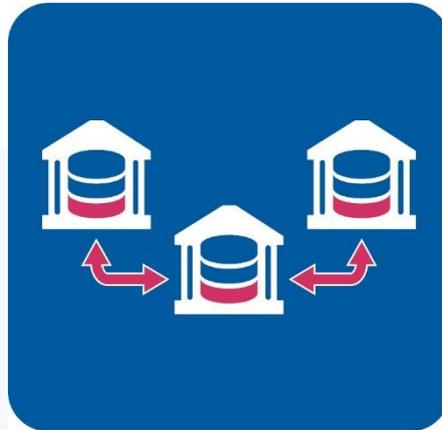


sormas

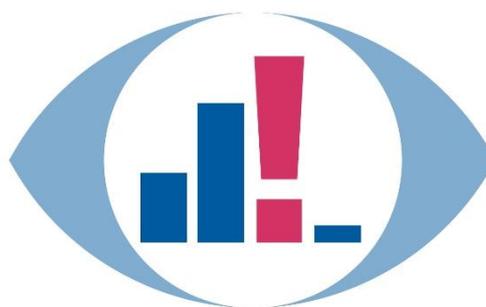
**[VERTRAULICH]**



## Löschkonzept für SORMAS-X

Version 1.0.1

Stand 28.04.2022



**COVID-19**  
**SORMAS-ÖGD Deutschland**

## Wahrung der Vertraulichkeit

Dieses Dokument darf ohne schriftliche Genehmigung des Helmholtz-Zentrums für Infektionsforschung weder ganz noch teilweise dupliziert, an Dritte weitergegeben oder anderweitig veröffentlicht werden. Dies gilt nicht für Kopien, die für die interne Verwendung bestimmt sind.

## Versionsübersicht

Version	Datum	Autor	Gepr.	Beschreibung
14_SORMAS-X_Löschkonzept_kge_210328.docx	15.12.2020	MAN	CHA	Inhaltliche Anpassungen
14_SORMAS-X_Löschkonzept_kge_210328.docx	19.12.2020	SOW	GSO	Korrekturen und Anpassungen
14_SORMAS-X_Löschkonzept_kge_210328.docx	19.12.2020	VWE	GSO	Anpassung an die Vorlage
14_SORMAS-X_Löschkonzept_kge_210328.docx	20.12.2020	GSO	SOW	Überarbeitung, Inhalte zusammengeführt
14_SORMAS-X_Löschkonzept_kge_210328.docx	22.12.2020	CHA	GSO	Überarbeitung
14_SORMAS-X_Löschkonzept_vwe_210120	20.01.2021	VWE	CHA	Informationen zur technischen Umsetzung eingefügt
14_SORMAS_Löschkonzept_kge_20210328	28.03.2021	KGE	GSO	Anpassung als Löschkonzept entsprechend DIN 66398
14_SORMAS_Löschkonzept_V1-0_220329	29.03.2022	GSO		Änderung der Nomenklatur
14_SORMAS_Löschkonzept_V.1.0.1_220428	28.04.2022	KS		Wasserzeichen hinzugefügt

## Inhaltsverzeichnis

1	Klassifizierung des Berechtigungskonzeptes .....	6
2	Inhalt des Löschkonzeptes .....	6
3	Geltungsbereich .....	6
4	Hintergrund .....	7
4.1	Gegenstand und Ziele des Löschkonzeptes.....	7
4.2	Begriffe und Definitionen .....	7
5	Grundlagen des Löschkonzeptes .....	8
5.1	Allgemeines .....	8
5.2	Was bedeutet ‚Löschen‘ .....	9
5.3	Eine Löschrregel für jede Datenart .....	9
5.3.1	Datenarten .....	9
5.3.2	Löschrregeln.....	10
5.3.3	Vorhaltefrist und Regellöschrfrist.....	10
5.3.4	Unterscheidung zwischen Archiv, Sicherungskopie und gesperrten Daten.....	12
5.3.5	Standardlöschrfristen, Startzeitpunkte, Löschrregeln und Löschrklassen .....	12
5.4	Etablieren des Löschkonzeptes .....	13
5.4.1	Dokumentation des Löschkonzeptes .....	13
5.4.2	Prozesse und Verantwortlichkeiten .....	13
5.4.3	Phasen in der Umsetzung des Löschkonzeptes.....	13
6	Datenarten festlegen.....	15
6.1	Beispiele für Datenbestände, Zwecke und Datenarten .....	15
6.2	Datenarten systematisch erfassen .....	17
6.3	Gestaltungskriterien für die Bildung von Datenarten .....	17
6.3.1	Datenarten aus den fachlichen Zusammenhängen.....	17
6.3.2	Vertraulichkeitsklassifikation und Datenarten .....	18
7	Löschrfristen festlegen .....	18
7.1	Standardlöschrfristen verwenden .....	19
7.2	Fristfestlegungen .....	19
7.2.1	Übersicht über die Vorgehensweisen zur Fristdefinition.....	19
7.2.2	Unmittelbare Fristen aus Rechtsvorschriften.....	20
7.2.3	Fristfestlegung nach Prozessanalyse .....	21
7.2.4	Ableitung von Löschrfristen nach einfachen Kriterien .....	21
7.3	Besonderheiten für Fristfestlegungen.....	22
7.3.1	Regellöschrfristen und Abweichungen .....	22
7.3.2	Friständerungen durch Verdichtung mit Wechsel der Datenart.....	22

7.3.3	Wechsel der Datenart für Sonderfälle.....	22
7.3.4	Ausnahmen von Regelprozessen: Aussetzung der Löschung.....	23
7.3.5	Abweichungen von Standardlöschfristen für Sicherungskopien.....	23
8	Löschklassen.....	24
8.1	Abstrakte Startzeitpunkte – abstrakte Löschrregeln.....	24
8.2	Matrix der Löschklassen.....	25
8.3	Zuordnung von Datenarten zu Löschklassen und Löschrregeln.....	25
9	Löschrregeln.....	26
9.1	Struktur und Inhalte der Umsetzungsvorgaben.....	26
9.1.1	Verhältnis zwischen Dokument ‚Löschrregeln‘ und Umsetzungsvorgaben für Löschrregeln 26	
9.1.2	Inhalt von Umsetzungsvorgaben.....	28
9.2	Umsetzungsvorgaben für Querschnittsbereiche.....	28
9.3	Umsetzungsvorgaben für einzelne IT-Systeme.....	29
9.4	Einzelmaßnahmen zur Löschung von Datenbeständen.....	30
9.4.1	Allgemeine Hinweise zu Umsetzungsvorgaben für Einzelmaßnahmen.....	30
9.4.2	Umsetzungsvorgaben für Datenobjekte im allgemeinen Bürobetrieb.....	30
9.4.3	Umsetzungsvorgaben für Datenbestände in manuellen Prozessen.....	30
9.4.4	Umsetzungsvorgaben für Datenabzüge für Sonderverwendungen.....	31
9.4.5	Umsetzungsvorgaben für Restbestände in IT-Systemen.....	31
9.4.6	Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten.....	31
9.5	Umsetzungsvorgaben für Auftragnehmer.....	32
10	Verantwortung u. Prozesse für das Löschen von personenbezogenen Daten.....	32
10.1	Allgemeine Einbettung in das Datenschutz-Management-System.....	32
10.2	Rolle der Datenschutzbeauftragten.....	32
10.2.1	Pflegeverantwortung für Dokumente.....	32
10.2.2	Überwachung von Prozessen durch die Datenschutzbeauftragte.....	32
10.2.3	Freigabe-Beteiligungen.....	33
10.3	Verantwortung und Prozesse bezüglich Umsetzungsvorgaben.....	33
10.3.1	Organisationseinheiten mit Verantwortung für Bestände mit pbD.....	33
10.3.2	Weitere Aufgaben bezüglich Umsetzungsvorgaben.....	34
10.3.3	Organisationseinheit Change-Management.....	34
10.3.4	Organisationseinheiten mit Verantwortung zur Steuerung von Auftragnehmern.....	34
11	Referenzierte Dokumente.....	35
11.1	Anlage 01, Dokument ‚Löschrregeln‘.....	35
11.2	Anlage 02, Dokument ‚Umsetzungsvorgaben für Querschnittsbereiche‘.....	35

11.3	Anlage 03, Dokument „Bestandsverzeichnis der Datenträger“ .....	36
11.4	Anlage 04, Dokument „Umsetzungsvorgaben für einzelne IT-Systeme“ .....	36
11.5	Anlage 05, Dokument „Arbeitsanweisung Löschrregeln im allgemeinen Bürobetrieb“ .....	36
11.6	Anlage 06, Dokument „Arbeitsanweisung Datenbestände in manuellen Prozessen“ .....	37
11.7	Anlage 07, Dokument „Arbeitsanweisung für Datenabzüge für Sonderverwendungen“ .....	38
11.8	Anlage 08, Dokument „Übersicht über Ausnahmeregelungen“ .....	38
11.9	Anlage 09, Dokument „Umsetzungsvorgaben für Restbestände in IT-Systemen“ .....	39
11.10	Anlage 10, Dokument „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“ .....	39
11.11	Anlage 11, Dokument „Umsetzungsvorgaben für Auftragnehmer“ .....	39
11.12	Anlage 12, Dokument „Übersicht über IT-Systeme und andere Bestände mit pbD“ .....	40
11.13	Anlage 13, Dokument „Handlungsbedarfe aus Umsetzungsvorgaben“ .....	40
12	Anhang.....	42
12.1	Abkürzungen.....	42
12.2	Abbildungsverzeichnis .....	42
12.3	Tabellenverzeichnis .....	42
12.4	Quellenverzeichnis .....	43
12.5	Regelverzeichnis .....	43
13	Änderungshistorie .....	44
13.1	Änderungen von der vorherigen Version zur aktuellen Version.....	44

## 1 Klassifizierung des Berechtigungskonzeptes

Die Dokumentation des Löschkonzeptes und seiner Anlagen ist ein wesentlicher Teil des Sicherheitsprozesses des Gesundheitsamt Musterstadt und sollte entsprechend des Klassifikationsschemas des Gesundheitsamt Musterstadt gekennzeichnet und behandelt werden.

In Anlehnung an den ‚BSI-Standard 200-2, IT-Grundschutzmethodik‘, Abschnitt 5, ‚Dokumentation im Sicherheitsprozess‘ könnten die Informationen des Löschkonzeptes und der Anlagen wie folgt klassifiziert werden.

<b>Gewährleistungsziel ‚Vertraulichkeit‘</b>	
Löschkonzept	Vertraulich
Anlagen zum Löschkonzept	Streng vertraulich
<b>Gewährleistungsziel ‚Integrität‘</b>	
Löschkonzept	wichtig
Anlagen zum Löschkonzept	essentiell
<b>Gewährleistungsziel ‚Verfügbarkeit‘</b>	
Löschkonzept	Eine Woche
Anlagen zum Löschkonzept	Ein Tag

Tabelle 1, Klassifikation der Dokumente des Löschkonzeptes

## 2 Inhalt des Löschkonzeptes

Diese Anlage beinhaltet die aktuelle Version der Beschreibung des Löschkonzeptes des ‚Gesundheitsamt Musterstadt‘ (nachfolgend mit ‚GA Musterstadt bezeichnet).

Damit erfüllt das GA Musterstadt die Verpflichtungen nach

- Artikel 5, Abs. 1, Buchst. c und e DSGVO, Grundsätze für die Verarbeitung personenbezogener Daten.

Im Löschkonzept müssen neben den Grundprinzipien ‚Datenminimierung‘ und ‚Speicherbegrenzung‘ aus der DSGVO auch die Anforderung anderer Gesetze nach sicherer Archivierung beachtet werden.

Auf das Löschkonzept wird Bezug genommen u. a. in der Beschreibung der einzelnen Geschäftsprozesse, in denen personenbezogenen Daten verarbeitet werden und in der Anlage 06, Beschreibung der Technischen und Organisatorischen Maßnahmen (TOM).

Dieses Löschkonzept orientiert sich an der Norm DIN 66398 (2016): Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten.

## 3 Geltungsbereich

Diese Anlage gilt für die Verarbeitung personenbezogener Daten durch Beschäftigte von GA Musterstadt.

Diese Anlage gilt für alle Standorte von GA Musterstadt.

Diese Anlage verpflichtet alle Beschäftigte von GA Musterstadt zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

## 4 Hintergrund

### 4.1 Gegenstand und Ziele des Löschkonzeptes

In diesem Löschkonzept legt die Geschäftsleitung des GA Musterstadt fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von personenbezogenen Daten (pbD) erfüllt.

Dazu gehören:

- eine Beschreibung der Vorgehensweise für die Festlegung von Löschrregeln für personenbezogene Datenbestände,
- eine Übersicht über notwendige Umsetzungsvorgaben zur Löschung durch die verantwortliche Stelle,
- Vorgaben für die Dokumentationsstruktur und
- Anforderungen an Prozesse und Verantwortung für die Etablierung, Fortschreibung und Umsetzung des Löschkonzeptes

Dieses Konzept soll die folgenden Ziele unterstützen:

- Der Ressourcenbedarf der Beteiligten soll möglichst geringgehalten werden.
- Es werden gemeinsame Begriffe für die Diskussionen zwischen Datenschutzverantwortlichen, fachlichen Anwendern, Administratoren, Software-Entwicklern und anderen Beteiligten bereitgestellt.
- Es werden möglichst wenige und einfache Löschrregeln definiert. Dadurch soll das Löschkonzept von den Beteiligten besser verstanden und leichter umgesetzt werden.
- Der Dynamik von Veränderungen an Geschäftsprozessen und IT-Systemen wird Rechnung getragen.

Diese Ziele können nur erreicht werden, wenn die Komplexität des Löschkonzeptes im Rahmen der einschlägigen Rechtsvorschriften so weit wie möglich reduziert wird.

### 4.2 Begriffe und Definitionen

**Anonymisieren:**

Prozess, durch den personenbezogene Daten (pbD) so verändert werden, dass der Betroffene nicht mehr direkt oder indirekt identifiziert werden kann.

**Aufbewahrungsfrist:**

Frist, für die eine Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein muss.

**Betroffener:**

natürliche Person oder anderes Schutzsubjekt, auf das sich Daten beziehen.

**Datenart:**

Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird.

**Datenbestand:**

eine Menge an personenbezogenen Daten der verantwortlichen Stelle.

**Datenobjekt:**

Sammelbezeichnung für Objekte wie z. B. Dateien, Dokumente, Datensätze oder Attribute.

