# DIN
# Deutsches Institut für Normung e.V.

# "Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten"

Version 1.0.3
Stand 26. Oktober 2015

Dr. Volker Hammer, Karin Schuler

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

INNOVATION MIT NORMEN UND STANDARDS

# Inhaltsübersicht

## Historie

| Version | Datum | Änderung | Autor |
|---|---|---|---|
| 0.2 | 14.05.2012 | initiale Fassung zur Diskussion mit dem DIN | V. Hammer |
| 0.3 | 07.08.2012 | Strukturentwurf auf der Basis von Kickoff-Workshop und Vorarbeiten des Löschkonzepts von Toll Collect | V. Hammer |
| 0.4 | 10.08.2012 | Inhaltliche und strukturelle Anpassungen nach Diskussion im Projekt-Team | V. Hammer |
| 0.9 | 08.10.2012 | Textentwurf für den Review-Workshop | V. Hammer, K. Schuler |
| 1.0 | 10.12.2012 | Anmerkungen der Teilnehmer des Review-Workshops und Hr. Cebulla eingearbeitet<br>Zahlreiche redaktionelle Überarbeitungen<br>Hinweise für die Weiterarbeit an einem internationalen Standard ergänzt | V. Hammer, K. Schuler |
| bis 1.0.3 | 23.10.2015 | redaktionelle Korrekturen<br>Hinweis auf DIN 66398 ergänzt | V. Hammer |

# Vorwort

Dieses Dokument ist das Ergebnis des Projekts „Datenschutzkonformes Löschkonzept – Standardisierungsmöglichkeiten für einen Best-Practice-Ansatz“. Das Projekt wurde im Rahmen des Programms „Innovation mit Normen und Standards“ vom Bundesministerium für Wirtschaft und Technologie gefördert. Projektträger war das DIN – Deutsches Institut für Normung e.V. Ziel des Projekts war es, die Möglichkeit einer internationalen Standardisierung einer Leitlinie zur Etablierung eines betrieblichen Löschkonzepts zu prüfen.

Wir bedanken uns für die inhaltlichen Diskussionen und Beiträge bei den Teilnehmern des Kickoff-Workshops und des Review-Workshops. Besonderer Dank gebührt Herrn Fraenkel, dem betrieblichen Datenschutzbeauftragten der Toll Collect GmbH, für die Unterstützung des Projekts. Bei der Toll Collect GmbH bedanken wir uns für den sehr offenen Umgang mit den Informationen zum Löschkonzept der Toll Collect und der Unterstützung bei der Durchführung der Workshops.

*Karlsruhe im Dezember 2012*
*Volker Hammer und Karin Schuler*

**Hinweis:**

Die Leitlinie Löschkonzept wurde im Rahmen eines Normungsprojekts mit Unterstützung der Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect zur DIN 66398 weiterentwickelt und vom zuständigen Arbeitskreis im DIN im September 2015 verabschiedet. Die Norm wird im Beuth-Verlag veröffentlicht.

# 1 Einleitung

1. In sehr vielen Geschäftsprozessen und IT-Anwendungen werden personenbezogene Daten (pbD) verwendet. Sie unterliegen daher den Rechtsvorgaben des Datenschutzes. Diese fordern unter anderem, die Prinzipien der Erforderlichkeit, Datenvermeidung und Datensparsamkeit im Umgang mit pbD zu beachten, die auch eine Löschung derartiger Daten erfordern. So enthält Artikel 6 der EU-Datenschutzrichtlinie von 1995 eine Lösch- und Anonymisierungsvorgabe. Sie war in allen nationalen Datenschutzgesetzen der EU-Länder umzusetzen. Wenn datenschutzrechtliche Regelungen auf einem Verbot mit Erlaubnisvorbehalt beruhen, endet die Erforderlichkeit der Verarbeitung, wenn die Verwendung der Daten für die zulässigen Zwecke abgeschlossen wurde. Beispielsweise konkretisiert das deutsche Bundesdatenschutzgesetz in den §§ 20 Abs. 2 und 35 Abs. 2 die Forderung nach Löschung für diejenigen Daten, die für die rechtlich zulässigen Zwecke nicht mehr erforderlich sind. Die Prinzipien wurden in [ISO 29100] als „*Data minimization*“ und „*Use, retention and disclosure limitation*“ aufgegriffen.

2. In der Praxis wird die Rechtsvorgabe der Löschung allerdings nur in geringem Maß umgesetzt. Sie stößt auf vielfältige Probleme, insbesondere weil

   - unbestimmte Rechtsbegriffe ausgelegt werden müssen,
   - es verantwortlichen Stellen schwerfällt, für Datenbestände das Ende von Prozessen und damit konkrete Löschfristen festzulegen,
   - viele Beteiligte gegebenenfalls differenzierte Löschregeln verstehen müssen, um die Löschmechanismen konsequent in relevanten IT-Systemen und anderen Abläufen zu implementieren und
   - es an klaren Vorstellungen fehlt, wie die korrekte Umsetzung der Löschregeln überprüft und gegebenenfalls nachgewiesen werden kann.

3. Um eine rechtskonforme, geordnete Löschung von pbD sicherzustellen, müssen verantwortliche Stellen daher ein Regelwerk entwickeln und Verantwortung zuweisen. Die Etablierung eines solchen Löschkonzepts ist eine komplexe und umfangreiche Aufgabe. Die Erfolgsaussichten für die Entwicklung eines konkreten Löschkonzepts können verbessert werden, wenn die verantwortliche Stelle auf einen bewährten Vorschlag zur Vorgehensweise und zur Gestaltung zurückgreifen kann.

4. In dieser Leitlinie wird eine Vorgehensweisen für die Etablierung eines betrieblichen Löschkonzepts vorgeschlagen. Die Vorgehensweise geht von der Annahme aus, dass ein tragfähiger Kompromiss zwischen den Vorgaben der Rechtsnormen und der Praktikabilität von Löschprozessen gefunden werden muss.

5. Dieses Dokument dient auch dazu, die Möglichkeit einer internationalen Standardisierung der Leitlinie zu prüfen.

6. Für diesen Text wird angenommen, dass beim Leser Datenschutzkenntnisse vorhanden sind. Andernfalls wären an vielen Stellen Erläuterungen notwendig, die den Rahmen dieser Untersuchung überschreiten würden.

