. Dorstewitz | enercity AG

Willkommen in der
Energiewelt von morgen!

Das ist enercity

enercity „generisches Löschkonzept“

Thomas H. Dorstewitz

21.09.2022, IT-Sicherheitsrechtstag - TeleTrust

Es gilt das gesprochene Wort!

Historie

- Aufbewahrungs- und Löschfristen zu etablieren war enercity intern zu Zeiten des BDSG (a. F.) ein „unbequemes“ Thema
- Die mit dem Löschen verbundene Komplexität steckt im Detail und wird durch oftmals nicht datenschutzkonforme IT-Werkzeuge erheblich erschwert.
- Die bestehende Betriebsvereinbarung „IT“ zwang Organisationseinheiten „unstrukturiert“ Aufbewahrungs- und Löschfristen zu benennen; das Bewusstsein war jedoch oft wenig ausgeprägt

Neuer Schwung durch die DSGVO, auch im Hinblick auf neue/erweiterte Sanktionsmaßnahmen:

- Generelles Löschen erforderlich (Art. 5 DSGVO)
 - Zulässigkeit, Datenminimierung, Speicherbegrenzung
- Löschen im Einzelfall auf Antrag (Art. 17 DSGVO)
 - Recht auf Vergessenwerden
- Recht auf Sperren - oder auch „nicht Löschen“ (Art. 18 DSGVO)
- Aber: Das nachhaltige und systematische Löschen personenbezogener Daten bedeutet eine erhebliche Anstrengung und missglückt oftmals oder wird stillschweigend ignoriert; dies aufgrund fehlender Orientierung, unzureichender Erfahrung in der Praxis und dem Mangel an geeigneten Vorgehensweisen.

- Grundüberlegung: Wie können Organisationseinheiten positiv bewegt werden, sich diesem nach wie vor „unbequemen“ Thema zuzuwenden?
- Erkenntnis: „Betreutes Arbeiten“ zum Thema „Aufbewahrungs- und Löschfristen“

Handlungsversprechen:

- Im Rahmen des internen Umsetzungsprojektes zur DSGVO (08.2016 -06.2018) wurde durch die Projektleitung das Handlungsversprechen gegeben, für enercity ein „generisches Löschkonzept“ - gemeinsam mit den Organisationseinheiten - zu erarbeiten.

→ Ziel: Datenschutz-Compliance

enercity Vorgehensweise DIN 66398

Die DIN 66398¹ als Grundlage für den Verantwortlichen, um...

- ✓ rechtliche Pflichten zur Löschung personenbezogener Daten zu erfüllen
- ✓ um Löschkonzepte, deren Vorgehensweise und Strukturierung zu entwickeln
- ✓ eine Richtlinie „generisches Löschkonzept“ zu etablieren
- ✓ Projektverantwortliche und Organisationseinheiten anzuleiten
- ✓ Anlehnung an DIN; mögliche Wirkung als antizipiertes Sachverständigengutachten
- ✓ Berücksichtigung der DIN 66398 ggf. als Nachweis „Stand der Technik“
- ✓ Anschein für Dritte bei Anlehnung an DIN; strukturierte und sinnhafte Handlungsweise; mögliche „Freude“ bei der Aufsichtsbehörde 😊

DIN 66398 als Blueprint für die ISO/IEC 27555:2021

Information security, cybersecurity and privacy protection –
Guidelines on personally identifiable information deletion.

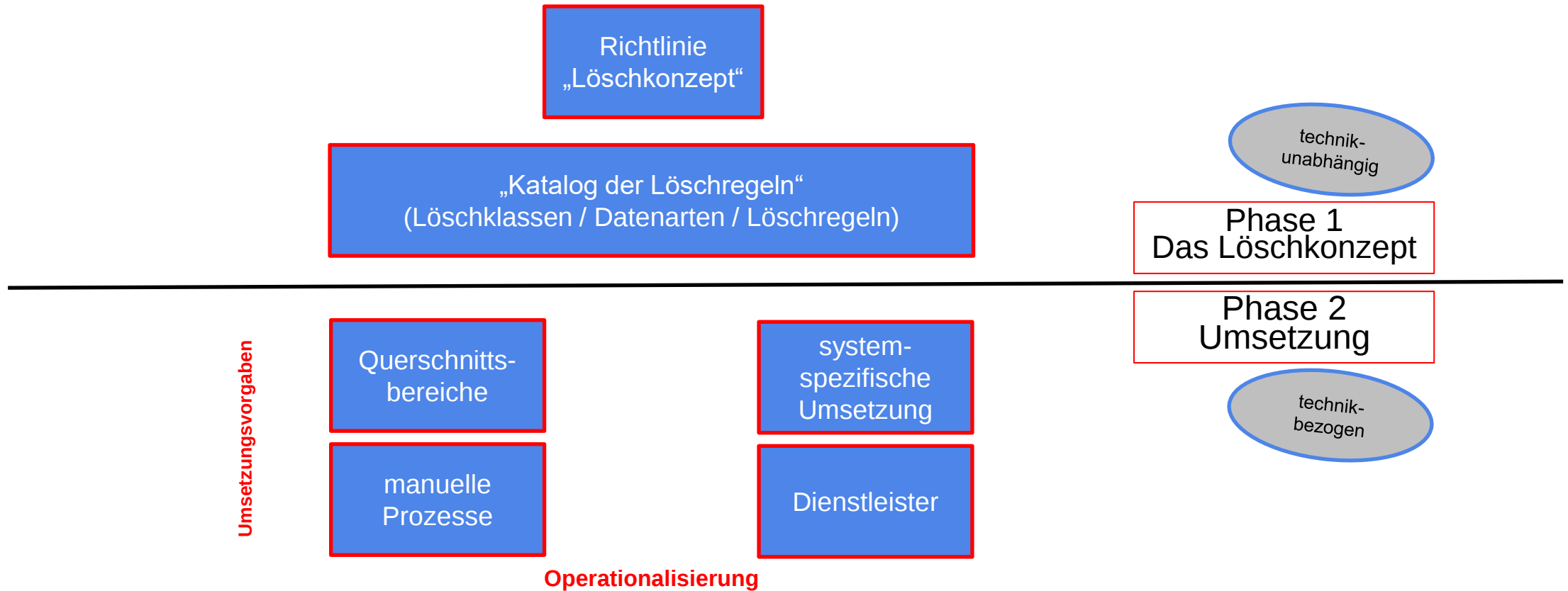
1 Die DIN 66398 (Hrsg. DIN e. V.) kann käuflich erworben werden im Beuth-Verlag – www.beuth.de