**Dokument:**

Schriftstück, in dem Teile des Löschkonzepts oder seiner Umsetzung beschrieben werden.

**Einschlägige Rechtsvorschriften:**

die für einen spezifischen Datenbestand geltenden datenschutzrechtlichen Regelungen.

**Löschen:**

Behandeln von personenbezogenen Daten derart, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können.

**Löschklasse:**

Kombination aus Löschfrist und abstraktem Startzeitpunkt für den Fristlauf.

**Löschkonzept:**

Festlegungen, mit denen eine verantwortliche Stelle sicherstellt, dass ihre personenbezogenen Datenbestände rechtskonform gelöscht werden.

**Löschregel:**

Kombination aus Löschfrist und Bedingung für den Startzeitpunkt des Fristlaufs.

**Personenbezogene Daten (pbD):**

Einzelangaben über persönliche oder sachliche Verhältnisse eines Betroffenen.

**Regellöschfrist (Löschfrist):**

Frist, nach der eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle spätestens zu löschen ist.

**Verantwortliche Stelle:**

Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. In diesem Sinne ist GA Musterstadt die verantwortliche Stelle.

**Vorhaltefrist:**

Frist, für die eine Datenart zur Verwendung in der verantwortlichen Stelle verfügbar sein muss.

## 5 Grundlagen des Löschkonzeptes

### 5.1 Allgemeines

Dieses Konzept bezieht sich nur auf das Löschen von pbD. Es beschreibt, wie es etabliert wird und welche Festlegungen dafür getroffen und dokumentiert werden müssen.

Dieser Abschnitt stellt die Bausteine des Löschkonzepts im Überblick vor. In den weiteren Abschnitten werden die einzelnen Bausteine detailliert beschrieben.

GA Musterstadt muss als verantwortliche Stelle im Sinne der einschlägigen Rechtsvorschriften das datenschutzkonforme Löschen von pbD sicherstellen. Für eine dauerhafte Umsetzung von

Löschprozessen, die den gesamten Bestand an pbD des GA Musterstadt abdecken, ist ein strukturiertes und geregeltes Vorgehen erforderlich. Die Festlegungen müssen umfassen,

- welche Löschrregeln für welche Datenbestände gelten,
- wie die Umsetzung der Löschung in Prozessen des GA Musterstadt erreicht wird,
- wie die Löschrregeln, Umsetzungsvorgaben und durchgeführten Löschrmaßnahmen zu dokumentieren sind und
- wer für die aus dem Löschkonzept entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung verantwortlich ist.

Diese Festlegungen bilden das Löschkonzept des GA Musterstadt.

## 5.2 Was bedeutet ‚Löschen‘

Datenobjekte, die Personenbezug aufweisen, werden gemäß der Definition gelöscht, wenn sie nach der Löschung nicht mehr vorhanden sind, unkenntlich sind und nicht mehr verwendet werden können. Löschr wird z. B. durch das physische Überschreiben von Datenobjekten erreicht.

Datenobjekte können auch gelöscht werden, indem der Datenträger, auf dem sie enthalten sind, geeignet zerstört oder vernichtet wird.

Gegebenenfalls können die Datenobjekte auch anonymisiert werden, statt sie zu löschen. Denn wenn kein Personenbezug mehr hergestellt werden kann, unterliegen sie nicht mehr den datenschutzrechtlichen Löschrregeln. Das Anonymisieren von pbD ist Gegenstand des ‚Anonymisierungs- / Pseudonymisierungskonzept‘ des GA Musterstadt.

## 5.3 Eine Löschrregel für jede Datenart

### 5.3.1 Datenarten

Es muss entschieden werden, wann pbD zu löschen sind. Die einschlägigen Rechtsvorschriften fordern in der Regel, dass Daten gelöscht werden müssen, wenn sie nicht mehr erforderlich sind. Außerdem sind für eine datenschutzgerechte Gestaltung von IT-Prozessen die Prinzipien „Transparenz“ (Art. 5 Abs. 1 lit. a), „Datenminimierung“ (Art. 5 Abs. 1 lit. c), „Richtigkeit“ (Art. 5 Abs. 1 lit. d), „Speicherbegrenzung“ (Art. 5 Abs. 1 lit. e), „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f) und insbesondere die Zweckbindung (Art. 5 Abs. 1 lit. b) anzuwenden. Danach sind pbD so früh wie möglich zu löschen.

Soweit Teile des Gesamtdatenbestandes des GA Musterstadt für unterschiedliche Zwecke verwendet werden, können sich auch unterschiedliche Regeln für die Löschung ergeben.

Ein Teil des Datenbestandes, der für einen einheitlichen fachlichen Zweck verwendet wird, bildet eine Datenart, unabhängig davon wo die Daten im Einzelfall gespeichert werden. Jeder so abgegrenzten Datenart wird dann eine Löschrregel zugeordnet.

Für eine klare Kommunikation über das Löschkonzept ist es sinnvoll, jede Datenart eindeutig zu bezeichnen. Die Bezeichnung soll sich am fachlichen Verwendungszweck in den Geschäftsprozessen des GA Musterstadt orientieren und zwischen der Datenschutzbeauftragten und den anderen Beteiligten abgestimmt werden.

### 5.3.2 Löschrregeln

Personenbezogene Daten sollen nicht nur zufällig, sondern nach sinnvollen Regeln gelöscht werden. Deshalb wird für jede Datenart eine datenschutzkonforme Löschrregel definiert. Jede Löschrregel enthält eine Löschrfrist und einen Startzeitpunkt, ab dem die Frist zu laufen beginnt.

Löschrregeln, die die Löschung des gesamten Datenobjekts vorgeben, sind in der Regel einfach zu dokumentieren und zu implementieren. Wenn ein Datenobjekt nur anonymisiert werden soll, muss für die Attribute im Einzelnen geprüft und festgelegt werden, wie dies hinreichend sicher erfolgt. In der Regel ist es daher viel aufwändiger, Anonymisierungsregeln zu erstellen und zu implementieren, als Datenobjekte insgesamt zu löschen.

### 5.3.3 Vorhaltefrist und Regellöschrfrist

#### 5.3.3.1 Löschr im Regelprozess

Für jede Datenart ist zu klären, wie lange sie in Geschäftsprozessen benötigt wird. Der Zeitraum, innerhalb dessen sie auf Grund eigener fachlicher Anforderungen oder gesetzlicher Aufbewahrungspflichten **mindestens** verfügbar sein muss, wird als **Vorhaltefrist** bezeichnet.

Rechtliche Aufbewahrungspflichten sind Teil des Verwendungsprozesses in der verantwortlichen Stelle und damit auch Teil der Aufbewahrungsfrist. Sie ergeben sich, wenn in einschlägigen Rechtsvorschriften Mindestfristen für die Aufbewahrung von Datenarten festgelegt sind. Aufbewahrungsfristen können sich auch aus vertraglichen Vereinbarungen ergeben.

Schließlich können auch andere fachliche Anforderungen dazu führen, dass eine verantwortliche Stelle Datenarten für einen Zeitraum nach dem Ende der aktiven Verwendung der Daten aufbewahren will. Aus den verschiedenen Anforderungen ergeben sich überlappende Anteile der Aufbewahrungsfrist.

Die Aufbewahrungsfrist für eine Datenart impliziert, dass diese Datenart in mindestens einem System bis zu ihrem Ende verfügbar sein muss.

Die datenschutzrechtlichen Vorschriften können besondere Maßnahmen fordern, wenn Datenobjekte nur noch gespeichert werden, um Aufbewahrungspflichten zu erfüllen. In einem solchen Fall sollen die Daten gesperrt werden. Die Daten dürfen also nur noch für die Zwecke benutzt werden, für die sie aufbewahrt werden. Als Konsequenz daraus soll bei jeder Löschrregel geprüft werden, ob eine Regel für die Sperrung der jeweiligen Datenart mit festgelegt werden muss.

Nach dem Ende der jeweiligen Aufbewahrungsfrist werden die Daten in der verantwortlichen Stelle nicht mehr benötigt. Sie müssen dann innerhalb einer datenschutzrechtlichen vertretbaren Frist gelöscht werden. Die Summe aus Aufbewahrungsfrist und der datenschutzrechtlich vertretbaren Frist für die Gestaltung der Löschrprozesse definiert die längste Löschrfrist bei der Verarbeitung der Daten im Regelprozess. Diese Frist wird als **Regellöschrfrist** bezeichnet. Nach Ablauf der Regellöschrfrist müssen die entsprechenden Bestände der Datenart in allen Systemen der verantwortlichen Stelle gelöscht sein. Dies schließt die Löschrung bei Auftragnehmern des GA Musterstadt ein.

Soweit die Verwendung von pbD nach der jeweiligen Rechtsordnung einer Rechtsgrundlage bedarf, bestimmen die zulässigen Verwendungszwecke auch die Aufbewahrungsfrist und die Regellöschrfrist. Wenn die Rechtslage Spielräume für die Fristen zur Verwendung einer Datenart einräumt, kann der Verwendungs- und Löschrprozess gestaltet werden. GA Musterstadt muss abschätzen und

datenschutzrechtlich verantworten, ob und wie lange nach dem Ende der Aufbewahrungsfrist die Löschung erfolgen kann.

(vgl. Abb. 1)

### Beispiel Fristabschnitte im Löschkonzept

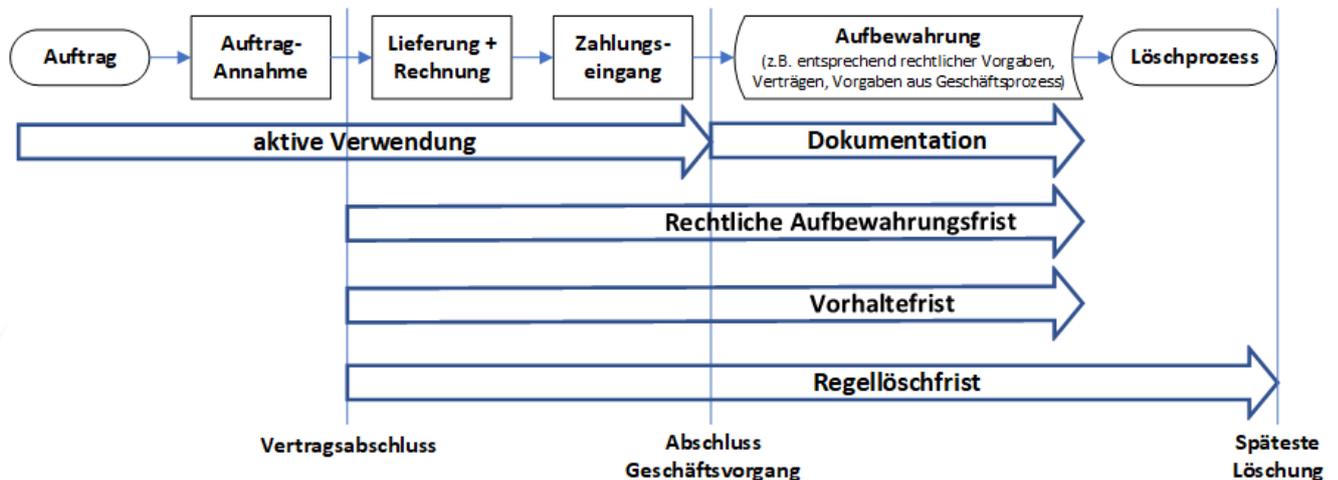


Abbildung 1: Beispiel Fristabschnitte im Löschkonzept

#### 5.3.3.2 Löschen in Ausnahmefällen, bei Störfällen und in Sondersituationen

Wenn Daten in **Ausnahmefällen** in einem vom Regelbetrieb abweichenden Prozess verwendet werden, können sie für diese Verarbeitung einer anderen Datenart zugeordnet werden, soweit dies nach den einschlägigen Rechtsvorschriften zulässig ist (Abschnitt 7.3.3).

Zur Behandlung von **Störfällen** kann die Löschung zeitweise ausgesetzt werden (Abschnitt 7.3.4).

Das Löschen in manchen **Sondersituationen** kann nicht von Löschrregeln im Sinne dieses Löschkonzeptes bestimmt werden. Dazu gehören:

- das Löschen von unberechtigt erhobenen pbD,
- das Löschen von pbD nach einem berechtigten Löschbegehren des Betroffenen,
- das Löschen von pbD beim Rückbau von Systemen.

Für diese und ähnliche Sonderfälle müssen ebenfalls Löschrmaßnahmen bestimmt werden. Sie sind im Rahmen der Prozesse und Verantwortlichkeiten für das Löschen von pbD zu organisieren (vgl. Kapitel 10).

Voraussetzung für das Löschen einzelner Daten von Betroffenen ist, dass die technischen Systeme über eine geeignete Funktion zum Löschen verfügen. Diese Funktion muss bereits bei der Systembeschaffung oder -entwicklung berücksichtigt werden.

## 5.3.4 Unterscheidung zwischen Archiv, Sicherungskopie und gesperrten Daten

### 5.3.4.1 Archive und Sicherungskopien

Für das Löschkonzept ist eine klare Unterscheidung zwischen Archiven und Sicherungskopien notwendig.

**Archive** dienen dazu, Daten langfristig vorzuhalten. Daten werden häufig in Archive verlegt, wenn an Datensätzen oder anderen Beständen keine Veränderungen mehr vorgenommen werden, sie jedoch aus zulässigen Gründen weiterhin aufbewahrt werden müssen. Ein Archiv kann unterschiedliche Datenarten mit unterschiedlichen Löschrufen enthalten.

**Sicherungskopien (Backup)** dürfen nicht als Archive verwendet werden, denn sie haben eine andere Funktion. Sie werden zur Wiederherstellung von Systemen und Datenbeständen nach Störungen benötigt. Sie dürfen daher nicht verändert werden.

Sicherungskopien existieren in der Regel in verschiedenen Versionen oder Versionsketten. Jede der Versionen kann unterschiedlich alte Datenbestände der gleichen Datenart enthalten. Die einzelnen Instanzen von Datenobjekten erreichen daher ihre Löschrufen zu sehr unterschiedlichen Zeiten. Zur Einhaltung von Löschrufen wären deshalb häufig einzelne Daten aus den Sicherungskopien zu löschen.

Zwischen Sicherungskopien und Archiven muss deshalb klar getrennt werden. Die pbD in Archiven unterliegen den Löschrufen der jeweiligen Datenarten und müssen nach diesen Regeln im Archiv gelöscht werden. Für die Löschung von Sicherungskopien müssen dagegen eigene Fristen festgelegt werden, die bezüglich der Regellöschrufen der im Backup enthalten „gemischten“ Daten verhältnismäßig sind (siehe Abschnitt 7.3.5).