### Ziele der Leitlinie

7. Die Leitlinie unterstützt verantwortliche Stellen dabei, ihre rechtlichen Pflichten zur Löschung personenbezogener Daten zu erfüllen. Sie gibt Empfehlungen für die Inhalte, den Aufbau

und die Zuordnung von Verantwortung in einem Löschkonzept für pbD. Die Vorgehensweise und die Strukturierungsvorschläge sind auf alle verantwortlichen Stellen übertragbar.

8. Die Leitlinie richtet sich primär an Verantwortliche für den Datenschutz und an Personen, die an der Entwicklung eines Löschkonzepts mitarbeiten.

### Löschklassen

9. Ein Löschkonzept kann nur dann mit akzeptablem Aufwand etabliert werden, wenn alle Beteiligten die Löschregeln nachvollziehen können und die Komplexität der Anforderungen überschaubar bleibt. Einfache Regeln sind daher der Schlüssel zum Erfolg. Die Leitlinie empfiehlt aus diesem Grund die Verwendung standardisierter Löschfristen und sogenannter Löschklassen, die gegebenenfalls organisationsspezifisch angepasst werden. Diese Löschklassen reduzieren die Komplexität der unterschiedlichen Löschanforderungen und bilden den Kern des Löschkonzepts. Sie werden für die Zuordnung von personenbezogenen Datenbeständen zu Löschregeln verwendet.

### Nutzen

10. Ein Löschkonzept der hier vorgeschlagenen Art hat für eine verantwortliche Stelle vielfältigen Nutzen:

- Es dient dem Schutz der Betroffenen im Sinne des Rechts auf informationelle Selbstbestimmung.
- Die verantwortliche Stelle kann belegen, dass sie Maßnahmen definiert und umgesetzt hat, um ihre datenschutzrechtlichen Pflichten zur Löschung Daten zu erfüllen.
- Die Umsetzung von Löschfristen erfordert, dass Prozessabläufe vollständig bis zum Abschluss geklärt werden. Unklare Prozesse werden geklärt, aufwändige Abläufe gegebenenfalls effizienter gestaltet.
- Die Datenhaltung wird systematisiert und konsolidiert, weil auch Altbestände in die Löschung einbezogen werden müssen und diese dadurch bereinigt werden. Dadurch können auch der Aufwand und die Kosten für Datenmigrationen bei Systemwechseln erheblich reduziert werden.
- Durch die Bereinigung von Datenbeständen und das Auflösen unnötiger Redundanz können Kosten im IT-Betrieb gesenkt werden.
- Da das Löschkonzept Soll-Vorgaben für die Löschung von Datenbeständen macht, können daraus mit geringem Aufwand Prüfbedingungen für Audits abgeleitet werden.
- Durch die systematische Erfassung der pbD und der Löschprozesse in den Systemen erhält der Verantwortliche für Datenschutz wertvolle Detailinformationen als Ergänzung zum betrieblichen Verfahrensverzeichnis.
- Nicht zuletzt verbessert die Diskussion um Löschregeln und die konstruktive Gestaltung von Geschäfts- und IT-Prozessen die Verankerung des Datenschutzes innerhalb der verantwortlichen Stelle.

11. In der Leitlinie werden auch zentrale Begriffe definiert, die in den Diskussionen um Löschregeln benötigt werden. Sie erleichtern die Verständigung zwischen fachlichen Anwendern, IT-Verantwortlichen, Systementwicklern, Management, Verantwortlichen für den Datenschutz und anderen Beteiligten.

### Anwendungsbereiche

12. Primärer Anwendungsbereich der Leitlinie ist die Entwicklung eines Löschkonzepts mit Löschregeln und deren Umsetzung durch eine verantwortliche Stelle.

13. Die Umsetzungsvorgaben für eine regelgerechte Löschung von pbD in IT-Systemen können bereits bei der Konzeption von Geschäftsprozessen hilfreich sein. Für Systementwicklungs- und Systembeschaffungsprozesse können aus ihnen Löschanforderungen definiert werden.

14. Die Leitlinie gibt zudem Software-Herstellern Hinweise darauf, wie IT-Systeme die Aufgaben der Löschung personenbezogener Daten durch verantwortliche Stellen unterstützen können. Wenn die Hersteller entsprechende Funktionen in die IT-Produkte aufnehmen, tragen sie zum rechtskonformen Design bei („Privacy by Design“).

15. Darüber hinaus bietet die Leitlinie eine Grundlage, um Muster-Kataloge mit Löschklassen entsprechend nationaler, supranationaler oder branchenspezifischer Rechtsvorgaben zu entwickeln. Liegen solche Kataloge vor, kann der Aufwand für die Erstellung des Löschkonzepts durch die verantwortliche Stelle weiter verringert werden.

# 2 Gegenstand der Leitlinie

16. In einem Löschkonzept legt eine verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von pbD erfüllt.

17. Die Leitlinie beschreibt, wie ein solches Löschkonzept etabliert werden kann. Dazu gehören:

- Vorgehensweisen, durch die Löschregeln für personenbezogene Datenbestände festgelegt werden,
- eine Übersicht über notwendige Umsetzungsvorgaben zur Löschung innerhalb der verantwortlichen Stelle,
- Vorschläge für die Dokumentationsstruktur und
- Anforderungen an Prozesse und Verantwortung für die Etablierung, Fortschreibung und Umsetzung des Löschkonzepts.

### Abgrenzung

18. Die Leitlinie legt keine konkreten Löschregeln und Löschfristen fest. Diese hängen von den jeweils einschlägigen Rechtsvorschriften und den zulässigen Zwecken der Verarbeitung durch die jeweilige verantwortliche Stelle ab. Auch die Rechtsvorgaben selbst, beispielsweise der EU oder nationale Gesetze, sind nicht Gegenstand der Leitlinie. In der Leitlinie werden auch keine Aussagen dazu getroffen, unter welchen Umständen Datenbestände als anonymisiert gelten, deshalb nicht mehr unter die Datenschutzregeln fallen und daher weiter gespeichert werden dürfen.

19. Technische Mechanismen des Löschens sind ebenfalls nicht Gegenstand die Leitlinie, beispielsweise Löschen durch Überschreiben von Attributen, Löschen von Datensätzen oder Löschen ganzer Tabellen oder Dateien. Auch Fragen, die die Sicherheit von Mechanismen zum Löschen von Daten oder Vernichten von Datenträgern betreffen, werden nicht betrachtet.