DIN 66398¹: Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten

- Nutzen²:
 - ✓ Validierte Dokumentation; auch als Nachweis gegenüber Aufsichtsbehörden
 - ✓ Transparenz über Geschäftsprozesse, Datenarten und Rechtsgrundlagen
 - ✓ Systematisierung und Konsolidierung der Datenbestände
 - ✓ Reduzierung von Kosten durch Bereinigen und Löschen von Datenbeständen
 - ✓ Grundlage für interne/externe Audits durch Soll-/Ist-Abgleiche
 - ✓ Durch systematische Erfassung der Datenbestände und der Löschprozesse ergeben sich zahlreiche Detailinformationen, die auch für weitere Zwecke verwendet werden können
 - ✓ Die Erarbeitung von Löschregeln schafft bei allen Betroffenen ein grundlegendes Verständnis für das Löschen und damit für den Datenschutz

1 Die DIN 66398 (Hrsg. DIN e. V.) kann käuflich erworben werden im Beuth-Verlag – www.beuth.de

2 Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 7,8



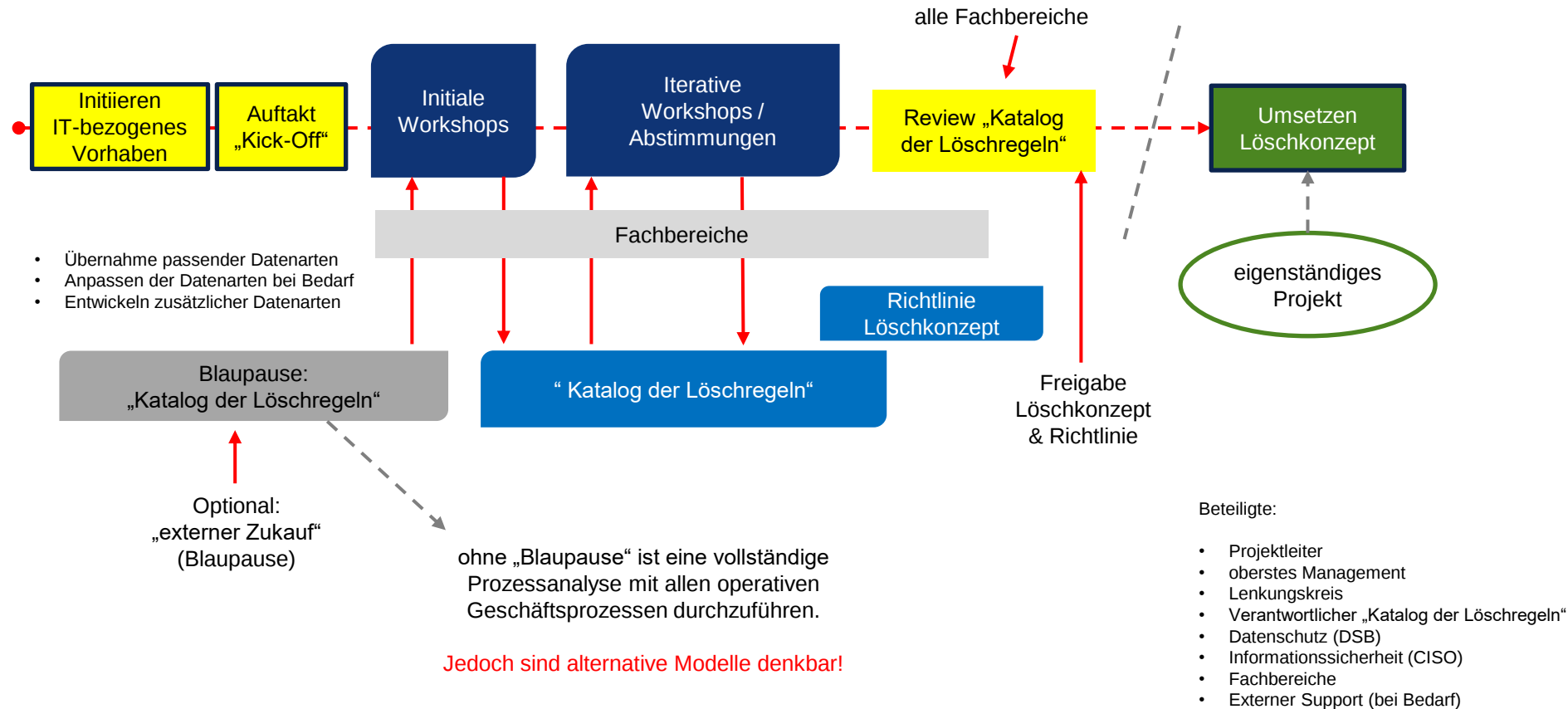
1 Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 32