### 5.3.4.2 Gesperrte Datenbestände

Manche Rechtsvorschriften verlangen, dass Datenbestände besonderen Zugriffsbeschränkungen unterliegen, wenn sie nicht mehr für produktive Prozesse benötigt werden (**Sperrung von Daten**). Beispiele hierfür sind Datenbestände, die nur noch zu Dokumentationszwecken gespeichert werden oder solche, die nur noch der Fehlerbehebung oder Fehleranalyse dienen. Die Zugriffsrechte sind dann auf die Mitarbeiter einzuschränken, die die verbliebenen Aufgaben bearbeiten.

Für Datenbestände des GA Musterstadt soll stets geprüft werden, ob neben den Löschrufen auch Sperrregeln festgelegt werden.

## 5.3.5 Standardlöschrufen, Startzeitpunkte, Löschrufen und Löschklassen

Für die Festlegung der Löschrufen für einzelne Datenarten kann vielfältiger Analyseaufwand entstehen. Die Datenschutzbeauftragte muss stets an der datenschutzrechtlichen Bewertung von Abläufen beteiligt sein. Zum Aufwand trägt bei, dass Geschäftsprozesse und IT-Systeme teilweise mit hoher Dynamik geändert werden. Das kann auch wiederholte Analysen erfordern.

Beim GA Musterstadt sollen deshalb **Standardlöschrufen** verwendet werden, die sich an den einschlägigen Rechtsvorschriften orientieren.

Auch die **Startzeitpunkte** für die Löschfristen lassen sich zu wenigen abstrakten Kategorien gruppieren. Beispiel: Ein solcher abstrakter Startzeitpunkt ist „Entstehung der Daten“, ein anderer „Ende eines Vorgangs“.

Die Standardlöschfristen und die abstrakten Startzeitpunkte werden kombiniert. Jede Kombination von Löschfrist und Startzeitpunkt bildet eine sogenannte **Löschkategorie**.

Die Datenarten können den Löschkategorien auf einfache und effiziente Weise zugeordnet werden. In einer Löschkategorie werden alle Datenarten zusammengefasst, die der gleichen Löschfrist unterliegen und für die der gleiche abstrakte Startzeitpunkt gilt.

Von den Beteiligten kann somit gut verglichen und geprüft werden, ob die Datenarten richtig eingeordnet wurden.

## 5.4 Etablieren des Löschkonzeptes

### 5.4.1 Dokumentation des Löschkonzeptes

Die schriftliche Dokumentation des Löschkonzeptes des GA Musterstadt muss folgendes beinhalten:

- Festlegungen des Löschkonzeptes,
- Umsetzung der Festlegungen,
- Protokolle der Durchführung von Löschungen und
- Protokoll der regelmäßigen Überprüfung des Löschkonzeptes und der Festlegungen.

Diese Dokumentation ist ein Bestandteil des Datenschutz-Managementsystem (DSMS) bzw. des Informationssicherheitsmanagement-System (ISMS) des GA Musterstadt.

### 5.4.2 Prozesse und Verantwortlichkeiten

Das GA Musterstadt muss für die Umsetzung des Löschkonzeptes Prozesse definieren und Verantwortlichkeiten festlegen.

Diese Festlegung erfolgt bereits zu einem Teil in Kapitel 10 dieses Dokumentes.

### 5.4.3 Phasen in der Umsetzung des Löschkonzeptes

Um den Implementierungsaufwand für Löschrmaßnahmen zu reduzieren, sollen die Löschrregeln für alle Arten von pbD in einem IT-System gemeinsam implementiert werden.

Zusätzlich ist zu berücksichtigen, ob zwischen den Löschrfunktionen in verschiedenen IT-Systemen Abhängigkeiten bestehen, weil Datenbestände in Folgesystem abhängig von Daten in Primär-Systemen zu löschen sind. Solche Abhängigkeiten müssen für die Implementierung von Löschrmaßnahmen in einem IT-System berücksichtigt werden.

Es sollen deshalb in einer **ersten Phase** zur Etablierung des Löschkonzeptes die Löschrregeln möglichst vieler Datenarten bestimmt werden. Dazu sind

- die Datenarten festzulegen (Kap. 6),

- die Standardlöschfristen zu bestimmen (Kap. 7),
- die Datenarten den Löschklassen zuzuordnen (Kap. 8.3) und
- alle Löschrregeln zu dokumentieren.

Diese Festlegungen sind in den Dokumenten „Löschrregeln“ und „Umsetzungsvorgaben für Querschnittsbereiche“ beschrieben (Kap. 11).

In der **zweiten Phase** erfolgt die Implementierung der Löschrregeln für die Regelprozesse. Dazu sind die Umsetzungsvorgaben zu erstellen und zu realisieren.

Die Reihenfolge der Maßnahmen sollte so bestimmt werden, dass

- Bestände mit sehr sensiblen Datenarten hoch priorisiert werden,
- Datenarten mit kurzen Löschrfristen hoch priorisiert werden,
- Datenarten mit großen Beständen, die bereits die Löschrfrist überschritten haben, möglichst bald bereinigt werden und
- abhängige Systeme auf die Löschrung in Primär-Systemen vorbereitet sind.

Mit Abschluss der zweiten Phase sollten die initialen Aufgaben, die einen vergleichsweise hohen Aufwand erfordern, umgesetzt sein. Die Regellöschrfristen, die Zuordnung der Verantwortung und die Prozesse des Löschrkonzepts sind dann etabliert.

In der **dritten Phase** erfolgt die kontinuierliche Umsetzung der Löschrungen, die Fortschreibung des Löschrkonzepts und die Pflege seiner Umsetzungsvorgaben in den Regelprozessen des GA Musterstadt.

Änderungen im Löschrkonzept, in den Festlegungen und Umsetzungsvorgaben sollen im Rahmen des Change-Managements des GA Musterstadt vorgenommen werden.

sor

## Phasen in der Umsetzung des Löschkonzeptes

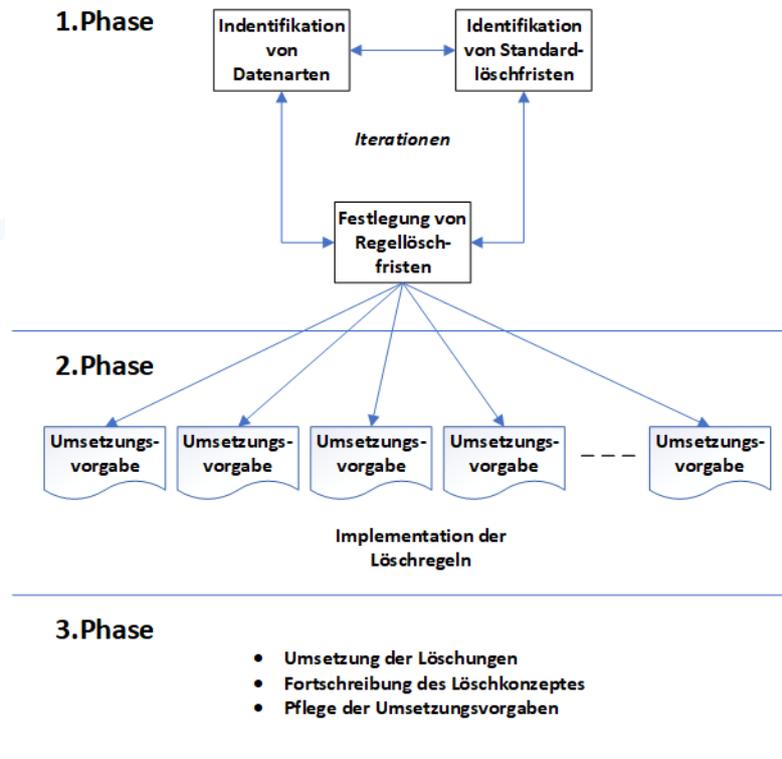


Abbildung 2: Phasen in der Umsetzung des Löschkonzeptes

## 6 Datenarten festlegen

Folgende Aspekte sollen bei der Festlegung der Datenarten berücksichtigt werden.

### 6.1 Beispiele für Datenbestände, Zwecke und Datenarten

Datenbestände können nach Verwendungszwecken logisch unterschieden werden. Die Unterscheidung ist nach den einschlägigen Rechtsvorschriften und den fachlichen Zwecken zu treffen. Die unterschiedenen Bestände werden als Datenarten bezeichnet. Unterschiedliche Zwecke und damit unterschiedliche Datenarten ergeben sich insbesondere, wenn

- die einschlägigen Rechtsvorschriften unterschiedliche Vorgaben für Datenbestände machen,
- sich Datenbestände auf unterschiedliche Betroffene beziehen,
- sich die Rechtsgrundlage für die Erhebung von Datenbeständen unterscheidet oder die in der Rechtsgrundlage angegebenen Zwecke für verschiedene Datenbestände unterschiedlich sind,
- Datenbestände nur innerhalb von eigenständigen Teilprozessen verwendet werden.

Datenbestände können unterschiedlich strukturiert sein, z. B. in Form von Attributen oder Datensätze in Datenbanken, in Dateien oder in Form von Dokumenten. Im Weiteren wird die Bezeichnung ‚Datenobjekt‘ stellvertretend für die verschiedenen Objekte verwendet, die einer Datenart zuzuordnen sind. Datenobjekte können Daten in unterschiedlicher Granularität sein, beispielsweise Attribute, Datensätze, elektronische Dokumente oder Ausdrücke.

sormas

Eine Datenart kann durch alle Datenobjekte gebildet werden, die zu einem Zweck verarbeitet werden. Der Datenbestand einer Datenart kann an verschiedenen Speicherorten abgelegt sein, z. B. in mehreren Tabellen einer Datenbank und in den Dateien, aus denen er eingelesen wurde.

(BEISPIELE: Beispiele für Datenarten sind: Buchhaltungsdaten, Vertragsdokumente oder Protokolle, in denen Anmeldungen an IT-Systemen aufgezeichnet werden. Zur Datenart ‚Buchhaltungsdaten‘ könnten z. B. die Datenobjekte ‚Buchungssatz‘ (mit den Angaben zu Kreditor/Debitor, Zahlungszeitpunkt und Betrag) wie auch Rechnungen und Zahlungstransaktionen mit Banken gehören.)

Eine Datenart kann durch die Datenobjekte gebildet werden, die den Personenbezug herstellen sowie die Datenobjekte, die zum jeweiligen Zweck verwendet werden. Der Personenbezug kann in der Regel über ein oder mehrere identifizierende Attribute hergestellt werden. Da es sich bei den hier betrachteten Datenarten um pbD handelt, enthält jede Datenart Datenobjekte, durch die die Betroffenen identifiziert werden können.

(BEISPIELE: Name, Adresse und Geburtsdatum, eine eindeutige Kundennummer oder technische Schlüssel, die den Rückschluss auf den Betroffenen zulassen, sind solche identifizierenden Attribute. Name, Anschrift und Kundennummer sind einerseits Teil der Datenart „Stammdaten des Kunden“ und werden immer auch auf Rechnungen verwendet, sind also auch Teil der Datenart „Buchhaltungsdaten“).

In der Regel sind in verschiedenen Datenarten die gleichen identifizierenden Attribute enthalten. Wenn ein anderes Datenobjekt zu verschiedenen Zwecken verwendet wird, kann es ebenfalls sinnvoll sein, es in mehrere Datenarten aufzunehmen. Dies sollte insbesondere dann erfolgen, wenn die Datenarten unterschiedlichen Löschregeln unterliegen. Die Löschregeln der verschiedenen Datenarten müssen für die jeweils zugehörigen Datenobjekte eindeutig sein.

(BEISPIEL: Die Datenart "Protokolle" enthält alle Datensätze, die für Ereignisse an einem IT-System zum Zweck des Monitorings aufgezeichnet werden. Für Protokolle könnte eine einheitliche Löschrfrist von 42 Tagen nach Aufzeichnung gelten, weil sie monatlich ausgewertet werden. Gleichzeitig will die verantwortliche Stelle aber den Zustand des IT-Systems nachvollziehen können und verwendet dazu Datenobjekte in der Datenart „Systemzustandsdokumentation“. Ausgewählte Log-Datensätze werden auch in die Systemzustandsdokumentation übernommen, weil sie Zustände und Auffälligkeiten in Systemkomponenten, Defekte und erfolgreiche Reparaturen belegen. Für die Log-Datensätze der Datenart Systemzustandsdokumentation wird eine eigene Löschregel definiert, z. B. 4 Jahre nach Aufzeichnung, die auch die dort enthaltenen Log-Datensätze umfasst. Wenn erkannt wird, dass die Datenarten mit überschneidenden Datenobjekten der gleichen Löschregel unterliegen, kann es sinnvoll sein, die Datenobjekte in einer Datenart zusammenzufassen.)

Die Zuordnung von Datenobjekten zu Datenarten ist organisationsspezifisch festzulegen, da einzelne Datenobjekte je nach verantwortlicher Stelle unterschiedlich verwendet werden können.

(BEISPIELE: Für die Verwaltung von Kundenbeziehungen kann zwischen Datenobjekten unterschieden werden, die nur während der aktiven Kundenbeziehung und kurz danach benötigt werden und solchen, die wegen Aufbewahrungspflichten noch mehrere Jahre danach vorgehalten werden müssen. Diese Unterscheidung ist oft auch für Datenobjekte von Stammdaten möglich. Z. B. könnten die „ergänzenden Stammdaten“ als Datenart für Informationen verwendet werden, die Kontaktdaten der aktiven Kundenbeziehung enthalten. Datenobjekte, die erforderlich sind, um das Kundenkonto zu bilden (das aufrechterhalten

werden muss, um den Aufbewahrungspflichten nachzukommen), könnten der Datenart „Kernstammdaten“ zugeordnet werden. In einer Bank wird die Kontonummer eines Kunden dann vermutlich in die Datenart Kernstammdaten eingeordnet. Ein Versandhändler benötigt die Kontonummer eines Kunden dagegen nur als Bankverbindung, beispielsweise für Gutschriften, und ordnet sie deshalb in die Datenart „ergänzende Stammdaten“ ein. Bei ihm würden die Kernstammdaten die Kundennummer, Name und Adresse umfassen.)