20. Diese Leitlinie bezieht sich nur auf das Löschen personenbezogener Daten. Daten, die keinen Personenbezug aufweisen, werden in der Leitlinie nicht betrachtet. Allerdings kann die Vorgehensweise grundsätzlich auch auf solche Datenbestände übertragen werden.

# 3 Begriffe und Definitionen

21. **Anonymisieren**
Prozess, durch den pbD so verändert werden, dass der Betroffene nicht mehr direkt oder indirekt identifiziert werden kann.

ANMERKUNG 1: Um pbD zu anonymisieren, werden beispielsweise einzelne Attribute eines Datenobjekts gelöscht oder überschrieben, die die Zuordnung zum Betroffenen ermöglichen. Die verbleibenden Daten (für die der Personenbezug aufgehoben wurde), fallen nicht mehr unter die Regeln des Datenschutzes und müssen demnach nicht mehr nach deren Vorgaben gelöscht werden. Identifizierende Attribute können z. B. sein Name und Geburtsdatum, Identifikationsnummern, biometrische Merkmale, zugeordnete Kontonummern, Telefonnummern, Steuernummern und dergleichen, Datenbankschlüssel, die auf Personen verweisen, oder auch eine Kombination mehrerer oder vieler einzelner Merkmale, die auf eine einzelne Person (oder eine kleine Gruppe) rückschließen lässt.

ANMERKUNG 2: Je nach den Vorgaben der einschlägigen Rechtvorschriften muss der Aufwand zur Wiederherstellung eines Personenbezugs unverhältnismäßig hoch sein oder er darf gar nicht möglich sein. [ISO 29100] fordert, dass die Anonymisierung irreversibel ist.

ANMERKUNG 3: Je nachdem, welcher Datenbestand nach der Aufhebung des Personenbezugs noch vorhanden ist und welche Daten für die Wiederherstellung benutzt werden können, können sehr vielfältige Strategien zur Wiederherstellung des Personenbezugs greifen. So können z. B. Zeitpunkte bestimmter Ereignisse, Bewegungsprofile oder Rechnungsbeträge verwendet werden, um Korrelationen zwischen Datenbeständen zu bestimmen und damit den Personenbezug wieder herzustellen. Solche Möglichkeiten müssen bereits in den Umsetzungsvorgaben für die Aufhebung des Personenbezugs berücksichtigt werden. Datenbestände zu anonymisieren ist deshalb häufig wesentlich schwieriger, als sie fristgerecht zu löschen. Je nach Umsetzung kann die Anonymisierung möglicherweise auch mit neuen Erkenntnissen oder neu verfügbaren Datenbeständen wieder rückgängig gemacht werden.

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

ANMERKUNG: Eine Aufbewahrungsfrist trägt zur Vorhaltefrist bei.

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

ANMERKUNG: Datenschutzvorschriften können sich auch auf andere Schutzsubjekte als natürliche Personen beziehen, beispielsweise juristische Personen. In dieser Leitlinie wird trotzdem durchgängig nur vom Betroffenen gesprochen. Werden von den einschlägigen Rechtvorschriften andere Schutzsubjekte eingeschlossen, sind auch deren Daten im Löschkonzept zu berücksichtigen.

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

25. **Datenbestand**
eine Menge an personenbezogenen Daten der verantwortlichen Stelle

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

ANMERKUNG: Datenobjekte können mit anderen Datenobjekten in einer Datenart zusammengefasst werden. Die einzelnen Datenobjekte können unterschiedlich komplex sein: so enthält ein Datenobjekt „Datensatz in einer Datenbank“ mehrere Datenobjekte vom Typ „Attribut“. Detaillierte Hinweise gibt Kapitel 6.1.

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

ANMERKUNG: Als Dokument wird hier eines der Dokumente verstanden, in denen die verantwortliche Stelle die Festlegungen ihres Löschkonzepts trifft. Die Gruppe von Dokumenten, die das Löschkonzept bildet (siehe auch Löschkonzept), darf nicht verwechselt werden mit Dokumenten, die als Datenobjekte Teil eines Datenbestands sind und Löschregeln unterworfen werden.

28. **Einschlägige Rechtsvorschriften**
die für einen spezifischen Datenbestand geltenden datenschutzrechtlichen Regelungen.

ANMERKUNG 1**:** Zu den einschlägigen Rechtsvorschriften zählen z. B. Gesetze, Verordnungen oder vertragliche Regelungen. Da sich die einschlägigen Rechtsvorschriften länderspezifisch, nach Datenarten und verantwortlicher Stelle unterscheiden, führen sie zu spezifischen Löschregeln. Die Leitlinie gibt daher nur einen Rahmen vor, in dem diese Regeln entwickelt und angewandt werden können.

ANMERKUNG 2**:** Zu Rechtsvorschriften zählen in Deutschland beispielsweise auch Betriebs- oder Dienstvereinbarungen.

29. **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.

ANMERKUNG 1: In der Regel ist "sicheres Löschen" gefordert. Sicheres Löschen meint, dass der Aufwand für die Rekonstruktion der Daten unverhältnismäßig hoch ist oder aus physikalischen Gründen unmöglich ist.

ANMERKUNG 2**:** Wenn die einschlägigen Rechtsvorschriften dies zulassen, können personenbezogene Daten auch anonymisiert werden, statt sie zu löschen. Siehe zu den Anforderungen an die Anonymisierung auch unter dem Begriff „anonymisieren“.

30. **Löschklasse**
Kombination aus Löschfrist und abstraktem Startzeitpunkt für den Fristlauf.

ANMERKUNG: In einer Löschklasse werden alle Datenarten zusammengefasst, die der gleichen Löschfrist unterliegen. Im Unterschied zur Löschregel für eine Datenart wird in der Löschklasse nur auf den Typ des Startzeitpunkts, nicht aber auf eine konkrete Bedingung für den Start des Fristlaufs abgestellt (siehe auch Kapitel 8).

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

32. **Löschregel**
Kombination aus Löschfrist und Bedingung für den Startzeitpunkt des Fristlaufs.

33. **Personenbezogene Daten (pbD)**
Einzelangaben über persönliche oder sachliche Verhältnisse eines Betroffenen.