Ermitteln der relevanten Datenarten, Aufbewahrungs- und Löschfristen, Löschregeln und Umsetzungsvorgaben innerhalb der Organisationseinheiten / Prozesse

Ziel: „Löschkonzept mit „Katalog der Löschregeln“

- ✓ Zentrale Steuerung; damit weitgehende Vollständigkeit und Richtigkeit
- ✓ Fachbereiche konzentrieren sich auf „ihre“ Daten
- ✓ Datenschutzwissen wird zentral eingebracht
- ✓ Kenntnisse über Aufbewahrungs- und Löschpflichten werden zentral und dezentral erarbeitet
- ✓ homogenes Löschkonzept; Methoden, Dokumentation, etc.
- ✓ Abstimmung zwischen Geschäftsprozessen bei „gemeinsamen“ Daten gewährleistet
- ✓ geringe Fehlerquote, hohe Compliance

Achtung: hoher zeitlicher Aufwand (Workshops und Dokumentation)



01.2019

06.2020

05.2021

4. Q. 2021

2024

Version 1.0 Version 1.2

- **Aufbewahrungsfrist:**
Zeitraum, innerhalb dessen die Objekte einer Datenart nach rechtlichen Vorgaben aufbewahrt werden müssen
- **Datenart**
Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet werden; technikunabhängig!
- **Löschfrist**
Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden sollte
- **Löschklasse**
Kombination aus einer Standardlöschfrist und einem abstraktem Startzeitpunkt für den Fristablauf
- **Datenobjekte**
Elemente, die Daten enthalten, wie zum Beispiel Dateien, Dokumente, Datensätze, Attribute

- **Löschregel**
Kombination aus Löschfrist und (abstrakter) Bedingung für den Startzeitpunkt des Fristablaufs
- **Regellöschfrist**
Maximaler Zeitraum, nach dessen Ablauf eine Datenart bei regulärer Verwendung in den Prozessen gelöscht werden sollte
- **Standardlöschfristen**
Einheitliche Löschfristen für mehrere Datenarten
- **Vorhaltefrist**
Zeitraum, innerhalb dessen die Objekte einer Datenart aufgrund der fachlichen Verwendung oder gesetzlicher Aufbewahrungsvorschriften mindestens verfügbar sein sollten

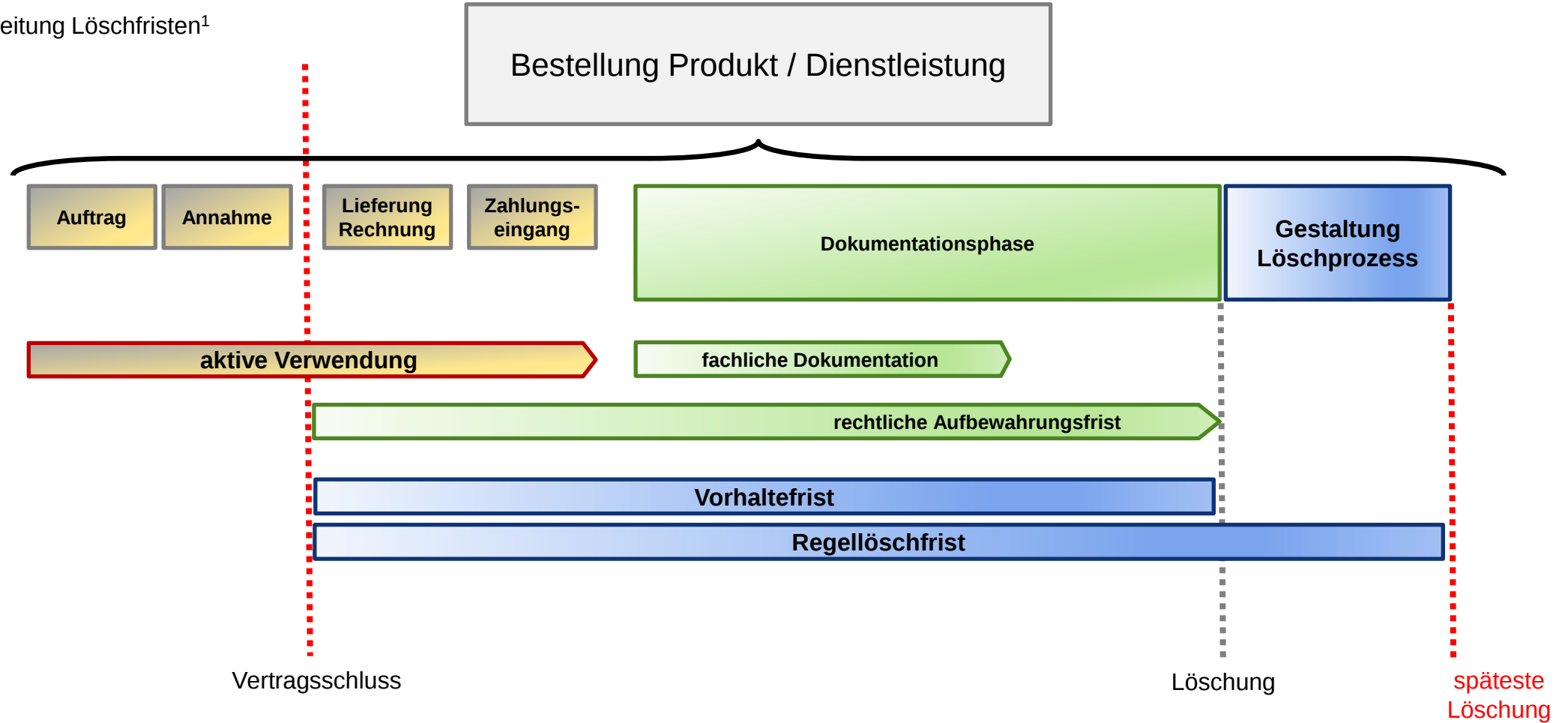
¹ Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Kapitel 2