## 6.2 Datenarten systematisch erfassen

Im Löschkonzept des GA Musterstadt soll sichergestellt werden, dass alle Datenobjekte, die als pbD einzustufen sind, Datenarten zugeordnet werden.

Dazu soll zunächst identifiziert werden, welche Datenarten in den verschiedenen Geschäftsprozessen verwendet werden.

Zusätzliche Datenarten ergeben sich aus den Arbeiten am Löschkonzept und seiner Umsetzung in mehreren Iterationen:

- Im Rahmen der Festlegung von Löschklassen und Löschrregeln für die bereits identifizierten Datenarten kann festgestellt werden, dass einzelne Datenarten aufgeteilt werden müssen.
- Im Kontext der Festlegung von Umsetzungsvorgaben muss bestimmt werden, welche Datenbestände in konkreten IT-Systemen oder anderen Abläufen verwendet werden. Alle Datenbestände mit Personenbezug müssen einer Datenart zugeordnet werden. Wenn dies für einen Datenbestand nicht möglich ist, weil er für einen bisher nicht identifizierten Zweck verwendet wird, muss eine neue Datenart definiert werden.

## 6.3 Gestaltungskriterien für die Bildung von Datenarten

### 6.3.1 Datenarten aus den fachlichen Zusammenhängen

Vielfach ist die Bildung von Datenarten aus fachlichen Zusammenhängen naheliegend. Die folgenden Unterscheidungsmöglichkeiten helfen bei der Zuordnung von Datenobjekten zu Datenarten.

#### 6.3.1.1 Orientierung an Rechtsvorgaben

Wenn für Gruppen von Datenobjekten einheitliche Rechtsregeln gelten, ist es sinnvoll, sie in einer Datenart zusammenzufassen. Wenn Aufbewahrungspflichten nur für bestimmte Teile einer Datenart gelten würden, und dadurch die Regellöschfrist insgesamt erheblich verlängert würde, sollten sie auf verschiedene Datenarten aufgeteilt werden.

#### 6.3.1.2 Orientierung an Verwendungszwecken

Wenn Gruppen von Datenobjekten gemeinsam verwendet und gelöscht werden, kann es sinnvoll sein, sie in einer Datenart zusammenzufassen.

Die Namen der Datenarten dienen der Verständigung zwischen den am Löschkonzept beteiligten Gruppen von Datenobjekten. Es kann daher sinnvoll sein, für Datenbestände, die fachlich unterschiedlich verwendet werden, verschiedene Datenarten einzuführen, obwohl sie den gleichen Löschrregeln unterliegen.

(BEISPIEL: Die ergänzenden Stammdaten eines Kunden können in einem Kundenstammdatensatz gespeichert werden. Sollen die Daten geändert werden, werden Änderungsaufträge für ergänzende Stammdaten angelegt, die möglicherweise – genauso wie die ergänzenden Stammdaten – ein Jahr nach dem Ende der Kundenbeziehung gelöscht werden sollen. Obwohl die Änderungsaufträge wie die eigentlichen ergänzenden Stammdaten gelöscht werden, kann es für die fachlichen Diskussion sinnvoll sein, sie als eigene Datenart zu führen.)

Wenn sich Datenobjekte auf unterschiedliche Gruppen von Betroffenen beziehen, kann es sinnvoll sein, getrennte Datenarten zu bilden.

(BEISPIELE: Kontaktdaten wie Ansprechpartner, Telefonnummern und E-Mail-Adressen können z. B. für Kunden, Mitarbeiter von Lieferanten und Servicetechniker von Dienstleistern gespeichert werden. In der Regel ist es dann sinnvoll, zwischen den Datenarten "ergänzende Stammdaten von Kunden", "ergänzende Stammdaten von Lieferanten" und "ergänzende Stammdaten von Servicetechnikern" zu unterscheiden.)

Wenn Datenobjekte mit stark unterschiedlichen Vorhaltefristen in einem Datenbestand enthalten sind, ist es sinnvoll, diese in unterschiedliche Datenarten zu gruppieren. Wenn alle pbD einer Datenart aus produktiven Beständen archiviert werden müssen, dann geht die Archivierungsdauer in die Regellöschfrist ein. Wenn nur einige ausgewählte Bestände einer Datenart archiviert werden sollen, sollte dieser Bestand eine eigene Datenart bilden.

### 6.3.2 Vertraulichkeitsklassifikation und Datenarten

Daten hoher Sensitivität, beispielsweise Patientendaten oder generell besondere Arten pbD, sind auch mit hoher Vertraulichkeit zu behandeln. Da das sichere Löschen von Daten deren künftige Vertraulichkeit sicherstellt, stehen für eine eventuelle Erweiterung der Vorhaltefrist zu einer längeren Regellöschfrist in der Regel nur geringe Spielräume zur Verfügung. Eine verzögerte Löschung von Datenarten mit hoher Sensitivität ist daher datenschutzrechtlich besonders kritisch zu prüfen.

Datenarten hoher Sensitivität müssen in der Regel vertraulicher behandelt werden als pbD niedriger Sensitivität. Grundsätzlich kann einer Datenart auch die Schutzstufe einer entsprechenden Vertraulichkeitsklassifikation zugeordnet werden. Dadurch wird implizit festgelegt, welchen Sicherheitsanforderungen die Löschrmechanismen genügen müssen, die für die Datenart angewandt werden.

Wenn mit einer Löschrregel allerdings unterschiedliche Vertraulichkeitsstufen umgesetzt werden sollen, müssten mehrere Datenarten gebildet werden. Dadurch würden die Anzahl der Löschrregeln und die Umsetzungskomplexität des Löschrkonzepts erhöht. Es erscheint stattdessen sinnvoller, allen Teilen der Datenart die höhere Vertraulichkeitsstufe zuzuweisen. Dadurch wird für diese Datenart eine einheitliche Löschrregel einem Sicherheitsniveau definiert.

## 7 Löschrfristen festlegen

Folgende Aspekte sollen bei der Festlegung der Löschrfristen berücksichtigt werden.

## 7.1 Standardlöschfristen verwenden

Ein sehr wichtiger Baustein zur Vereinfachung des Löschkonzepts ist die Verwendung von Standardlöschfristen. Sie erleichtern das Verständnis des Löschkonzepts und sparen Ressourcen bei allen Beteiligten. Standardlöschfristen sollten immer eingesetzt werden, wenn unter Datenschutz-Gesichtspunkten auf eine feingranulare Festlegung von Löschrfristen verzichtet werden kann und stattdessen eine Nutzung der jeweils „nächstgelegenen“ Standardlöschfrist ausreicht.

Standardlöschfristen werden von jeder verantwortlichen Stelle für ihren Bereich festgelegt. Mit den in Abschnitt 7.2 vorgeschlagenen Vorgehensweisen zur Fristdefinition kann sie Löschrfristen bestimmen und Standardlöschfristen auswählen. Die Standardlöschfristen werden verwendet, um die Löschklassen zu bilden (siehe Kapitel 8). Es wird empfohlen, die Zahl der Standardlöschfristen klein zu halten.

Einer Datenart mit einer Vorhaltefrist, die nicht ohnehin einer Standardlöschfrist entspricht, wird die nächst größere Standardlöschfrist zugewiesen. Die Differenz der gewählten Standardlöschfrist zur Vorhaltefrist muss unter dem Gesichtspunkt der einschlägigen Rechtsvorschriften verhältnismäßig und vertretbar sein. Andernfalls ist zu prüfen, ob eine zusätzliche Standardlöschfrist sinnvoll ist.

Zur Festlegung ihrer Standardlöschfristen kann die verantwortliche Stelle auf Fristkataloge zurückgreifen, soweit solche vorhanden und geeignet sind. Für spezifische Zwecke muss die verantwortliche Stelle aber prüfen, ob es notwendig ist, dass sie eigene Standardlöschfristen festlegt.

Die Begrenzung auf wenige Standardlöschfristen hat sich in der praktischen Umsetzung bewährt. Viele Standardlöschfristen führen zu Komplexität sowohl bei Festlegung der Regellöschfristen als auch für die nachgelagerten Maßnahmen zur Implementierung und betrieblichen Umsetzung der Löschrmaßnahmen. Die Zahl der Standardfristen soll einen guten Kompromiss zwischen einer datenschutzrechtlich vertretbaren Fristabstufung und einer beherrschbaren Komplexität der Fristen ermöglichen.

Der Grund für eine Begrenzung auf wenige Standardlöschfristen ist ein einfach verständliches Löschkonzept und die einfache Ableitung von Löschrregeln. Standardfristen für einzelne Datenarten einzuführen, widerspricht diesem Ziel. Wenn die Überschreitung der Vorhaltefrist nur für eine einzelne Datenart als Spezialfall nicht vertretbar ist, kann es daher sinnvoll sein, für diese Datenart eine besondere Löschrfrist zu verwenden, die nicht in den Katalog der Standardfristen aufgenommen wird. Nach Möglichkeit sollten die Sonderfälle aber vermieden werden. Alternativ sollte für solche Datenarten geprüft werden, ob die Vorhaltefrist nicht durch Anpassungen des Verwendungsprozesses verkürzt werden kann, um nach der nächst kürzeren Standardfrist zu löschen.

## 7.2 Fristfestlegungen

### 7.2.1 Übersicht über die Vorgehensweisen zur Fristdefinition

Wenn die verantwortliche Stelle eigene Löschrfristen festlegen muss, benötigt sie dafür geeignete Vorgehensweisen. Diese Vorgehensweisen müssen berücksichtigen:

- Die einschlägigen Rechtsvorschriften. Dazu gehören beispielsweise Vorgaben aus Gesetzen, Verordnungen oder vertraglichen Regelungen. Diese können sowohl konkrete Fristvorgaben machen als auch die Einhaltung allgemeiner Prinzipien wie Erforderlichkeit und Datensparsamkeit verlangen.

- Wie lange die pbD für die Zwecke der verantwortlichen Stelle in ihren Geschäftsprozessen benötigt werden (Regelverarbeitung). Dazu gehören auch alle rechtlich geforderten Prozessschritte, beispielsweise die Aufbewahrung von Unterlagen für die Prüfung durch Finanzbehörden.

Die einschlägigen Rechtsvorschriften räumen unterschiedlich große Gestaltungsspielräume ein, um Löschrufen zu bestimmen. Es treten drei Fälle auf, für die jeweils unterschiedliche Vorgehensweisen zur Fristanalyse verwendet werden:

- Für die Datenart ist in den Rechtsvorschriften eine Löschrufen angegeben: Die Löschrufen kann direkt übernommen werden.
- Für die Löschrufen der Datenart bestehen spezifische Rechtsvorschriften ohne konkrete Fristvorgabe oder die Sensitivität der Datenbestände erfordern eine enge Fristregelung: Für solche Datenarten muss die Fristfestlegung häufig durch die Analyse von Verwendungsprozess und die Interpretation der Rechtsvorschriften erfolgen.
- Die Löschrufen der Datenart muss nur an den allgemeinen Prinzipien der Erforderlichkeit und Datensparsamkeit ausgerichtet werden, beispielsweise in Deutschland nur nach § 35 BDSG: Die Ableitung von Standardlöschrufen anhand einfacher Kriterien ist ausreichend.

Im Regelfall ist es ausreichend, die Standardlöschrufen des Löschkonzepts anhand ausgewählter Datenarten festzulegen. Dazu werden in einem iterativen Prozess Datenarten identifiziert, die mögliche Stellvertreter für Löschrufen sind. Für diese erfolgt die Fristfestlegung und die Definition der Löschrufen. Wenn alle weiteren Datenarten in datenschutzrechtlich vertretbarer Weise den so gefundenen Löschrufen zugeordnet werden können (Kapitel 8), ist der Prozess abgeschlossen. Wenn Datenarten nicht geeignet zugeordnet werden können, müssen ein oder mehrere weitere Stellvertreter ausgewählt werden und weitere Löschrufen gebildet werden.

Fristen, die als Regellöschrufen für Kernprozesse der verantwortlichen Stelle identifiziert werden, sind häufig für viele Datenbestände und verschiedene Datenarten anzuwenden. Sie sind daher meist auch sinnvolle Standardlöschrufen.

(BEISPIEL: Ein Telekommunikations-Provider könnte beispielsweise die Frist für die Löschrufen von Einzelbindungsnachweisen als eine Standardfrist wählen. Ein Unternehmen, das Maut erhebt, würde dagegen die Löschrufen für Fahrtdaten als eine Standardfrist einsetzen.)

### 7.2.2 Unmittelbare Fristen aus Rechtsvorschriften

Wenn die einschlägigen Rechtsvorschriften feste Fristen für die Löschrufen von Datenarten vorgeben, müssen diese Fristen als Obergrenze für die Löschrufen herangezogen werden.

Die Prozesse der verantwortlichen Stelle müssen so gestaltet werden, dass die vorgegebene Frist in der Regelverarbeitung eingehalten wird.

Es ist sinnvoll, solche Fristen in den Katalog der Standardlöschrufen aufzunehmen, wenn der Katalog dadurch nicht zu sehr differenziert wird.

(ANMERKUNG: Wenn dies im Verwendungsprozess möglich ist, und die einschlägigen Rechtsvorschriften es zulassen, muss diese Frist aber nicht ausgeschöpft werden. Durch eine Verkürzung der Löschrufen gegenüber der Maximalfrist aus einer Rechtsvorgabe auf eine Standardlöschrufen kann die Zahl der Standardlöschrufen gegebenenfalls verringert werden.)

### 7.2.3 Fristfestlegung nach Prozessanalyse

Sensitive Datenarten oder Datenarten, für die die einschlägigen Rechtsvorschriften nur enge Spielräume für die Löschung zulassen, müssen kurz nach dem Wegfall der Erforderlichkeit gelöscht werden.

Die verantwortliche Stelle ist dann gehalten, die Vorhaltefrist für die jeweilige Datenart genau zu bestimmen, damit die Löschrfrist entsprechend eng daran orientiert werden kann. Dazu kann eine Analyse des Geschäftsprozesses durchgeführt werden. In dieser Prozessanalyse wird bestimmt, wie lange die einzelnen Prozessschritte in der Regelverarbeitung dauern. Die Summe über diese Zeitabschnitte ergibt die Vorhaltefrist für die Datenart.

Die Regellöschrfrist für die jeweilige Datenart darf dann nur so viel länger als die Vorhaltefrist gewählt werden, wie dies nach den einschlägigen Rechtsvorschriften verhältnismäßig und zulässig ist.