ANMERKUNG: Hier wurde die Definition des personenbezogenen Datums nach § 3 Abs. 1 BDSG verwendet. Für die Etablierung eines betrieblichen Löschkonzepts ist die Definition nach den jeweils einschlägigen Rechtsvorschriften zu verwenden.

34. **Regellöschfrist (Löschfrist)**
Frist, nach der eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle spätestens zu löschen ist.

ANMERKUNG: Zu den Randbedingungen der Fristfestlegung siehe Abschnitt 5.3.3.

35. **Verantwortliche Stelle**
Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

ANMERKUNG 1: Hier wurde die Definition der verantwortlichen Stelle nach § 3 Abs. 3 BDSG verwendet. Für die Etablierung eines Löschkonzepts ist die Definition nach den einschlägigen Rechtsvorschriften zu verwenden.

ANMERKUNG 2: Die Leitlinie kann auch angewendet werden, wenn datenschutzrechtlich künftig das „Shared-Data-Konzept" zugelassen wird. In diesem Fall nutzen verschiedene verantwortliche Stellen einen Datenbestand gemeinsam. Die Löschung muss dann zwischen diesen Stellen abgestimmt werden, beispielsweise dadurch, dass eine Stelle die Koordination für die Festlegung der Löschregeln übernimmt.

36. **Verantwortlicher für Datenschutz**
Person in der verantwortlichen Stelle, die auf die Einhaltung datenschutzrechtlicher Anforderungen hinwirkt.

ANMERKUNG 1: In Deutschland ist dies regelmäßig der betriebliche Datenschutzbeauftragte. Wo dieser nicht bestellt ist, muss die Geschäftsführung trotzdem sicherstellen, dass die datenschutzrechtlichen Anforderungen erfüllt werden. Es ist grundsätzlich sinnvoll, dass in der verantwortlichen Stelle ein Ansprechpartner (oder ein Team) mit Datenschutzkompetenz zur Verfügung steht. Dieser Ansprechpartner sollte die Aufgaben wahrnehmen, die in dieser Leitlinie dem Verantwortlichen für Datenschutz zugeordnet werden.

ANMERKUNG 2: Welche konkreten Anforderungen an die verantwortliche Stelle bestehen, einen Verantwortlichen für Datenschutz zu benennen, ergibt sich aus den einschlägigen Rechtvorschriften und ist außerhalb des Gegenstands der Leitlinie.

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

ANMERKUNG: Neben der Aufbewahrungsfrist tragen auch andere Anforderungen zur Vorhaltefrist bei. Zu den Randbedingungen der Fristfestlegung siehe Abschnitt 5.3.3.

# 4 Abkürzungen

| | |
|---|---|
| Abb. | Abbildung |
| Abs. | Absatz |
| AO | Abgabenordnung |
| BDSG | Bundesdatenschutzgesetz |
| BFStrMG | Bundesfernstraßenmautgesetz |
| BGB | Bürgerliches Gesetzbuch |
| DIN | Deutsches Institut für Normung e.V. |
| INS | Innovationen durch Normen und Standards |
| HGB | Handelsgesetzbuch |
| ISO | International Standardization Organisation |
| pbD | personenbezogene Daten |
| StGB | Strafgesetzbuch |
| TKG | Telekommunikationsgesetz |
| TMG | Telemediengesetz |

# 5 Grundlagen eines Löschkonzepts

## 5.1 Allgemeines

48. Diese Leitlinie bezieht sich nur auf das Löschen von pbD. Sie beschreibt, wie ein betriebliches Löschkonzept etabliert werden kann und welche Festlegungen dafür getroffen und dokumentiert werden müssen.

49. Dieses Kapitel stellt die Bausteine eines Löschkonzepts im Überblick vor. In den weiteren Kapiteln werden die einzelnen Bausteine detailliert beschrieben.

50. Das Löschen von pbD muss die jeweils gemäß der einschlägigen Rechtsvorschriften verantwortliche Stelle sicherstellen. Das Löschen dieser Daten stellt die verantwortliche Stelle allerdings vor vielfältige Herausforderungen. Für eine dauerhafte Umsetzung von Löschprozessen, die den gesamten Bestand an pbD einer verantwortlichen Stelle abdecken, ist daher ein strukturiertes und geregeltes Vorgehen erforderlich. Die verantwortliche Stelle muss dazu Festlegungen treffen, durch die eine datenschutzkonforme Löschung erreicht wird. Die Festlegungen müssen umfassen,

- welche Löschregeln für welche Datenbestände gelten,
- wie die aus den Löschregeln die Umsetzung der Löschung in Prozessen der verantwortlichen Stelle erreicht wird,
- wie die Löschregeln, Umsetzungsvorgaben und durchgeführten Löschmaßnahmen zu dokumentieren sind und
- wer für die aus dem Löschkonzept entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung verantwortlich ist.

51. Diese Festlegungen bilden das Löschkonzept der verantwortlichen Stelle.

52. Diese Leitlinie soll die folgenden Ziele unterstützen:

- Der Ressourcenbedarf der Beteiligten soll nach Möglichkeit gering gehalten 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 Löschregeln definiert. Dadurch soll das Löschkonzept von den Beteiligten besser verstanden werden. Die Löschregeln sind außerdem betrieblich einfacher umsetzbar.
- Der Dynamik von Veränderungen an Geschäftsprozessen und IT-Systemen wird Rechnung getragen.

53. Diese Form der Effizienz kann nur erreicht werden, wenn die Komplexität des Löschkonzepts im Rahmen der einschlägigen Rechtsvorschriften so weit wie möglich reduziert wird. Andernfalls droht die Entwicklung oder Umsetzung eines Löschkonzepts zu scheitern.

## 5.2 Was bedeutet „Löschen“?

54. 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. Löschen wird z. B. durch das physische Überschreiben von Datenobjekten erreicht.

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

56. 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 Löschregeln. Daten richtig zu anonymisieren ist allerdings oft sehr schwierig. Es wird dringend empfohlen, der Löschung von Daten den Vorrang zu geben.

ANMERKUNG 1: Welche Verfahren für die Löschung oder Vernichtung einzusetzen sind, richtet sich nach der Sensitivität der Daten, den Datenträgern und den einschlägigen Rechtsvorschriften. Die Auswahl der Verfahren ist nicht Gegenstand der Leitlinie. Weiterführende Informationen dazu finden sich z. B. in [NIST SP 800-88] und [CSEC 2006].