Grundlegende Schritte der DIN 66398¹:

- Datenarten bilden
- Aufbewahrungs- und Löschvorschriften ermitteln
- Erarbeiten (möglichst weniger) Standardlöschfristen auf Grundlage exemplarischer Datenarten
- Bilden von Löschklassen durch kombinieren der Standardlöschfristen mit abstrakten Startzeitpunkten (Matrix der Löschklassen)
- Zuordnen der ermittelten Datenarten in entsprechende Löschklassen (Löschregel)
- Operationalisierung: Umsetzungsvorgaben für konkrete Datenbestände für das Löschen

1 Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Inhalt

Ableitung Löschfristen¹



¹ Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 18

- Um den Aufwand bei der Ermittlung und Zuordnung von Löschfristen zu Datenarten zu vereinfachen, werden Standardlöschfristen etabliert:
- Festlegen der benötigten Standardlöschfristen anhand ausgewählter Datenarten
- Ermittlung der Standardlöschfrist für eine Datenart
 - ✓ aktive Verwendung + laufendes Kalenderjahr + (betriebliche +) gesetzliche Aufbewahrungspflicht = **Vorhaltefrist**
 - ✓ **Vorhaltefrist** + Zeitraum für das organisieren/durchführen des Löschrprozesses = **Regellöschfrist**
 - ✓ **Regellöschfrist** wird einer passenden **Standard-Löschfrist** zugeordnet
 - ✓ Ist keine passende Standardlöschfrist vorhanden, wird die Datenart a) der nächsthöheren Standardlöschfrist zugeordnet oder b) wenn diese zeitlich unangemessen entfernt ist, eine neue Standard-Löschfrist eingeführt.

Ziel: möglich wenige Standardlöschfristen ~ praxisgerechtes Löschen

- Standardlöschfristen und abstrakte Startzeitpunkte ergeben abstrakte Löschregeln und bilden eine Löschklasse
- Für jede Standardlöschfrist – kombiniert mit den drei abstrakten Startzeitpunkten – ergeben sich drei Löschklassen

Standard-Löschfristen

Matrix der Löschklassen ¹		sofort	42 Tage	180 Tage	1 Jahr	4 Jahre	7 Jahre	11 Jahre
Abstrakte Startzeitpunkte	Ab Erhebung			Verbindungsdaten	Verbindungen mit besonderer Analyse			
	Ab Ende des Vorgangs	Web-Logs	Kurzzeit-Dokumentation, Betriebs-Logs	Einzelverbindungs-nachweise	Vorgänge ohne Dokumentations-pflichten	Reklamationen, Forderungsdate n	Handelsbrief e	Buchhaltungsdate n
	Ab Ende der Beziehung				Ergänzende Stammdaten		Verträge	Kernstammdaten

Die Kombination aus abstraktem Startzeitpunkt und Standardlöschfrist ergibt die **Löschklasse**

Datenarten

Nicht belegte Löschklasse, da für diese Kombination aus Startzeitpunkt und Standardlöschfrist keine Datenart vorliegt.