Es ist sinnvoll, solche Löschrfristen in den Katalog der Standardlöschrfristen aufzunehmen, wenn der Katalog dadurch nicht zu sehr differenziert wird.

### 7.2.4 Ableitung von Löschrfristen nach einfachen Kriterien

Die Abstufung der Standardlöschrfristen, die durch Rechtsvorgaben oder durch die Prozessanalyse gefunden wurden, kann große Abstände aufweisen. Dies kann dazu führen, dass bei der Zuordnung von Datenarten gemäß Kapitel 8.3 die Vorhaltefrist für mehrere Datenarten so weit überschritten werden, dass dies datenschutzrechtlich nicht mehr vertretbar ist. Dann sollten weitere Standardlöschrfristen ergänzt werden, um eine feinere Abstufung zu erreichen.

Soweit die Verwendung von pbD nur durch allgemeine Rechtsvorschriften geregelt ist, können Spielräume für die Festlegung von Löschrfristen bestehen. Diese Spielräume können genutzt werden, um die zusätzlichen Standardlöschrfristen festzulegen.

(ANMERKUNG: Eine langfristige Speicherung zu unbestimmten Zwecken (Vorratsdatenspeicherung) kann mit den Spielräumen aber nicht begründet werden und widerspricht dem Prinzip der Datensparsamkeit. Auch die frei gewählten Standardlöschrfristen müssen so festgelegt werden, dass für die zugeordneten Datenarten der Grundsatz der Erforderlichkeit auf datenschutzrechtlich vertretbare Weise eingehalten wird.)

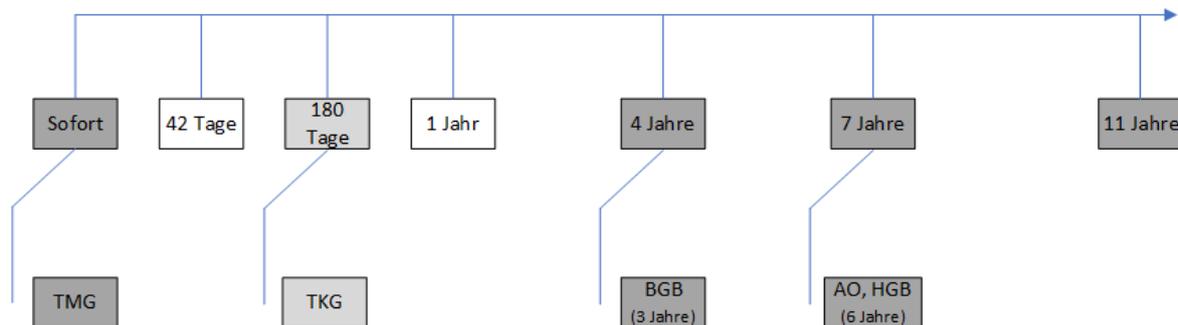
In der allgemeinen Ableitung werden zunächst Fristen bevorzugt, die sich aus Rechtsregeln ergeben, z.B. durch Aufbewahrungspflichten. Diese Fristen sollten so gewählt werden, dass die bestehenden Abstände sinnvoll unterteilt werden.

Sofern weitere Abstände zu groß sind, können diese durch frei gewählte Standardlöschrfristen unterteilt werden (vgl. auch Abb. 3).

Durch die Löschrfristen nach einfachen Kriterien kann der Fristkatalog so ergänzt werden, dass die Abstufung der Standardlöschrfristen datenschutzrechtlich vertretbar ist.

(Anmerkung: Einige Standardlöschrfristen in Abbildung 3 sind aus deutschen Gesetzen abgeleitet. Die Frist ‚Sofort‘ ergibt sich aus § 13 Abs. 4 Nr.2 TMG für Daten über den Ablauf des Zugriffs aus einem Telemediendienst. Die 4- und die 7-Jahresfrist ergeben sich, weil die Verjährungsfrist nach dem Bürgerlichen Gesetzbuch (§ 195 i.V.m. § 199 BGB: 3 Jahre) bzw. die Aufbewahrungsfrist nach AO/HGB am Ende des jeweiligen des jeweiligen Kalenderjahres beginnt.)

## Beispiel Standardlöschfristen



- Dunkelgraue Füllung: Frist abgeleitet aus allgemeinen Gesetzen.
- Hellgraue Füllung: Frist abgeleitet aus Telekommunikationsgesetz.
- Keine Füllung: Frist freige wählt.

Abbildung 3: Beispiel Standardlöschfristen

## 7.3 Besonderheiten für Fristfestlegungen

### 7.3.1 Regellöschfristen und Abweichungen

In der betrieblichen Praxis ist es kaum möglich, mit sehr starren Fristzuordnungen alle Sondersituationen in den Verarbeitungsprozessen abzudecken. Der Ausweg, für alle Datenarten sehr lange Löschkfristen festzulegen, ist datenschutzrechtlich jedoch nicht vertretbar.

Im Folgenden werden daher Verfahrensweisen beschrieben, mit denen ein Löschkonzept die notwendige Flexibilität erhält, um einerseits kurze Regellöschfristen zu definieren, andererseits aber auch für Sondersituationen tragfähige Vorgehensweisen anzubieten.

### 7.3.2 Friständerungen durch Verdichtung mit Wechsel der Datenart

Im Rahmen der Verarbeitungsprozesse kann ein Ausgangsdatenbestand durch statistische Auswertungen oder andere Verdichtungen in einen Ergebnisdatenbestand überführt werden. Der Ergebnisdatenbestand kann möglicherweise einer anderen Datenart zugeordnet werden, beispielsweise weil er einem anderen Zweck dient und weniger sensitiv ist. Für die andere Datenart gilt dann möglicherweise auch eine andere Löschregel mit längerer Frist oder späterem Startzeitpunkt.

### 7.3.3 Wechsel der Datenart für Sonderfälle

In manchen Geschäftsprozessen wird der überwiegende Anteil der Datenarten im Regelprozess verarbeitet. In einzelnen Fällen werden Daten aber länger benötigt als nach der Regellöschfrist vorgesehen, z. B. weil ein Reklamationsfall oder ein Rechtsstreit anhängig ist. Für diese Sonderfälle bietet es sich an, die betroffenen Daten einer anderen Datenart mit entsprechend längerer Löschkfrist zuzuordnen, wenn dies nach den einschlägigen Rechtsvorschriften zulässig ist. Technisch kann dies beispielsweise abgebildet werden, indem die Datenobjekte entsprechend gekennzeichnet oder an anderer Stelle gespeichert werden.

(BEISPIEL: Die Datenart für Daten, die zur Bearbeitung einer Reklamation benötigt werden, könnte „Reklamationsdaten“ heißen. Die Löschrregel dafür könnte lauten: „Ein Jahr nach dem Ende der Garantiedauer“. Die Daten, die für einen Rechtsstreit benötigt werden, könnten in die Datenart Streitfalldaten eingeordnet werden. Die Löschrregel könnte ebenfalls eine Frist von einem Jahr vorsehen und als Startzeitpunkt auf die Rechtskraft des Urteils abstellen.)

Auch bei Änderung des Verwendungszwecks von pbD, soweit diese Änderung nach den einschlägigen Rechtsvorschrift zulässig ist, kann gegebenenfalls die Löschrregel durch einen Wechsel der Datenart angepasst werden.

#### 7.3.4 Ausnahmen von Regelprozessen: Aussetzung der Löschung

In besonderen Situationen kann es notwendig sein, Ausnahmen von Fristregeln zu treffen. Zu diesen Situationen gehören z. B. Fehler in Programmen oder fehlerhafte Datenbestände.

Soweit die einschlägigen Rechtsvorschriften dies zulassen, kann für solche Sondersituationen die Regellöschung von Datenbeständen ausgesetzt werden. Durch allgemeine Regelungen kann für den betroffenen Datenbestand eine Verlängerung der Löschrfrist zugelassen werden.

(BEISPIEL: Eine Regelung zur Fehlerbehandlung könnte lauten: „Da ein Release-Zyklus für die Anpassung von IT-Systemen in der Regel 6 Monate dauert, kann die Löschrfrist für fehlerhafte Datenbestände grundsätzlich um 12 Monate verlängert werden. Dadurch besteht ausreichend Spielraum, um den Fehler zu analysieren und Maßnahmen zu seiner Beseitigung zu ergreifen.“)

Über geeignete Prozesse muss sichergestellt werden, dass die Aussetzung der Löschung begrenzt wird, der betroffene Datenbestand möglichst klein und der Zeitraum der Aussetzung verhältnismäßig ist. Als Kriterien für die Ausgestaltung der Aussetzung heranzuziehen sind beispielsweise die Sensitivität der Daten und die Maßnahmen zur Zweckbindung der Daten während der Ausnahme. Für die Rückkehr zum Regelbetrieb müssen alle Daten der Ausnahmeregelung gelöscht werden. Die Rückbaumaßnahmen sollen überwacht und bei Bedarf überprüft werden.

#### 7.3.5 Abweichungen von Standardlöschrfristen für Sicherungskopien

In Sicherungskopien mit pbD sind regelmäßig Daten enthalten, die bald gelöscht werden müssen. Für eine Wiederherstellung nach einem potentiellen Störfall müssen die Sicherungskopien aber eine gewisse Zeit vorgehalten gehalten werden. Dadurch wird die Löschrfrist für Teile der Daten überschritten.

Ein sinnvolles Sicherungs- und Wiederherstellungs-Konzept kann daher nur umgesetzt werden, wenn für die Datenbestände in Sicherungskopien akzeptiert wird, dass die Regellöschfristen überschritten werden. Durch spezifische Vorhaltefristen für Sicherungskopien dürfen die Löschrfristen der Datenarten, die in der Sicherungskopie enthalten sind, aber nur um ein datenschutzrechtlich vertretbares Maß überschritten werden. Die Löschrfrist der Sicherungskopie muss sich an der kürzesten Löschrfrist der jeweils enthaltenen Datenarten orientieren.

BEISPIELE So könnte eine kurze Löschrfrist von wenigen Wochen für Sicherungskopien von Datenarten mit kurzer Löschrfrist und eine Löschrfrist von 3 Monaten für Sicherungskopien von Datenarten mit langer Löschrfrist festgelegt werden. Um die Komplexität zu begrenzen, sollten nur wenige spezifische Löschrregeln für die Sicherungskopien festgelegt werden.

Gegebenenfalls müssen die Sicherungs-Strategien und die Maßnahmen zum Wiederanlauf so angepasst werden, dass sie mit den datenschutzrechtlich vertretbaren Löschrfristen für die Sicherungskopien auskommen. Dazu kann auch gehören, dass Datenbestände mit unterschiedlichen

Löschfristen in unterschiedliche Sicherungsbestände aufgenommen werden. Diese Sicherungsbestände können dann jeweils nach unterschiedlichen Fristen gelöscht werden.

Durch ein Recovery werden Daten in Systeme zurückgespielt, deren Löschfrist bereits überschritten sein kann. Die Umsetzungsmaßnahmen müssen dies berücksichtigen. Z. B. können automatische Löschrmechanismen alle löschfähigen Daten behandeln. Alternativ können in Wiederanlauf-Plänen auch geeignete einmalige Maßnahmen zur Bereinigung der löschfähigen Daten festgelegt werden.

Für die pbD in Sicherungskopien muss durch geeignete Maßnahmen gewährleistet werden, dass sie nur für Zwecke der Systemwiederherstellung verwendet werden.

## 8 Löschklassen

### 8.1 Abstrakte Startzeitpunkte – abstrakte Löschrregeln.

Eine Löschrregel besteht aus einer Löschfrist und einem Startzeitpunkt, ab dem der Lauf der Frist beginnt.

Der Startzeitpunkt stellt auf eine Bedingung ab, die im Lebenszyklus der jeweiligen Datenart auftritt. Die konkreten Bedingungen können danach unterschieden werden, ob sie auf den Erhebungszeitpunkt der Daten oder eine Bedingung während des Lebenszyklus abstellen. Damit ergeben sich zwei abstrakte Startzeitpunkte:

- **Erhebung der pbD:** Die Löschfrist für ein konkretes Datenobjekt beginnt bereits bei der Erhebung durch die verantwortliche Stelle.
- **Ende eines Vorgangs:** Die Löschfrist für ein konkretes Datenobjekt beginnt erst mit dem Abschluss eines Vorgangs im Lebenszyklus des Objekts.

Das „Ende der Beziehung zum Betroffenen“ ist ein Sonderfall des zweiten Typs. Da mit dem Ende der Beziehung zum Betroffenen die Löschfrist in der Regel mehrerer Datenarten gleichzeitig beginnt, sollte dieses Ereignis als dritter abstrakter Startzeitpunkt definiert werden:

- **Ende der Beziehung zum Betroffenen:** Die Löschfrist für eine konkretes Datenobjekt beginnt mit einem Ereignis, das als Ende der Beziehung zum Betroffenen definiert wird.

(ANMERKUNG 1: Unter Betroffenen sind auch andere Schutzsubjekte datenschutzrechtlicher Rechtsvorschriften eingeschlossen. Beispielsweise werden in Deutschland im Bereich des Postdatenschutzes oder der Mauterhebung auch juristische Personen erfasst. In diesem Fall wäre das Ende der Beziehung zum jeweiligen Schutzsubjekt der entsprechende Startzeitpunkt für die Löschfrist. Wegen der allgemeinen Ausrichtung des Datenschutzes auf natürliche Personen und um sprachlich klar zu den Datenobjekten zu unterscheiden, wird im Dokument nur die Bezeichnung „Betroffener“ verwendet.)

(ANMERKUNG 2: Häufig verwendet eine verantwortliche Stelle Daten unterschiedlicher Kategorien von Betroffenen, z. B. Mitarbeitern, Kunden und Ansprechpartnern bei Vertragspartnern. Für jede Kategorie kann das „Ende der Beziehung zum Betroffenen“ auf eine andere Bedingung abstellen.)

Eine Löschrregel, die nur auf einen abstrakten Startzeitpunkt abstellt, wird ‚abstrakte Löschrregel‘ genannt.

## 8.2 Matrix der Löschklassen

Mit den Standardlöschfristen und den abstrakten Startzeitpunkten können abstrakte Löschklassen gebildet werden. Jede Kombination bildet eine sogenannte Löschklassen. Da es drei abstrakte Startzeitpunkte gibt, können je Standardlöschfrist drei Löschklassen entstehen.