ANMERKUNG 2: Für die Anonymisierung von Datenarten müssen häufig zahlreiche Bedingungen beachtet werden – siehe dazu die Anmerkungen zur Definition „Anonymisieren“. Welche Eigenschaften und Qualität die Anonymisierung mindestens aufweisen muss, richtet sich nach den jeweils einschlägigen Rechtsvorschriften.

ANMERKUNG 3: Im Weiteren wird nur noch der Begriff "Löschen" verwendet. Die Alternativen „Vernichten von Datenträgern“ und „Anonymisieren von Datenarten“ sind immer eingeschlossen.

## 5.3 Eine Löschregel für jede Datenart

### 5.3.1 Löschregeln

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

BEISPIELE: Für die Datenart „Buchhaltungsdaten" könnte in Deutschland die Löschregel lauten: „11 Jahre nach dem Ende des Geschäftsjahres, in dem die Buchung in der Bilanz berücksichtigt wurde“. Für die Datenart "Interessentenadressen", die ausschließlich zur Bearbeitung von Anfragen nach Prospektmaterial verwendet wird, könnte die Löschregel lauten „1 Jahr nach Bearbeitung der Anfrage“.

58. Löschregeln, 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.

### 5.3.2 Datenarten

59. 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 „Use, Retention and Disclosure Limitation“ und „Data Minimization“ anzuwenden. Danach sind pbD so früh wie möglich zu löschen.

60. Soweit Teile des Gesamtdatenbestandes einer verantwortlichen Stelle für unterschiedliche Zwecke verwendet werden, können sich auch unterschiedliche Regeln für die Löschung ergeben.

61. 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 Löschregel zugeordnet.

62. Für eine klare Kommunikation über das Löschkonzept ist es sinnvoll, jede Datenart eindeutig zu bezeichnen. Die Bezeichnung soll sich am fachlichen Verwendungszweck innerhalb der verantwortlichen Stelle orientieren und zwischen dem Verantwortlichen für den Datenschutz und den anderen Beteiligten abgestimmt werden.

BEISPIELE: Als Datenarten könnten bei einem Telekommunikations-Provider z.B. Stammdaten, Standortdaten, Verkehrsdaten, Abrechnungsdaten und Einzelverbindungsnachweise unterschieden werden.

### 5.3.3 Vorhaltefrist und Regellöschfrist

#### *5.3.3.1 Löschen im Regelprozess*

63. 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.

64. Rechtliche Aufbewahrungspflichten sind Teil des Verwendungsprozesses in der verantwortlichen Stelle und damit auch Teil der Aufbewahrungsfrist. Sie ergeben sich, wenn in einschlägigen Rechtvorschriften 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 verschieden Anforderungen ergeben sich überlappende Anteile der Aufbewahrungsfrist.

BEISPIEL: Zu rechtlichen Aufbewahrungspflichten zählen beispielsweise die Vorgaben des Steuerrechts für Handelsbriefe und Buchhaltungsunterlagen. Zu anderen fachlichen Anforderungen zählen z. B. Garantiezusagen oder potentielle Rückrufaktionen.

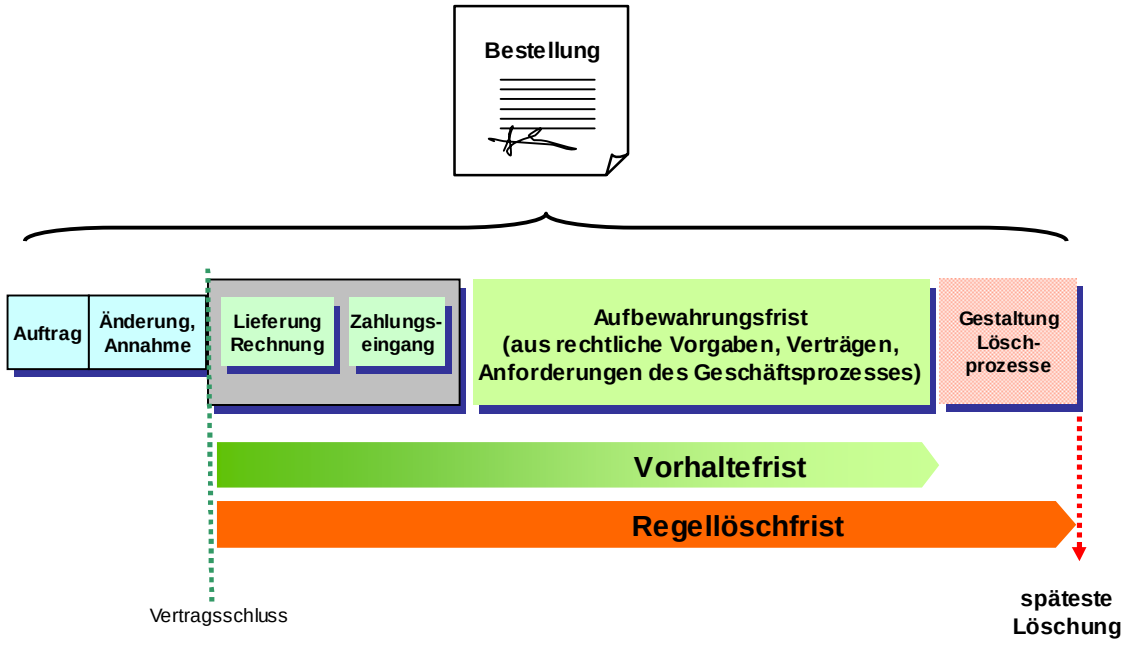
ANMERKUNG: Die einschlägigen Rechtvorschriften können besondere Maßnahmen fordern, wenn Datenobjekte nur noch gespeichert werden, um Aufbewahrungspflichten zu erfüllen. Nach dem BDSG ist beispielsweise die Einschränkung der Zugriffsberechtigten gefordert (Sperrung).