¹ Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 30

- Nr.
- Name der Datenart
- Verwendungszweck
- Inhalte (Konkrete Inhalte der Datenart)
- Abgrenzungen (Was nicht dieser Datenart zugeordnet ist, sondern einer anderen Datenart)
- Geltungsbereich (Unternehmen, verbundene Unternehmen)
- Bereich (Fachliche Gruppierung, z. B. HR, Buchhaltung)
- Fachbereiche (Relevant für welche Fachbereiche)
- Löschkategorie I (Standard-Löschfristen)
- Löschkategorie II (Abstrakter Startzeitpunkt)
- Rechtsgrundlage Verarbeitung
- Rechtsgrundlage Löschen
- Aufbewahrungspflichten
- Startzeitpunkt
- Vorhaltefrist
- Regellöschfrist
- Sperrregel
- Löschen im Einzelfall
- Aussetzen der Löschung im Einzelfall
- Anonymisierungsvorgaben
- Hinweise / Interessenabwägung

Dokumentation Datenarten

↔	ELRK-23	DA-0004	TK Verbindungsdaten
↔	ELRK-24	DA-0005	Druckjobs
↔	ELRK-36	DA-0006	Bewerberakte ohne Pooling
↔	ELRK-37	DA-0007	Akte freiwillige Sozialberatung
↔	ELRK-38	DA-0008	Benutzerkonten ohne Buchhaltungsrelevanz
↔	ELRK-39	DA-0009	Persönliche Speicherbereiche Beschäftigter
↔	ELRK-40	DA-0010	Betreuungsakte Schwerbehinderte
↔	ELRK-41	DA-0011	Besucherscheine und Besucherlisten
↔	ELRK-42	DA-0012	Log-Protokolle auf Applikationsebene
↔	ELRK-43	DA-0013	Personalplanungsdaten
↔	ELRK-52	DA-0014	Wachblätter
↔	ELRK-53	DA-0015	Vorfallsakte
↔	ELRK-44	DA-0016	Einträge zu Änderungshistorien kurz
↔	ELRK-45	DA-0017	Dokumentation der Ausstattung für Beschäftigte
↔	ELRK-46	DA-0018	Bewerberakte mit Pooling
↔	ELRK-47	DA-0019	Ausbildungsakte