Es bietet sich an, die Löschklassen in einer Matrix darzustellen. In der Praxis zeigt sich, dass oft nicht alle Löschklassen benötigt werden, weil nicht zu jeder Frist jeder abstrakte Startzeitpunkt benötigt wird (vgl. Tabelle 1 „Beispiel für Matrix der Löschklassen“)

In der Matrix der Löschklassen können Positionen frei bleiben, wenn dies nach den einschlägigen Rechtsvorschriften und den fachlichen Anforderungen gerechtfertigt ist. Dadurch reduziert sich die Komplexität des Löschkonzepts weiter.

		Standardfristen						
		Sofort	42 Tage	180 Tage	1 Jahr	4 Jahre	7 Jahre	11 Jahre
Startzeitpunkte	Ab Erhebung			Verbindungsdaten	Verbindungsdaten mit bes. Analysebedarf			
	Ab Ende Vorgang	Web-Logs	Kurzzeit-Doku, Betriebslogs	Einzelverbindungs-nachweise	Vorgänge ohne Dokumentationspflicht	Reklamationen, Forderungen	Handelsbriefe	Buchhaltungsdaten
	Ab Ende Beziehung				Ergänzende Stammdaten		Verträge	Kern-Stammdaten

Tabelle 2: Beispiel Matrix Löschklassen

- Dunkelgraue Füllung: Frist abgeleitet aus allgemeinen Gesetzen.
- Hellgraue Füllung: Frist abgeleitet aus Telekommunikationsgesetz.
- Keine Füllung: Frist frei gewählt.

## 8.3 Zuordnung von Datenarten zu Löschklassen und Löschklassen

Die Datenarten der verantwortlichen Stelle werden den Löschklassen zugeordnet. Jede Datenart mit einer Vorhaltefrist, die nicht einer der Standardlöschfristen entspricht, wird – wenn datenschutzrechtlich zulässig – in eine Löschklassen mit der nächst größeren Standardlöschfrist eingeordnet (Kapitel 7.1). Ist dies nicht möglich, muss geprüft werden, ob eine weitere Standardlöschfrist benötigt wird oder ob für die Datenart eine spezifische eigene Löschklassen festgelegt wird.

(ANMERKUNG 1: Zur Bewertung des Zeitraums zwischen dem Ende der Vorhaltefrist und dem Ende der Regellöschklassen sind die Prinzipien der Erforderlichkeit und der Datensparsamkeit heranzuziehen. Für die Praktikabilität des Löschkonzepts und die Gestaltung der Löschklassenprozesse können daher zwar rechtliche Spielräume genutzt werden. Diese erlauben es aber nicht, die Löschklassen beliebig lange hinauszuzögern.)

(ANMERKUNG 2: Die Frist, während der eine Datenart nach der Vorhaltefrist noch gespeichert wird, muss verhältnismäßig und datenschutzrechtlich vertretbar sein. So dürfte es nur in wenigen Fällen begründbar sein, dass die Regellöschfrist das Doppelte der Vorhaltefrist beträgt.)

Durch die Einordnung einer Datenart in eine Löschkategorie ist die abstrakte Löschrregel bestimmt. Um daraus eine konkrete Löschrregel für die Umsetzung zu bilden, muss festgelegt werden, durch welches konkrete Ereignis der Startzeitpunkt gebildet wird.

(BEISPIEL: Für einen Reparaturauftrag könnte der Startzeitpunkt die „Übergabe des reparierten Gerätes an den Kunden“ sein. Für Buchungsdatensätze und die zugehörigen buchungsbelegenden Unterlagen könnte der Startzeitpunkt die „Fertigstellung der Bilanz“ sein, in der die Buchungen berücksichtigt wurden. Für die Stammdaten eines Mitglieds in einem sozialen Netzwerk könnte der Startzeitpunkt sein „Link der Bestätigungs-Mail nach Deregistrierung wurde geklickt“).

(ANMERKUNG: Der Startzeitpunkt muss in Übereinstimmung mit den einschlägigen Rechtsvorschriften gewählt werden, damit durch ihn die Löschung nicht unnötig hinausgezögert wird.)

Die Standardlöschfristen, Löschklassen und die Zuordnung der Datenarten sollen im eigenständigen Dokument „Löschregeln“ festgelegt werden (Kapitel 11.1). Die Löschrregeln sollen technikneutral definiert werden. Es sollten in diesem Dokument auch Gründe für die Fristdefinitionen und die Zuordnung von Datenarten zu Löschklassen festzuhalten. Dadurch werden bisherige Entscheidungen nachvollziehbar und künftige Entscheidungen erleichtert.

## 9 Löschrregeln

### 9.1 Struktur und Inhalte der Umsetzungsvorgaben

#### 9.1.1 Verhältnis zwischen Dokument ‚Löschregeln‘ und Umsetzungsvorgaben für Löschrregeln

Das Dokument ‚Löschregeln‘ ist hinsichtlich der Löschrregeln die Referenz für die Dokumente mit Umsetzungsvorgaben zur Löschung von pbD.

Die Löschrregeln müssen in IT-Systemen und anderen Prozessen umgesetzt werden. Dazu soll die verantwortliche Stelle in ihrem Löschkonzept regeln, wo und wie Umsetzungsvorgaben festgelegt werden. Dabei kann unterschieden werden nach

- Umsetzungsvorgaben für Querschnittsbereiche. Durch solche allgemeinen Regelungen kann die Zahl der spezifischen Umsetzungsvorgaben für IT-System verringert werden.
- spezifischen Umsetzungsvorgaben für einzelne IT-Systeme.
- Einzelmaßnahmen zur Bereinigung von Datenbeständen.
- Umsetzungsvorgaben für Auftragnehmer.

(vgl. Abbildung 4: Beispiel Dokumentenstruktur)

Die Gesamtheit der Umsetzungsvorgaben soll alle Bestände an pbD von GA Musterstadt Stelle abdecken.

Die Umsetzungsvorgaben sollen als ‚Technische Anweisungen‘ in die Dokumentationsstruktur von GA Musterstadt eingeordnet werden.

In den weiteren Abschnitten dieses Kapitels werden Hinweise dazu und zur Verantwortung für die Pflege und die Freigabe der Umsetzungsvorgaben gegeben.

## Beispiel Dokumentenstruktur

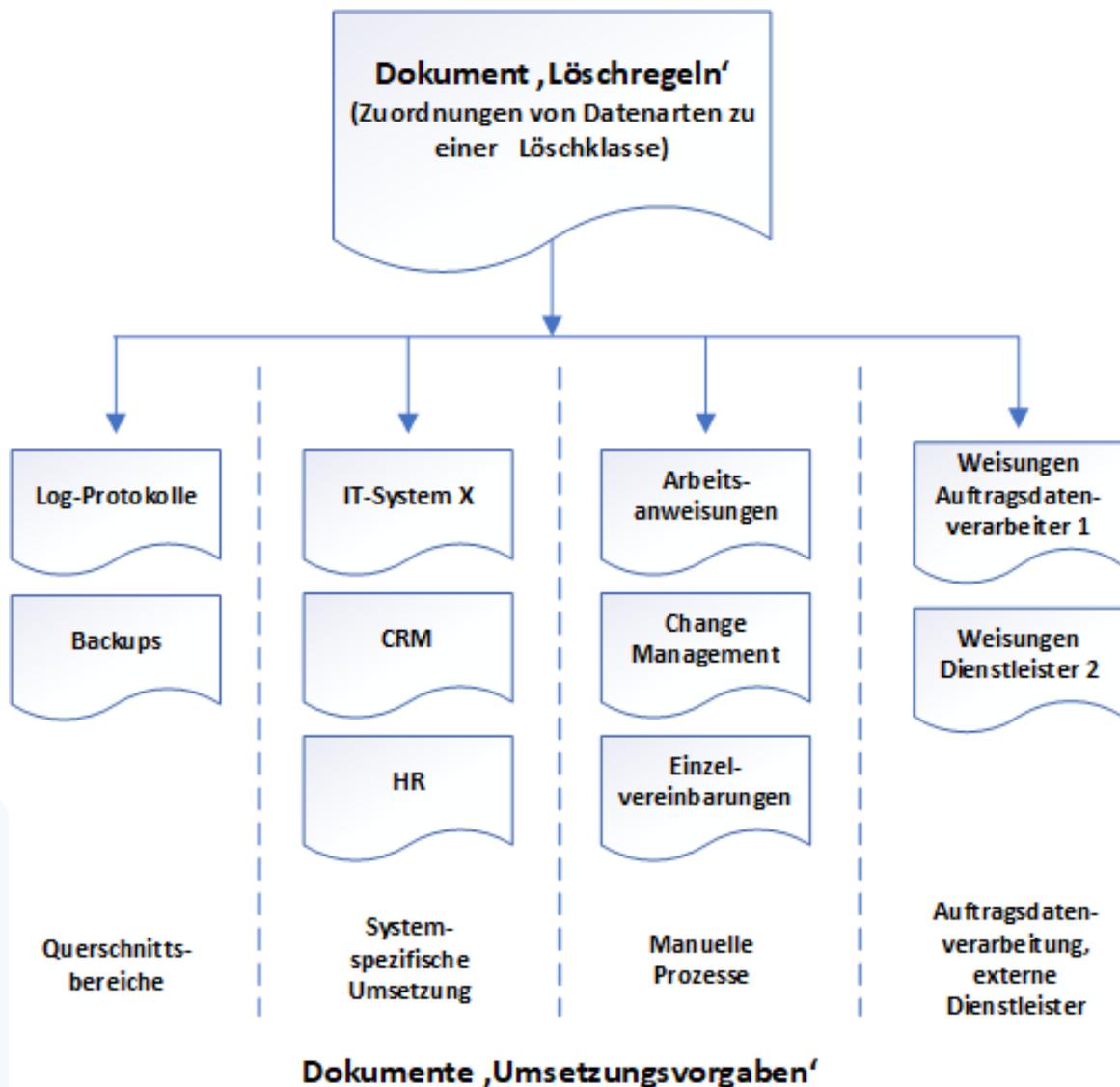


Abbildung 4: Beispiel Dokumentenstruktur

### 9.1.2 Inhalt von Umsetzungsvorgaben

Jede der Umsetzungsvorgaben sollte die folgenden Fragen beantworten:

- Für welche konkreten IT-Systeme oder anderen Datenbestände gilt die Umsetzungsvorgabe?
- Welche Datenarten werden im Regelungsbereich der Umsetzungsvorgabe verwendet?
- Für jede der Datenarten: welche Löschrregel ist anzuwenden? Welche technischen Bedingungen bilden den Auslöser der Frist?
- Durch welchen Mechanismus wird die Löschung durchgeführt?
- Soweit Löschrmechanismen 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?
- Wie ist die Durchführung von Löschrmaßnahmen zu dokumentieren?

Aus diesen Angaben lassen sich auf einfache Weise Audit-Pläne für die Löschrvorgaben erstellen.

Es ist häufig nicht notwendig, die Vorhaltefrist der einzelnen Datenarten in jedem IT-System auszunutzen. Deshalb können in den Umsetzungsvorgaben dann gegebenenfalls kürzere Löschrfristen definiert werden, als nach den Regellöschrfristen der jeweiligen Datenarten zulässig. Dadurch wird dem datenschutzrechtlichen Prinzip der Datensparsamkeit Rechnung getragen. Die Entscheidung über kürzere Fristen muss fachliche und betriebliche Anforderungen berücksichtigen.

## 9.2 Umsetzungsvorgaben für Querschnittsbereiche

Löschrmaßnahmen müssen in Querschnittsbereichen umgesetzt werden. Oft können die Vorgaben einheitlich geregelt werden. Insbesondere für die folgenden Querschnittsbereiche können einheitliche Regeln naheliegen.

**Querschnittsbereich „Backup“:** Für Sicherungskopien muss nach den enthaltenen Datenarten geregelt werden, wann sie zu löschen sind. Gegebenenfalls ist festzulegen, wie Datenbestände auf Sicherungskopien aufzuteilen sind, damit datenschutzrechtlich vertretbare Löschrfristen umgesetzt werden können. Sicherungskopien können neben der Produktionsumgebung auch für weitere Umgebungen erstellt werden, z. B. Testumgebungen oder Entwicklungsumgebungen. Wenn in diesen Sicherungskopien ebenfalls pbD enthalten sein können, müssen die Umsetzungsvorgaben auch für diese Umgebungen gelten.

**Querschnittsbereich „Protokolle“:** Soweit in Protokollen pbD enthalten sind, sind sie Datenarten zuzuordnen. Wenn vielfach ähnliche Inhalte protokolliert werden, kann die Löschung über eine Vorgabe für den Querschnittsbereich geregelt werden. Gegebenenfalls können auch eigene Datenarten für verschiedene Typen von Protokollen oder Log-Einträgen definiert werden. Falls in Protokollen Datenobjekte anderer Datenarten enthalten sind, ist zu beachten, dass diese Datenobjekte in Protokollen nicht später gelöscht werden dürfen, als die originären Datenobjekte.

**Querschnittsbereich „Transportsysteme“:** Manche Systeme nehmen nur Transportaufgaben war, z.B. Kommunikations-Server oder Middleware-Komponenten in service-orientierten Architekturen. Die Daten werden nach erfolgreicher Übertragung möglicherweise noch kurze Zeit für Prüf- oder Recovery-Zwecke vorgehalten, im Regelbetrieb aber spätestens nach wenigen Tagen gelöscht. Soweit keine Datenarten übertragen werden, deren Löschrfristen kürzer sind als die übliche Speicherdauer in den Transportsystemen, kann für die Gruppe von Systemen eine einheitliche Vorgabe für die Umsetzung getroffen werden. In dieser Vorgabe ist auch zu regeln, wie ein kontinuierliches Monitoring der

Transportfunktionen gewährleistet wird. Dies stellt sicher, dass Störungen zeitnah erkannt und behoben werden. Dadurch werden auch Verzögerungen der Löschung von Datenströmen vermieden.

**Querschnittsbereich „Rückbau von Systemen“:** Solange Datenträger noch pbD enthalten können, dürfen sie nicht wiederverwendet oder entsorgt werden. Um das Missbrauchsrisiko möglichst gering zu halten, müssen die enthaltenen Datenbestände daher möglichst bald nach dem Rückbau des Systems gelöscht werden. Die entsprechenden Vorgaben können einheitlich für den Querschnittsbereich getroffen werden. Solche Richtlinien können schon aus anderen Gründen bestehen, z. B. um eine Vertraulichkeitsklassifikation umzusetzen. Dann können die Aspekte des Löschkonzepts dort eingearbeitet werden.