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

66. Nach dem Ende der jeweiligen Vorhaltefrist werden die Daten in der verantwortlichen Stelle nicht mehr benötigt. Sie müssen dann innerhalb einer datenschutzrechtlichen vertretbaren Frist gelöscht werden. Die Summe aus Vorhaltefrist und der datenschutzrechtlich vertretbaren Frist für die Gestaltung der Löschprozesse definiert die längste Löschfrist bei der Verarbeitung der Daten im Regelprozess. Diese Frist wird als Regellöschfrist bezeichnet. Nach Ablauf der Regellöschfrist müssen die entsprechenden Bestände der Datenart in allen Systemen der verantwortlichen Stelle gelöscht sein. Dies schließt die Löschung bei Auftragneh-

mern der verantwortlichen Stelle ein.

**Abbildung 1: Beispiel für Fristabschnitte für einen Auftrag im Löschkonzept**




Im Beispiel beginnt der Lauf der Vorhalte- und der Regellöschfrist mit dem Vertragsschluss. Der Vertragsschluss ist ein Beispiel für einen Startzeitpunkt vom Typ „Ende eines Vorgangs“. Die aktive Verwendung des Vertrages endet mit dem Zahlungseingang. Danach wird der Vertrag noch für eventuelle Garantiefälle und als Handelsbrief nach AO und HGB aufbewahrt.

67. Soweit die Verwendung von pbD nach der jeweiligen Rechtsordnung einer Rechtsgrundlage bedarf, bestimmen die zulässigen Verwendungszwecke auch die Vorhaltefrist und die Regellöschfrist. Wenn die Rechtslage Spielräume für die Fristen zur Verwendung einer Datenart einräumt, kann der Verwendungs- und Löschprozess gestaltet werden. Die verantwortliche Stelle muss abschätzen und datenschutzrechtlich verantworten können, ob und wie lange nach dem Ende der Vorhaltefrist die Löschung erfolgen kann.

ANMERKUNG 1: Wenn rechtliche Spielräume bestehen, muss die Vorhaltefrist in vielen Fällen nicht exakt analysiert werden. Oft genügt es zu prüfen, ob die Verwendungszwecke für eine Datenart vernünftigerweise innerhalb einer bestimmten Vorhaltefrist abgearbeitet werden. In anderen Fällen kann die Vorhaltefrist direkt aus rechtlichen Vorgaben abgeleitet werden, weil die Aufbewahrungspflichten sowieso längere Fristen fordern, als die Datenobjekte aktiv in Prozessen verwendet werden. Für beide Fälle können Löschklassen zur Festlegung der Löschregeln benutzt werden (siehe Kapitel 8).

ANMERKUNG 2: Im Beispiel in der Abbildung ist die Vorhaltefrist kürzer als die Regellöschfrist. Je nach Datenart und Löschfristen der verantwortlichen Stelle können Vorhaltefrist und Regellöschfrist auch gleich lang sein. Wenn die einschlägigen Rechtsvorschriften die Regellöschfrist begrenzen, darf die Vorhaltefrist für eine Datenart die Regellöschfrist nicht überschreiten. Beispielsweise begrenzt § 97 TKG die Speicherdauer der für die Berechnung der Entgelte erforderlichen Verkehrsdaten auf sechs Monate. Weitere Hinweise zur Zuordnung von Regellöschfristen zu Datenarten finden sich im Kapitel 8.3.

ANMERKUNG 3: Durch den Zeitraum zwischen dem Ende der Vorhaltefrist und dem Ende der Regellöschfrist soll die Praktikabilität des Löschkonzepts und der betrieblichen Umsetzung von Löschmaßnahmen erreicht werden. In diesem Zeitraum befinden sich die jeweiligen die Daten im Zulauf zum Löschen und sollten dem Zugriff der Anwender entzogen sein.

#### *5.3.3.2 Sonderfälle*

68. 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 7.3.2). Zur Behandlung von Störfällen kann die Löschung zeitweise ausgesetzt werden (Abschnitt 7.3.4).

### 5.3.4 Unterscheidung zwischen Archiv, Sicherungskopie und gesperrten Daten

#### *5.3.4.1 Archive und Sicherungskopien*

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

70. **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 Löschfristen enthalten.

71. **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.

72. 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 Löschfrist zu sehr unterschiedlichen Zeiten. Zur Einhaltung von Löschregeln wären deshalb häufig einzelne Daten aus den Sicherungskopien zu löschen.

73. Zwischen Sicherungskopien und Archiven muss deshalb klar getrennt werden. Die pbD in Archiven unterliegen den Löschregeln 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 Regellöschfristen der im Backup enthalten „gemischten“ Daten verhältnismäßig sind (siehe Abschnitt 7.3.5).

#### *5.3.4.2 Gesperrte Datenbestände*

74. 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.

75. Es ist möglich, für Datenarten neben den Löschregeln auch Sperrregeln anzugeben. Dieser Aspekt wird in dieser Leitlinie nicht weiter verfolgt.

### 5.3.5 Standardlöschfristen, Startzeitpunkte, Löschregeln und Löschklassen

76. Für die Festlegung der Löschregeln für einzelne Datenarten kann vielfältiger Analyseaufwand entstehen. Da die Verantwortlichen für den Datenschutz an der datenschutzrechtlichen Bewertung von Abläufen beteiligt sein müssen, sind deren Ressourcen bei der Entwicklung und Pflege des Löschkonzepts ein kritischer Faktor. Auch für andere Mitarbeiter der verantwortlichen Stelle sollen hohe Aufwände vermieden werden. Zum Aufwand trägt bei, dass Geschäftsprozesse und IT-System teilweise mit hoher Dynamik geändert werden. Das kann wiederholte Analysen erfordern.

77. Es wird deshalb empfohlen, **Standardlöschfristen** zu verwenden, die die verantwortliche Stelle anhand der einschlägigen Rechtsvorschriften festlegt.

78. 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“.

79. Die Standardlöschfristen und die abstrakten Startzeitpunkte können kombiniert werden. Jede Kombination von Löschfrist und Startzeitpunkt bildet eine sogenannte **Löschklasse**. Die Datenarten können den Löschklassen auf einfache und effiziente Weise zugeordnet werden: In einer Löschklasse werden alle Datenarten zusammengefasst, die der gleichen Löschfrist unterliegen und für die der gleiche abstrakte Startzeitpunkt gilt. Von den Beteiligten kann gut verglichen und geprüft werden, ob die Datenarten richtig eingeordnet wurden.