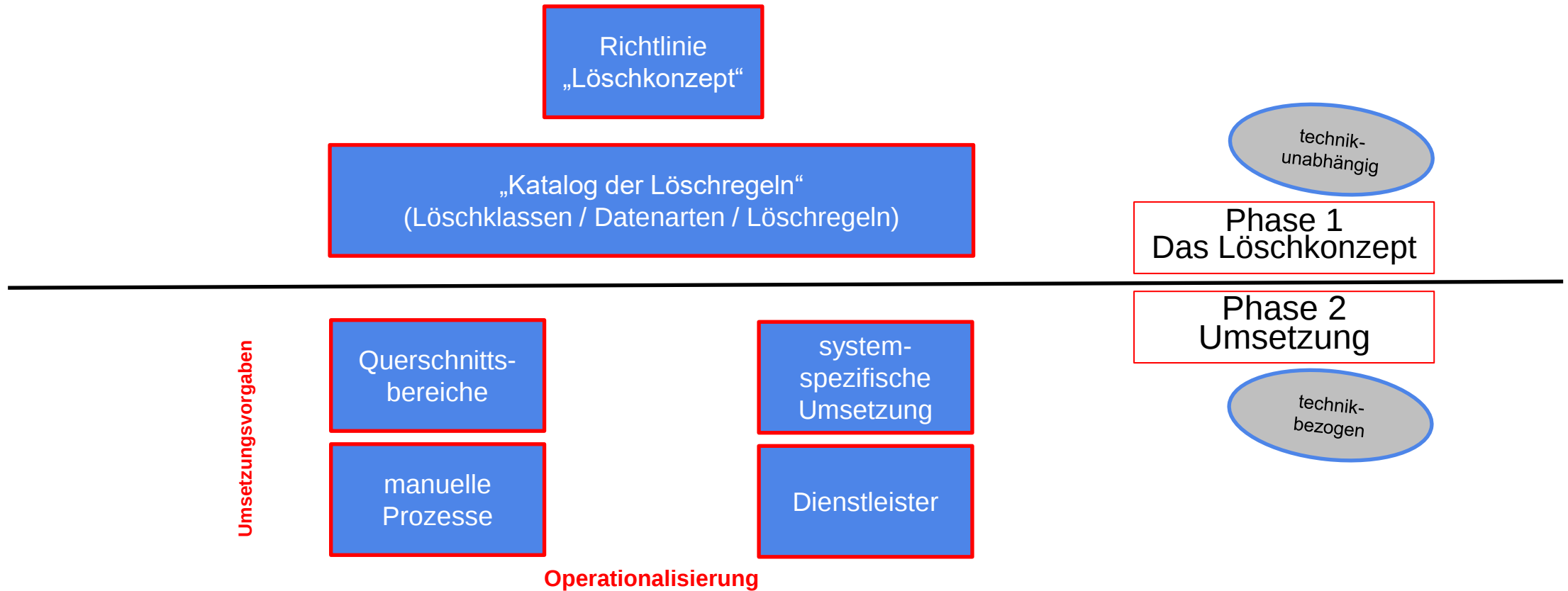
▼ Details

Typ:	↔ Datenart	Status:	AKTIV (Arbeitsablauf anzeigen)
betrifft Version(en):	1.2	Lösung:	Nicht erledigt
Komponente(n):	Basis		
ID (ISM):	DA-0008		
Löschklasse (ELRK):	Ende Beziehung - 7 Monate		
Einleitung:	▼ Die Zuordnung der Benutzerkennungen (User-IDs) zum Beschäftigten ist vorzuhalten, so lange ein Benutzerkonto besteht.		
Zweck:	◦ das/die Benutzerkonten für Beschäftigte und externe Berater bereitzustellen und zu pflegen ◦ die Rechte von Benutzern auf IT-Systeme einzuräumen und zurückzuziehen		
Datenobjekte:	◦ Active Directory-Konto ◦ Einträge in anderen Systemen zur Benutzerverwaltung (Konten), z. B. in Anwendungssystemen ◦ Zugriffsrechte in Systemen		
Merkmale der Datenart:	◦ USER-ID ◦ Passwort (verschlüsselt)		
Abgrenzung der Datenart:	▼ ◦ Benutzerkonten mit Buchhaltungsrelevanz (DA-0101) ◦ Berechtigungsanträge (DA-0030) ◦ Persönliche Speicherbereiche Beschäftigter (DA-0009) ◦ Persönliche Speicherbereiche oberstes Management (DA-0107) ◦ Benutzerkonto e-Learning (DA-0048) ◦ Kernstammdaten Beschäftigte ohne Einwilligung (DA-0100) ◦ Erweiterte Stammdaten Beschäftigte (DA-0047) ◦ Stammdaten Self Service Accounts (DA-0031)		

Rechtsgrundlage	◦ Arbeitsvertrag und Nebenpflichten
Verarbeitung:	◦ Art. 6 (1f) DSGVO (Interessenabwägung), ◦ für externe Berater: Dienstleistungsvertrag
Vorgaben zur Löschung:	✓ Gemäß Artikel 5 DSGVO
Vorgaben zur Aufbewahrung:	✓ keine
Löschregel:	✓ Startzeitpunkt: Datum des Ausscheidens des Beschäftigten oder des externen Beraters aus dem Unternehmen Regellöschfrist: 7 Monate Vorhaltefrist: 6 Monate Freigabevorbehalt: Freigabe zur Löschung erfolgt durch den jeweiligen Fachbereich
Freigabevorbehalt (ELRK):	Offen
Sperrregel:	✓ Startzeitpunkt: Datum des Ausscheidens des Beschäftigten oder des externen Beraters aus dem Unternehmen Sperrfrist: 1 Tag. Die Sperrung des Benutzerkontos erfolgt direkt mittels systemseitiger Einstellung
Löschung im Einzelfall:	✓ Anträge auf Löschung im Einzelfall sind möglich. Genehmigte Anträge müssen über manuelle Prozesse und die IT-Administration umgesetzt werden.
Hinweise:	✓ Beispiele für Benutzerkonten ohne Buchhaltungsrelevanz ◦ Benutzerkonten in Content-Management-Systemen, um internen und externen Nutzern die Mitwirkung in digitalen Redaktionsprozessen zu ermöglichen ◦ Benutzerkonten für ITSM-Geschäftsprozesse ◦ Benutzerkonten inkl. Profildaten in WIKI-Systemen Die Unterscheidung zwischen Benutzerkonten mit und ohne Buchhaltungsrelevanz erfolgt im Rahmen der Umsetzung durch Abstimmung mit dem Bereich Finanzen.
BIA - Vertraulichkeit (VvV):	nicht ermittelt
BIA - Integrität (VvV):	nicht ermittelt