Die Umsetzungsvorgaben für Querschnittsbereiche sollen als ‚Technische Anweisungen‘ in die Dokumentationsstruktur von GA Musterstadt eingeordnet werden (Kapitel 11.2 und 11.3).

Es soll weiterhin dokumentiert werden, welche Datenträger durch Löschen freigegeben und welche vernichtet wurden. Ergänzend zu den Umsetzungsvorgaben im Querschnittsbereich „Rückbau von Systemen“ ist es dazu notwendig, ein „Bestandsverzeichnis der Datenträger“ zu führen und die Dokumentation der Löschung oder Vernichtung vorzusehen.

### 9.3 Umsetzungsvorgaben für einzelne IT-Systeme

Für IT-Systeme oder Datenbestände, die nicht durch die Umsetzungsvorgaben für Querschnittsbereiche abgedeckt werden, müssen spezielle Umsetzungsvorgaben erstellt werden.

Die Umsetzungsvorgaben für einzelne IT-Systeme beschreiben, welche Löschrmechanismen mit welcher Konfiguration sicherstellen, dass im konkreten System die Bestände mit pbD gelöscht werden. Sie beschreiben die Soll-Vorgabe für das jeweilige System. Die Umsetzungsvorgaben für die einzelnen IT-Systeme bilden damit die Grundlage für die betriebliche Konfiguration und Steuerung sowie das Monitoring einzelner IT-Systeme.

Es ist sinnvoll, in den Umsetzungsvorgaben für einzelne Systeme die konkreten Verwendungszwecke der einzelnen gespeicherten Datenbestände und die Abhängigkeiten zu anderen Systemen anzugeben. Dadurch kann schnell entschieden und nachvollzogen werden, ob im jeweiligen System die Löschrfrist für eine Datenart gegenüber der Regellöschrfrist verkürzt werden kann (Prinzip der Datensparsamkeit, Kosteneinsparungen).

[ANMERKUNG 1: Oft werden Datenbestände nach dem Ende des eigentlichen Geschäftsprozesses nur noch wegen gesetzlicher Aufbewahrungspflichten vorgehalten. Meist genügt es daher, dass ein System die Daten für diesen Zweck vorhält.)

[ANMERKUNG 2: Falls Datenobjekte an Dritte übertragen werden müssen, beispielsweise ein staatliches Archiv, ist dies als Abhängigkeit vor einer Löschung zu berücksichtigen. Die Umsetzungsvorgabe soll diese Abhängigkeit ausweisen und im Löschrmechanismus berücksichtigen.]

Häufig werden durch einen Löschrmechanismus ganze Datensätze oder Dateien gelöscht. In manchen Fällen sollen aber nur feingranulare Datenobjekte gelöscht werden. Dies ist beispielsweise dann der Fall, wenn Datenbestände anonymisiert werden sollen. In solchen Fällen muss die Umsetzungsvorgabe im Detail festlegen, welche Datenobjekte wie zu behandeln sind.

(BEISPIEL: Um den Personenbezug eines Datensatzes in einer Datenbank aufzulösen, müssen die einzelnen Attribute angegeben werden, deren Werte zu löschen sind. Wenn durch

Aggregation ein Wechsel zu einer Datenart mit längerer Löschfrist erreicht werden soll, muss beispielsweise angegeben werden, welche Attribute aufsummiert oder welche (vielleicht minutengenauen) Zeitangaben auf eine Jahresangabe verallgemeinert werden.)

Die Umsetzungsvorgaben für einzelne IT-Systeme sollen als ‚Technische Anweisung‘ jeweils als eigenständiges Systemlöschkonzept in die Dokumentationsstruktur von GA Musterstadt eingeordnet werden (Kapitel 11.4).

## 9.4 Einzelmaßnahmen zur Löschung von Datenbeständen

### 9.4.1 Allgemeine Hinweise zu Umsetzungsvorgaben für Einzelmaßnahmen

Die Umsetzungsvorgaben für Querschnittsbereiche und für die einzelnen IT-Systeme decken die großen Datenbestände in der automatisierten Regelverarbeitung ab. Neben diesen Datenbeständen müssen aber häufig weitere Bestände an pbD berücksichtigt werden.

Die folgenden Abschnitte beschreiben solche Datenbestände beispielhaft. GA Musterstadt muss gewährleisten, dass die Umsetzungsvorgaben für diese und gegebenenfalls weitere Datenbestände erstellt und umgesetzt werden.

Zu den Einzelmaßnahmen zählen auch manche Sondersituationen, in denen das Löschen nicht von Löschrregeln im Sinne dieser Leitlinie bestimmt werden kann.

Die Umsetzungsvorgaben für Einzelmaßnahmen sollen als ‚Technische Anweisung‘ oder als ‚Arbeitsanweisungen‘ in die Dokumentationsstruktur von GA Musterstadt eingeordnet werden.

### 9.4.2 Umsetzungsvorgaben für Datenobjekte im allgemeinen Bürobetrieb

Für den allgemeinen Bürobetrieb sollen Löschrregeln festgelegt werden, beispielsweise zur Behandlung von Dokumenten abgeschlossener Projekte oder für E-Mails. Diese Umsetzungsvorgaben sollen in eine Arbeitsanweisung für Mitarbeiter integriert werden. Darin soll auch über sichere Entsorgungsmöglichkeiten für Dateien, Papierdokumente und Datenträger informiert werden (Kapitel 11.5).

### 9.4.3 Umsetzungsvorgaben für Datenbestände in manuellen Prozessen

Bestände mit pbD, die in regelmäßigen manuellen Prozessen verwendet werden, müssen ebenfalls innerhalb der Regellöschrfristen gelöscht werden. Beispiel dafür sind Papier-Personalakten.

Solche Umsetzungsvorgaben sollen in spezifischen Arbeitsanweisungen beschrieben werden (Kapitel 11.6).

#### 9.4.4 Umsetzungsvorgaben für Datenabzüge für Sonderverwendungen

In manchen Situationen werden Kopien von Daten aus dem Regelbetrieb (Datenabzüge) für besondere Verwendungen benötigt. Datenabzüge, die außerhalb der Regelprozesse verwendet werden, müssen innerhalb der Frist gelöscht werden, die mit der Datenschutzbeauftragten vereinbart wurde.

Es sollen die entsprechenden Aufgaben für die Löschung von Datenabzügen gemeinsam mit der Datenschutzbeauftragten in spezifischen Arbeitsanweisungen festgelegt werden (Kapitel 11.7).

Für die Nachverfolgung von Ausnahmeregelungen für Umsetzungsvorgaben oder Datenabzüge soll eine Übersicht über diese Fälle geführt werden. Die Rückkehr zum Regelbetrieb oder die Löschung der Datenabzüge wird in dieser Übersicht nach einer entsprechenden Rückmeldung der jeweils verantwortlichen Organisationseinheit dokumentiert (Kapitel 11.8).

#### 9.4.5 Umsetzungsvorgaben für Restbestände in IT-Systemen

Die Umsetzungsvorgaben für Querschnittsbereiche und für die einzelnen IT-Systeme decken die automatisierten Regelverarbeitung ab. Die dort festgelegten Mechanismen erfassen aber möglicherweise nicht alle pbD, die zu löschen sind. Es ist daher sicherzustellen, dass auch Restbestände gelöscht werden. Darunter fallen beispielsweise die folgenden und gegebenenfalls weitere Datenbestände:

- Datenbestände, für die keine Regelprozesse implementiert wurden.
- Datenbestände, die z.B. im Zusammenhang mit Migrationen nicht von Regelprozessen gelöscht werden.
- Datenbestände, die durch Fehler in Löschmechanismen oder nach einem System-Recovery von Regelprozessen nicht gelöscht werden.

Die Verantwortlichen für die IT-Administration von GA Musterstadt sind für die Identifikation und Löschung solcher Datenbestände verantwortlich. Grundsätzlich sollte geklärt sein, dass sie zu löschen sind. Wenn Unsicherheit über die fachliche Verwendung der Restbestände besteht, sollen die anwendenden Organisationseinheiten in einen Review-Prozess eingebunden werden.

Identifizierte Bestände solcher Daten sind in regelmäßigen betrieblichen Prozessen zu löschen. Die Umsetzungsvorgaben, die regelmäßig durchgeführt werden müssen, sollen in spezifischen Arbeitsanweisungen für Administratoren festgelegt werden (Kapitel 11.9).

#### 9.4.6 Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten

Wenn festgestellt wird, dass Bestände mit pbD nach den einschlägigen Rechtsvorschriften durch GA Musterstadt unzulässigerweise gespeichert werden, muss unverzüglich die Datenschutzbeauftragte darüber informiert werden. Die Datenschutzbeauftragte koordiniert eine ordnungsgemäße Durchführung der Löschung solcher Datenbestände und mögliche Löschmaßnahmen dürfen nur nach ausdrücklicher Absprache mit ihr durchgeführt werden.

Die eingesetzten IT-Systeme und Prozesse müssen die Möglichkeit bieten, dass nach einer entsprechenden Vorgabe der Datenschutzbeauftragten die Löschung unverzüglich umgesetzt wird.

Die Umsetzungsvorgabe erfolgt in Form einer betrieblichen Einzelanweisungen (Kapitel 11.10).

## 9.5 Umsetzungsvorgaben für Auftragnehmer

GA Musterstadt muss auch sicherstellen, dass die Regellöschfristen auch für ihre Datenbestände eingehalten werden, die bei Auftragnehmern für eine Auftragsdatenverarbeitung verarbeitet werden.

Die Umsetzungsvorgaben müssen über vertragliche Regelungen und verbindliche Weisungen getroffen werden (siehe auch Kapitel 10.3.4 und 11.11).

# 10 Verantwortung u. Prozesse für das Löschen von personenbezogenen Daten

## 10.1 Allgemeine Einbettung in das Datenschutz-Management-System

Im Löschkonzept von GA Musterstadt muss festgelegt werden, wer für welche Aufgaben verantwortlich ist. Dazu ist es notwendig, die Aufbauorganisation für das Löschen zu definieren. Außerdem muss in der Ablauforganisation geregelt werden, wie die im Rahmen des Löschkonzepts relevanten Prozesse durchzuführen sind.

Die Verantwortung und Prozesse zur Etablierung, Umsetzung, Pflege und Verbesserung des Löschkonzepts sollen in das Management-System für Datenschutz-Aufgaben eingebettet werden. Hierfür ist die Geschäftsführung verantwortlich.

Die folgenden Abschnitte fassen die in den vorangehenden Kapiteln aufgeführten Aufgaben zusammen und ordnen sie nach Verantwortungsbereichen.

## 10.2 Rolle der Datenschutzbeauftragten

### 10.2.1 Pflegeverantwortung für Dokumente

Die folgenden Dokumente sollen durch die Datenschutzbeauftragte erstellt und gepflegt werden:

- **Pflege des Dokuments „Löschkonzept“:** Auslöser für Änderungen sind Entscheidungen der verantwortlichen Stelle, Verantwortung oder Dokumentationsstruktur des Löschkonzepts anzupassen.
- **Pflege des Dokuments „Löschregeln“:** Auslöser für Änderungen sind die Identifikation zusätzlicher Datenarten, Anpassungen von Löschregeln oder Änderungen von einschlägigen Rechtsvorschriften mit Auswirkungen auf Löschregeln. Durch solche Änderungen kann es auch notwendig sein, die Zuordnung von Datenarten zu Löschklassen anzupassen oder geänderte oder zusätzliche Standardfristen zu verwenden.
- **Pflege des Dokuments „Umsetzungsvorgaben für Querschnittsbereiche“:** Auslöser für Änderungen sind Änderungen betrieblicher Anforderungen oder Prozesse.

Für die genannten Dokumente ist der jeweilige Änderungs- und Freigabeprozess zu beachten.

### 10.2.2 Überwachung von Prozessen durch die Datenschutzbeauftragte

Die Datenschutzbeauftragte soll folgende Prozesse überwachen:

- **Löschen von unzulässigen Beständen mit pbD** (Abschnitt 9.4.6): Für den Prozess ist festzulegen, wie die Datenschutzbeauftragte die Löschung unzulässig erhobener oder gespeicherter pbD veranlassen kann. Es sollte festgelegt werden, welche Organisationseinheit die Löschung umsetzen muss und dass sie der Datenschutzbeauftragten über den Vollzug berichtet.
- **Datenschutz-Audit für Löschrmaßnahmen:** Für den Prozess ist festzulegen, wie die Planung und die Durchführung von Datenschutz-Audits erfolgen sollen. Die Datenschutzbeauftragten ist ermächtigt, die jeweils für die Umsetzungsvorgaben verantwortliche Organisationseinheit aufzufordern, ein Audit durchzuführen und über das Ergebnis zu berichten.

### 10.2.3 Freigabe-Beteiligungen

Die Datenschutzbeauftragte soll an der Freigabe der folgenden Dokumente beteiligt sein:

- **Umsetzungsvorgaben für Löschrmaßnahmen** (siehe Kap. 9): Es sollen die Erstellungs- und Pflegeprozesse für die jeweiligen Umsetzungsvorgaben in vorhandene Prozesse eingebettet werden, z. B. Betrieb, Change-Management und Einkauf. Die Prozesse müssen sicherstellen, dass die Datenschutzbeauftragte neuen Dokumenten und relevanten Änderungen zustimmen muss.
- **Anforderungsdokumente für Systembeschaffungen und Systementwicklungsprojekte:** Die Erstellungs- und Pflegeprozesse müssen sicherstellen, dass die Datenschutzbeauftragte prüfen kann,
  - ob pbD im jeweiligen System verwendet und deshalb Löschrmechanismen realisiert werden müssen,
  - ob die in den Anforderungen definierten Löschrmechanismen ausreichend sind und den Löschrregeln entsprechen und
  - ob gegebenenfalls gefordert werden muss, dass Löschrungen im Einzelfall möglich sind (Abschnitt 9.4.6).

Diese Prüfungen sollen in die datenschutzrechtlichen Freigabeprozesse für Systembeschaffungen und Systementwicklungsprozesse integriert werden.

## 10.3 Verantwortung und Prozesse bezüglich Umsetzungsvorgaben

### 10.3.1 Organisationseinheiten mit Verantwortung für Bestände mit pbD

Für jeden Bestand an pbD soll sichergestellt werden, dass eine Organisationseinheit die Verantwortung für die Umsetzung von Löschrmaßnahmen trägt. Zu ihren Aufgaben gehört es,

- Umsetzungsvorgaben der Löschrregeln für den jeweiligen Datenbestand mit der Datenschutzbeauftragten abzustimmen und festzulegen,
- die Durchführung der Umsetzungsvorgaben sicherzustellen, zu überwachen und gegebenenfalls den Erfolg der Maßnahmen zu überprüfen,
- im Falle von Änderungen am Datenbestand oder den Verwendungsprozessen die Umsetzungsvorgaben zu aktualisieren und der Datenschutzbeauftragten in die Freigabe einzubinden.