### 5.3.6 Löschen in Sondersituationen

80. Das Löschen in manchen Sondersituationen kann nicht von Löschregeln im Sinne dieser Leitlinie bestimmt werden. Dazu gehören:

- das Löschen von unberechtigt erhobenen pbD
- das Löschen von pbD nach einem berechtigten Löschbegehren des Betroffenen (z. B. § 35 BDSG)
- das Löschen von pbD beim Rückbau von Systemen

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

82. Voraussetzung für das Löschen einzelner Daten von Betroffenen ist, dass die technischen Systeme über eine geeignete Funktion zum Löschen verfügen. Diese sind in Prozessen der Systembeschaffung oder -entwicklung zu fordern.

## 5.4 Etablieren des Löschkonzepts

### 5.4.1 Dokumentationsstruktur des Löschkonzepts

83. Die Festlegungen des Löschkonzepts müssen dokumentiert werden. Die Inhalte der Dokumente sollen zielgruppenspezifisch aufgeteilt und beschrieben werden. Als Zielgruppen können in der Regel unterschieden werden: die Verantwortlichen für Datenschutz, fachliche

Anwender, Entwickler, Administratoren und Auftragnehmer. Vorschläge für die Aufteilung von Inhalten ergeben sich aus Kapitel 9 und 10.

84. Die Dokumente sollen möglichst in eine bestehende Dokumentationsstruktur der verantwortlichen Stelle eingeordnet werden. Wo dies sinnvoll ist, können die Inhalte auch in bestehende Dokumente integriert werden. Um sicherzustellen, dass in der Dokumentation keine Inkonsistenzen entstehen und die Pflege effizient erfolgen kann, sollte jede Festlegung nur an einer Stelle dokumentiert werden.

85. In den einzelnen Abschnitten dieser Leitlinie werden Empfehlungen gegeben, wo Festlegungen des Löschkonzepts und Maßnahmen zu seiner Umsetzung dokumentiert werden können.

### 5.4.2 Prozesse und Verantwortlichkeiten

86. Im ersten Schritt wird die Verantwortung für die Aufgaben im Löschkonzept festgelegt (siehe Kapitel 10).

87. Die Verantwortlichen sind entsprechend dem Projektfortschritt mit den notwendigen Ressourcen auszustatten.

### 5.4.3 Projekt Löschkonzept

88. Um den Implementierungsaufwand für Löschmaßnahmen zu reduzieren, ist es sinnvoll, die Löschregeln für alle Arten von pbD in einem IT-System gemeinsam zu implementieren. Zusätzlich können zwischen den Löschfunktionen in verschiedenen Systemen Abhängigkeiten bestehen, weil Datenbestände in Folgesystemen abhängig von Daten in Primär-Systemen zu löschen sind. Solche Abhängigkeiten müssen für die Implementierung von Löschmaßnahmen in einem System berücksichtigt werden.

BEISPIEL: In einem Dokumentenmanagementsystem (DMS) werden Dokumente zu Vorgängen aus einem Customer-Relationship-Managementsystem (CRM) gespeichert. Wenn das CRM führend für die Löschung im DMS ist, müssen für die Implementierung von Löschfunktionen im CRM alle Datenarten bekannt sein, für die das CRM die Löschung im DMS anstoßen soll.

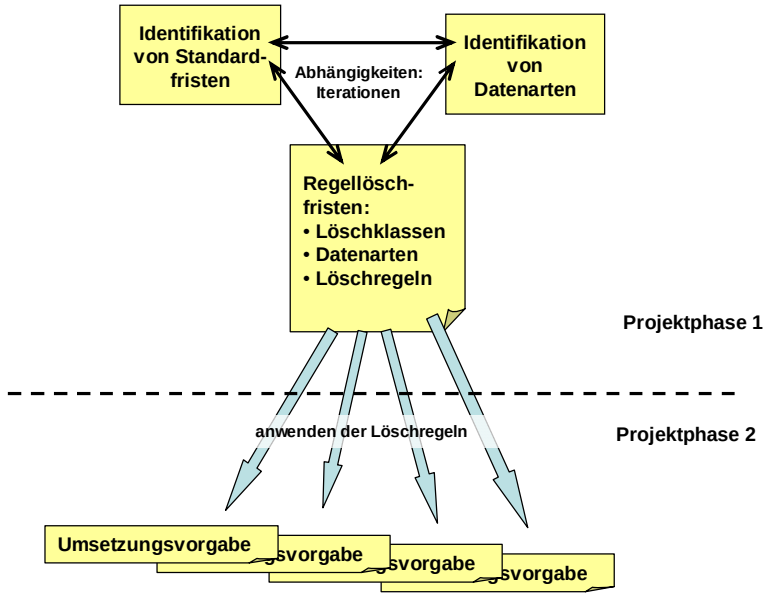
89. Es ist deshalb empfehlenswert, in einer **ersten Phase** zur Etablierung des Löschkonzepts die Löschregeln möglichst vieler Datenarten zu bestimmen. Dazu sind die Datenarten abzugrenzen (Kap. 6), die Standardlöschfristen zu bestimmen (Kap. 7) und die Datenarten den Löschklassen zuzuordnen (Kap. 8.3). Alle Löschregeln werden dokumentiert, z. B. im Dokument „Regellöschfristen“ (Kap. 8.3).

90. In der **zweiten Projekt-Phase** steht die Implementierung der Löschregeln für die Regelprozesse im Mittelpunkt. Dazu sind die Umsetzungsvorgaben zu erstellen und zu realisieren.

91. Die Reihenfolge der Maßnahmen sollte so bestimmt werden, dass

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

**Abbildung 2: Projektphasen „Regellöschfristen“ und „Umsetzung von Löschregeln“**




In der ersten Projektphase werden in mehreren Iterationen die Löschregeln der verantwortlichen Stelle möglichst vollständig zusammengestellt. Zwischen den Datenarten, den Standardfristen und den Löschregeln bestehen wechselseitige Abhängigkeiten. Z. B. kann eine neue Datenart eine zusätzliche Standardlöschfrist erfordern, die dann auch für andere Datenarten enger an der Vorhaltefrist liegt. Anschließend werden die Umsetzungsvorgaben erstellt und Implementierungsprojekte aufgesetzt.