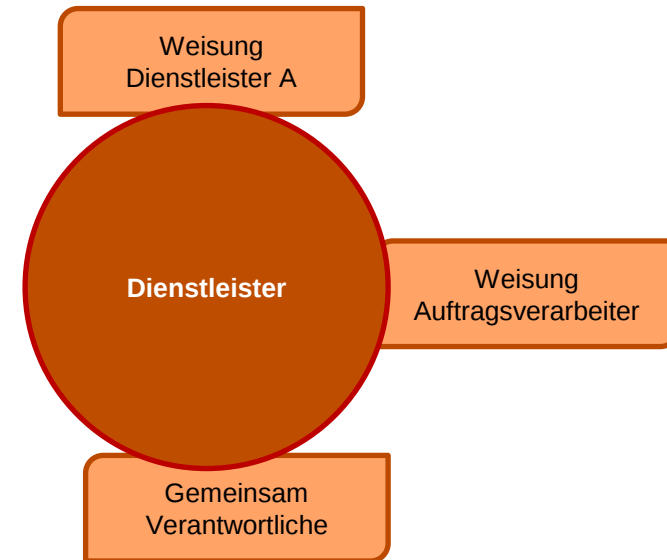
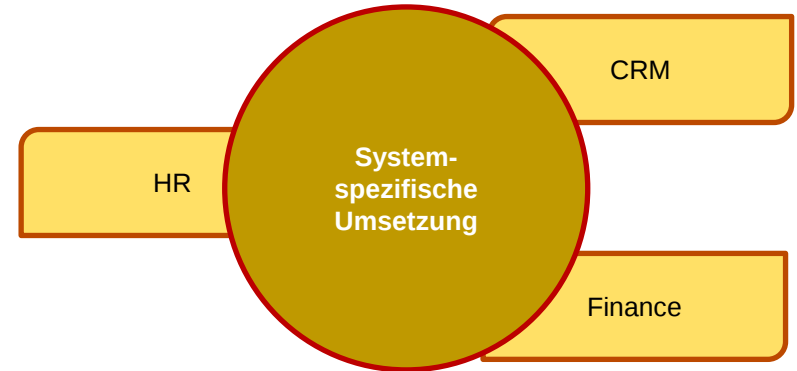
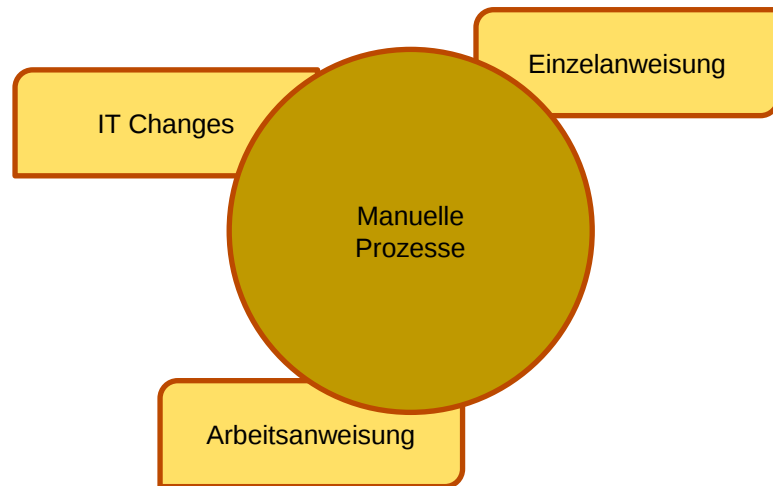
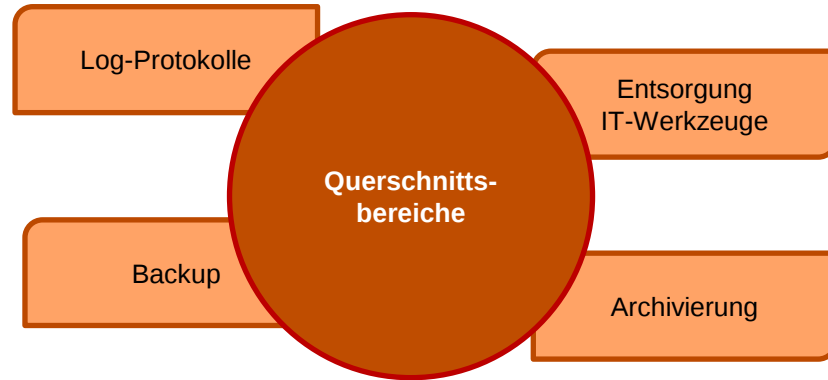
...da ist doch noch etwas...

Die Umsetzung



1 Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 32

Umsetzungsvorgaben



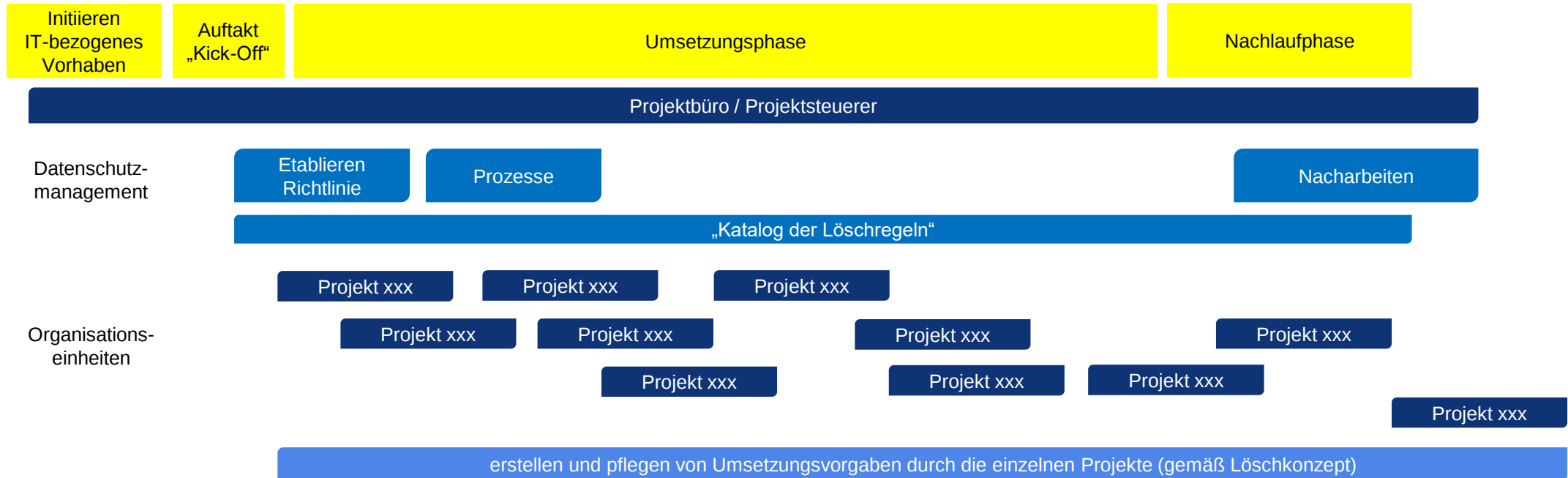
1 Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Seite 32