### 10.3.2 Weitere Aufgaben bezüglich Umsetzungsvorgaben

Das GA Musterstadt muss sicherstellen, dass jeder Bestand mit pbD geeigneten Umsetzungsvorgaben unterliegt. Um die Datenbestände den jeweiligen Verantwortlichen zuordnen zu können, soll die IT-Administration eine Liste der IT-Systeme und anderer Datenbestände anlegen, laufend überprüfen und aktualisieren. Unter andere Datenbestände können z. B. manuell oder bei Auftragnehmern geführte Datenbestände fallen. Diese Liste und die Zuordnung der Verantwortlichen müssen in der aktuellen Fassung der Datenschutzbeauftragten zur Verfügung gestellt werden (Kapitel 11.12).

In manchen Fällen können Löschmaßnahmen nicht sofort realisiert werden, beispielsweise weil eine Fehlerbehebung oder eine Weiterentwicklung eines IT-Systems notwendig ist. Die Geschäftsführung der MUSTERMANN GmbH und die Datenschutzbeauftragte müssen einen Überblick über solche Handlungsbedarfe haben, damit sie diese priorisieren und nachverfolgen können. Die Liste der aktuellen Handlungsbedarfe in den jeweiligen Umsetzungsvorgaben sollen in einem separaten Dokument erfasst werden (Kapitel 11.13).

### 10.3.3 Organisationseinheit Change-Management

Die Veränderungen u.a. im IT-Betrieb und in betrieblichen Abläufen des GA Musterstadt sollen grundsätzlich durch ein Change-Management gesteuert werden.

Die für das Change-Management verantwortliche Organisationseinheit muss sicherstellen, dass die Datenschutzbeauftragte beteiligt wird zur datenschutzrechtlichen Freigabe z.b.

- von Aktivitäten, die zur Aussetzung der Löschung von pbD führen oder
- besondere Aktivitäten, die das Löschen von pbD erfordern.

Letzteres ist beispielsweise der Fall, wenn Kopien von Datenbeständen außerhalb von Regelprozessen verwendet werden sollen.

Die Prozesse des Change-Managements sind entsprechend anzupassen.

### 10.3.4 Organisationseinheiten mit Verantwortung zur Steuerung von Auftragnehmern

Die Verantwortung für die Steuerung von Auftragnehmern des GA Musterstadt muss eindeutig zugewiesen sein.

Die für die Verträge mit Auftragnehmern verantwortlichen Organisationseinheiten müssen sicherstellen, dass neben anderen Pflichten auch die Umsetzung von Löschmaßnahmen vertraglich vereinbart wird.

Die für die Steuerung von Auftragnehmern verantwortlichen Organisationseinheiten müssen weiterhin sicherstellen, dass die vertraglichen Regelungen und weitere Weisungen beim Auftragnehmer auch umgesetzt werden (11.11).

Die Prozesse für Einkauf und Steuerung von Auftragnehmern sind entsprechend anzupassen.

## 11 Referenzierte Dokumente

### 11.1 Anlage 01, Dokument „Löschregeln“

Verantwortung und Freigabe für Dokument „Löschregeln“	
Verantwortung für Erstellung u. Pflege:	Datenschutzbeauftragte
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• die für den Datenschutz verantwortlichen Mitarbeiter,</li> <li>• die Projekt-Teams, die Umsetzungsvorgaben für Systeme entwickeln,</li> <li>• fachliche Anwender, die die Löschregeln von Datenarten prüfen oder als Information benötigen.</li> </ul>

Tabelle 3: Anlage 01, Dokument "Löschregeln"

### 11.2 Anlage 02, Dokument „Umsetzungsvorgaben für Querschnittsbereiche“

Verantwortung und Freigabe für Dokumente „Umsetzungsvorgaben für Querschnittsbereiche“	
Verantwortung für Erstellung u. Pflege:	IT-Administration
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• die für den jeweiligen Querschnittsbereich verantwortlichen Entscheidungsträger,</li> <li>• die Mitarbeiter, die die Technischen Anweisungen umsetzen müssen.</li> </ul>

Tabelle 4: Anlage 02, Dokument „Umsetzungsvorgaben für Querschnittsbereiche“

### 11.3 Anlage 03, Dokument „Bestandsverzeichnis der Datenträger“

<b>Verantwortung und Freigabe für Dokument ‚Bestandsverzeichnis der Datenträger‘</b>	
Verantwortung für Erstellung u. Pflege:	IT-Administration (Verantwortlicher für Rückbau von Systemen)
Voraussetzungen für Freigabe von Änderungen:	Review IT-Administration und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• IT-Administration,</li> <li>• die Mitarbeiter, die den Rückbau von Systemen umsetzen müssen.</li> </ul>

*Tabelle 5:Anlage 03, Dokument „Bestandsverzeichnis der Datenträger“*

### 11.4 Anlage 04, Dokument „Umsetzungsvorgaben für einzelne IT-Systeme“

<b>Verantwortung und Freigabe für Dokumente „Umsetzungsvorgaben für einzelne IT-Systeme“</b>	
Verantwortung für Erstellung u. Pflege:	IT-Administration
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• die IT-Administratoren,</li> <li>• die Anwender, die die Prozesse gestalten, in denen die jeweiligen Datenbestände verwendet werden.</li> </ul>

*Tabelle 6:Anlage 04, Dokument „Umsetzungsvorgaben für einzelne IT-Systeme“*

### 11.5 Anlage 05, Dokument „Arbeitsanweisung Löschrregeln im allgemeinen Bürobetrieb“

<b>Verantwortung und Freigabe für Dokument „Arbeitsanweisung Löschrregeln im allgemeinen Bürobetrieb“</b>	
Verantwortung für Erstellung u. Pflege:	Leitung der betroffenen Organisationseinheit
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• Alle Mitarbeitenden von GA Musterstadt.</li> </ul>

Tabelle 7:Anlage 05, Dokument „Arbeitsanweisung Löschrregeln im allgemeinen Bürobetrieb“

### 11.6 Anlage 06, Dokument „Arbeitsanweisung Datenbestände in manuellen Prozessen“

<b>Verantwortung und Freigabe für Dokument „Arbeitsanweisung Datenbestände in manuellen Prozessen“</b>	
Verantwortung für Erstellung u. Pflege:	Leitung der beteiligten Organisationseinheiten
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• Die Leitung der am manuellen Prozess beteiligten Organisationseinheit,</li> <li>• die jeweils am manuellen Prozess beteiligten Mitarbeiter.</li> </ul>

Tabelle 8:Anlage 06, Dokument „Arbeitsanweisung Datenbestände in manuellen Prozessen“

## 11.7 Anlage 07, Dokument „Arbeitsanweisung für Datenabzüge für Sonderverwendungen“

<b>Verantwortung und Freigabe für Dokument „Arbeitsanweisung für Datenabzüge für Sonderverwendungen“</b>	
Verantwortung für Erstellung u. Pflege:	Leitung der beteiligten Organisationseinheiten gemeinsam mit der Datenschutzbeauftragten
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• Die Leitung der am manuellen Prozess beteiligten Organisationseinheit,</li> <li>• die jeweils an der Sonderverwendung beteiligten Mitarbeiter.</li> </ul>

Tabelle 9: Anlage 07, Dokument „Arbeitsanweisung für Datenabzüge für Sonderverwendungen“

## 11.8 Anlage 08, Dokument „Übersicht über Ausnahmeregelungen“

<b>Verantwortung und Freigabe für Dokument „Übersicht über Ausnahmeregelungen“</b>	
Verantwortung für Erstellung u. Pflege:	Leitung der beteiligten Organisationseinheiten gemeinsam mit der Datenschutzbeauftragten
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• Die Leitung der am manuellen Prozess beteiligten Organisationseinheit,</li> <li>• die jeweils an der Sonderverwendung beteiligten Mitarbeiter.</li> </ul>

Tabelle 10: Anlage 08, Dokument „Übersicht über Ausnahmeregelungen“

### 11.9 Anlage 09, Dokument „Umsetzungsvorgaben für Restbestände in IT-Systemen“

<b>Verantwortung und Freigabe für Dokument „Umsetzungsvorgaben für Restbestände in IT-Systemen“</b>	
Verantwortung für Erstellung u. Pflege:	IT-Administration
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>Mitarbeitende der IT-Administration.</li> </ul>

*Tabelle 11: Anlage 09, Dokument „Umsetzungsvorgaben für Restbestände in IT-Systemen“*

### 11.10 Anlage 10, Dokument „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“

<b>Verantwortung und Freigabe für Dokument „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“</b>	
Verantwortung für Erstellung u. Pflege:	IT-Administration gemeinsam mit der Datenschutzbeauftragten
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>Prozessverantwortliche,</li> <li>die IT-Administration.</li> </ul>

*Tabelle 12: Anlage 10, Dokument „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“*

### 11.11 Anlage 11, Dokument „Umsetzungsvorgaben für Auftragnehmer“

<b>Verantwortung und Freigabe für Dokument „Umsetzungsvorgaben für Auftragnehmer“</b>	
Verantwortung für Erstellung u. Pflege:	die für die Umsetzung beim Auftragnehmer verantwortlichen Mitarbeiter gemeinsam mit der Datenschutzbeauftragten
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>die für die Umsetzung beim Auftragnehmer verantwortlichen Mitarbeiter von GA Musterstadt.</li> </ul>

Tabelle 13: Anlage 11, Dokument „Umsetzungsvorgaben für Auftragnehmer“

### 11.12 Anlage 12, Dokument „Übersicht über IT-Systeme und andere Bestände mit pbD“

<b>Verantwortung und Freigabe für Dokument „Übersicht über IT-Systeme und andere Bestände mit pbD“</b>	
Verantwortung für Erstellung u. Pflege:	IT-Administration
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>Geschäftsleitung und</li> <li>Datenschutzbeauftragte.</li> </ul>

Tabelle 14: Anlage 12, Dokument „Übersicht über IT-Systeme und andere Bestände mit pbD“

### 11.13 Anlage 13, Dokument „Handlungsbedarfe aus Umsetzungsvorgaben“

<b>Verantwortung und Freigabe für Dokument „Handlungsbedarfe aus Umsetzungsvorgaben“</b>
--

Verantwortung für Erstellung u. Pflege:	IT-Administration
Voraussetzungen für Freigabe von Änderungen:	Review durch betroffene Organisationseinheiten und Datenschutzbeauftragte
Freigabe durch:	Geschäftsleitung
Primäre Zielgruppen:	<ul style="list-style-type: none"> <li>• Geschäftsleitung und</li> <li>• Datenschutzbeauftragte.</li> </ul>

*Tabelle 15: Anlage 13, Dokument „Handlungsbedarfe aus Umsetzungsvorgaben“*

## 12 Anhang

### 12.1 Abkürzungen

Abkürzung	Beschreibung
Abs.	Absatz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
DIN	Deutsches Institut für Normung e.V.
DSGVO	Datenschutz-Grundverordnung
HGB	Handelsgesetzbuch
ISO	International Standardization Organisation
pbD	personenbezogene Daten
StGB	Strafgesetzbuch

### 12.2 Abbildungsverzeichnis

Abbildung 1: Beispiel Fristabschnitte im Löschkonzept.....	11
Abbildung 2: Phasen in der Umsetzung des Löschkonzeptes .....	15
Abbildung 3: Beispiel Standardlöschfristen.....	22
Abbildung 4: Beispiel Dokumentenstruktur.....	27

### 12.3 Tabellenverzeichnis

Tabelle 1, Klassifikation der Dokumente des Berechtigungskonzeptes.....	6
Tabelle 2:Beispiel Matrix Löschklassen .....	25
Tabelle 3: Anlage 01, Dokument "Löschregeln" .....	35
Tabelle 4: Anlage 02, Dokument „Umsetzungsvorgaben für Querschnittsbereiche“ .....	35
Tabelle 5:Anlage 03, Dokument „Bestandsverzeichnis der Datenträger“.....	36
Tabelle 6:Anlage 04, Dokument „Umsetzungsvorgaben für einzelne IT-Systeme“ .....	36
Tabelle 7:Anlage 05, Dokument „Arbeitsanweisung Löschregeln im allgemeinen Bürobetrieb“ .....	37
Tabelle 8:Anlage 06, Dokument „Arbeitsanweisung Datenbestände in manuellen Prozessen“ .....	37
Tabelle 9: Anlage 07, Dokument „Arbeitsanweisung für Datenabzüge für Sonderverwendungen“.....	38
Tabelle 10: Anlage 08, Dokument „Übersicht über Ausnahmeregelungen“.....	38
Tabelle 11: Anlage 09, Dokument „Umsetzungsvorgaben für Restbestände in IT-Systemen“ .....	39
Tabelle 12: Anlage 10, Dokument „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“ .....	39
Tabelle 13: Anlage 11, Dokument „Umsetzungsvorgaben für Auftragnehmer“.....	40
Tabelle 14: Anlage 12, Dokument „Übersicht über IT-Systeme und andere Bestände mit pbD“.....	40

Tabelle 15: Anlage 13, Dokument „Handlungsbedarfe aus Umsetzungsvorgaben“ ..... 41

## 12.4 Quellenverzeichnis

Abkürzung	Titel	Herausgeber/Verlag	Jahr
LKo	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten	Hammer, V., Schuler, K.	2012
	Download bei Secorvo Security Consulting GmbH ( <a href="https://www.secorvo.de/publikationen/fachartikel.html">https://www.secorvo.de/publikationen/fachartikel.html</a> )		

## 12.5 Regelverzeichnis

Bezeichnung	Regel/Norm/Standard/Richtlinie	Jahr
Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten	DIN 66398	2016

## 13 Änderungshistorie

Version	Datum	Beschreibung
14_SORMAS-X_Löschkonzept_V1-0_220329.docx	29.03.2022	Initialfassung

### 13.1 Änderungen von der vorherigen Version zur aktuellen Version

Das vorliegende Dokument ist die Initialversion. Es wurde lediglich die Nomenklatur angepasst, inhaltliche Änderungen wurden nicht vorgenommen, deswegen gibt es noch keine Änderungsangaben.