Inhalte der Umsetzungsvorgaben¹:

- Für welche IT-Systeme oder Datenbestände gilt die Umsetzungsvorgabe
- Welche Datenarten werden im Regelungsbereich der Umsetzungsvorgabe verwendet?
- Für welche dieser Datenarten ist welche Löschregel anzuwenden? Welche technischen Bedingungen entsprechen dem fachlichen Auslöser des Fristlaufs aus der Löschregel?
- Durch welchen Mechanismus wird die Löschung durchgeführt? Gegebenenfalls ist dafür auch zu klären, ob sich aus dem Schutzbedarf der Daten Sicherheitsanforderungen an den Löschmechanismus ergeben.
- Soweit Löschmechanismen konfigurierbar sind: Welche Parameter sind mit welchen Werten zu verwenden, um die zu löschenden Daten zu bestimmen?
- Wer ist für den Start und die Überwachung des Mechanismus verantwortlich?
- Wem gegenüber sind Nachweise über die Löschung zu führen? Wie ist die Durchführung von Löschmaßnahmen zu dokumentieren?

¹ Vgl. DIN e. V. (Hrsg.), DIN 66398:2016-05, Kapitel 8.1.2

Vorgehensmodell Operationalisierung



4. Q. 2021

2024/2025

Phase 1

- Projektbeginn: 01.2019
- Finalisierung Version 1.0 in 06.2020
 - Richtlinie
 - Katalog der Löschregeln Version 1.0
 - circa 120 Datenarten
- Finalisierung Version 1.2 in 05.2021
 - Katalog der Löschregeln Version 1.2 (Umfang: 420 Seiten)
 - circa 130 Datenarten
 - Beschreibung der Prozesse

Phase 2

- Projektbeginn: 4. Quartal 2021
- Voraussichtliche Ende: 2024/2025

Externe Beratung

- Herr Dr. Volker Hammer (Autor der DIN 66398)

Anmerkungen:

- Die richtigen Kolleginnen und Kollegen in den Organisationseinheiten (OE) finden
- Jedoch: Oft keine umfassenden Kenntnisse der Prozesse
- Das „Warum“ erfordert in den OEs Hintergrundrecherche (gesetzliche Grundlagen)
- erfahrene Projektleitung ist unerlässlich
- externer Support dringend zu empfehlen
- Verantwortliche Person für den Katalog der Löschregeln benennen!
- Workshop-Ergebnisse zeitnah in den Katalog der Löschregeln aufnehmen
- Sind alle Datenbestände/IT-Systeme tatsächlich berücksichtigt
- Review der Zwischenergebnisse pro OE
- Review des gesamten Katalogs durch alle OEs (aha-Effekt)
- Freigabe Vorstand/Geschäftsführung! Sonst fehlt der Druck...
- Regelmäßiger Review des „Löschkonzeptes“; denn das Leben geht weiter.

Vermarktung „Katalog der Löschregeln“

- Andere Unternehmen sind auf das Projekt und damit auf das Löschkonzept bei enercity aufmerksam geworden
- Hieraus Vermarktung des Löschkonzeptes als „Blaupause“ zur individuellen Entwicklung eines eigenen Löschkonzeptes
- Kooperation/Weiterentwicklung enercity Löschkonzept mit der Wohnungswirtschaft: Löschkonzept „enercity - WoWi 0.9“

Integration Löschkonzept in den „Digitalen Arbeitsplatz“ von enercity

- Löschregeln als Confluence/Jira - Projekt
- Integration in die Verarbeitungstätigkeiten (Verzeichnis von Verarbeitungstätigkeiten)
- Integration in die neue Betriebsvereinbarung „IT-bezogene Vorhaben“ (Stichwort: Beschäftigtendaten)



- ✓ Stand der Technik
- ✓ kein Löschen ohne Regeln
- ✓ kein Löschen ohne Implementierung
- ✓ keine Löschregeln ohne Ausnahmen
- ✓ kein Löschkonzept ohne Dokumentation
- ✓ eine Datenart ~ eine Löschregel
- ✓ Löschregel ~ Löschfrist und (abstrakter) Startzeitpunkt
- ✓ Löschregel ~ technikunabhängig
- ✓ aus Datenbeständen (Datenobjekten) werden Datenarten
- ✓ wenige Standardlöschfristen

- ✓ abstrakte Startzeitpunkte ~ konkrete Startzeitpunkte
- ✓ Datenarten ~ datenschutzrechtlich einheitliche Zwecke
- ✓ Alternativen zum Löschen ~ anonymisieren/sperren
- ✓ Sperren ~ begrenzen oder ausschließen des Zugriffs
- ✓ Anonymisieren ~ entfernen des Personenbezugs
- ✓ Wer macht Was ~ klare Zuständigkeiten
- ✓ Löschmechanismen in der Entwicklung
- ✓ Prozesse implementieren
- ✓ Löschen in Geschäftsprozesse integrieren

Am Ende wird alles gut!

Und wenn es nicht gut ist, ist es auch
nicht das Ende!

Thomas H. Dorstewitz

- CISO -
enercity | Informationssicherheitsmanagement

Vielen Dank
für Ihre Aufmerksamkeit!