### 5.4.4 Regelabläufe

92. Nach Abschluss des Projekts „Löschkonzept“ sollten die initialen Aufgaben, die einen vergleichsweise hohen Aufwand erfordern, umgesetzt sein. Die Regellöschfristen, die Zuordnung der Verantwortung und die Prozesse des Löschkonzepts sollten dann etabliert sein. Die kontinuierliche Fortschreibung des Löschkonzepts und die Pflege seiner Umsetzungsvorgaben erfolgt in Regelprozessen der verantwortlichen Stelle, beispielsweise im Betrieb und im Change-Management (siehe auch Kapitel 10.3.3).

# 6 Datenarten bilden

## 6.1 Datenbestände, Zwecke und Datenarten

93. 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 Rechtvorschriften unterschiedliche Vorgaben für Datenbestände treffen,
- 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.

94. Datenbestände sind unterschiedlich strukturiert, z. B. als Attribute 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 Ausdrucke.

95. Eine Datenart wird durch alle Datenobjekte gebildet, 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.

96. Eine Datenart wird durch die Datenobjekte gebildet, 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“.

97. 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 Löschfrist 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. Diese Regel gilt dann auch für die Log-Datensätze in dieser Datenart.

ANMERKUNG: Wenn erkannt wird, dass die Datenarten mit überschneidenden Datenobjekten der gleichen Löschregel unterliegen, kann es sinnvoll sein, die Datenobjekte in einer Datenart zusammenzufassen.

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

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 nach-

zukommen), 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

99. Im Löschkonzept der verantwortlichen Stelle sollte sichergestellt werden, dass alle Datenobjekte, die als pbD einzustufen sind, Datenarten zugeordnet werden.

100. Dazu kann zunächst identifiziert werden, welche Datenarten in den verschiedenen Geschäftsprozessen der verantwortlichen Stelle verwendet werden.

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

- Im Rahmen der Festlegung von Löschklassen und Löschregeln 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.

102. Alle Datenarten sollen im Dokument „Regellöschfristen“ beschrieben werden (vgl. Kapitel 8.3).

## 6.3 Gestaltungskriterien für die Bildung von Datenarten

### 6.3.1 Hinweise aus der Praxis

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

#### *6.3.1.1 Orientierung an Rechtsvorgaben*

104. Wenn für Gruppen von Datenobjekten einheitliche Rechtsregeln gelten, ist es sinnvoll, sie in einer Datenart zusammenzufassen.

105. 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*

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

107. Die Namen der Datenarten dienen der Verständigung zwischen den am Löschkonzept beteiligten Gruppen. Es kann daher sinnvoll sein, für Datenbestände, die fachlich unterschiedlich verwendet werden, verschiedene Datenarten einzuführen, obwohl sie den gleichen Löschregeln 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 fachliche Diskussion sinnvoll sein, sie als eigene Datenart zu führen.

108. 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.

109. Wenn Datenobjekte mit stark unterschiedlichen Vorhaltefristen in einem Datenbestand enthalten sind, ist es sinnvoll, diese in unterschiedliche Datenarten zu gruppieren.

110. 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

111. 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.

112. 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 Löschmechanismen genügen müssen, die für die Datenart angewandt werden.

ANMERKUNG: Vertraulichkeitsklassifikationen bestehen in vielen Organisationen bereits. Es ergeben sich unmittelbare Synergieeffekte, wenn für das Löschkonzept deren Sicherheitsanforderungen für die Löschmechanismen übernommen werden können. Eine Kombination von Datenart und Vertraulichkeitsstufe ist auch naheliegend, weil auch eine Vertraulichkeitsklassifikation Datenbestände in Klassen aufteilt.

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

114. Der Aspekt der Vertraulichkeitsklassifikation wird in dieser Leitlinie nicht weiter betrachtet.

# 7 Löschfristen festlegen

## 7.1 Standardlöschfristen verwenden

115. 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 Löschfristen verzichtet werden kann und stattdessen eine Nutzung der jeweils „nächstgelegenen" Standardlöschfrist ausreicht.

116. Standardlöschfristen werden von jeder verantwortlichen Stelle für ihren Bereich festgelegt. Mit den in Abschnitt 7.2 vorgeschlagenen Vorgehensweisen zur Fristdefinition kann sie Löschfristen 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.

117. 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.

ANMERKUNG 1: 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.

ANMERKUNG 2: 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 Löschmaßnahmen. Die Zahl der Standardfristen soll einen guten Kompromiss zwischen einer datenschutzrechtlich vertretbaren Fristabstufung und einer beherrschbaren Komplexität der Fristen ermöglichen. In Zweifelsfällen sollte die verantwortliche Stelle die Fristabstufung mit Ihrer Aufsichtsbehörde abstimmen.

ANMERKUNG 3: Der Grund für eine Begrenzung auf wenige Standardlöschfristen ist ein einfach verständliches Löschkonzept und die einfache Ableitung von Löschregeln. Standardfristen für einzelne Datenarten einzuführen, widerspräche 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 Löschfrist 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

118. Wenn die verantwortliche Stelle eigene Löschfristen 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.

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

- Für die Datenart ist in den Rechtsvorschriften eine Löschfrist angegeben: Die Löschfrist kann direkt übernommen werden.
- Für die Löschung 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 Löschung der Datenart muss nur an den allgemeinen Prinzipien der Erforderlichkeit und Datensparsamkeit ausgerichtet werden, beispielsweise in Deutschland nur nach § 35 BDSG: Die Ableitung von Standardlöschfristen anhand einfacher Kriterien ist ausreichend.

120. Im Regelfall ist es ausreichend, die Standardlöschfristen des Löschkonzepts anhand ausgewählter Datenarten festzulegen. Dazu werden in einem iterativen Prozess Datenarten identifiziert, die mögliche Stellvertreter für Löschklassen sind. Für diese erfolgt die Fristfestlegung und die Definition der Löschklassen. Wenn alle weiteren Datenarten in datenschutzrechtlich vertretbarer Weise den so gefundenen Löschklassen 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 Löschklassen gebildet werden.

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

BEISPIELE: Ein Telekommunikations-Provider könnte beispielsweise die Frist für die Löschung von Einzelverbindungsnachweisen als eine Standardfrist wählen. Ein Unternehmen, das Maut erhebt, würde dagegen die Löschfrist für Fahrtdaten als eine Standardfrist einsetzen.

### 7.2.2 Unmittelbare Fristen aus Rechtsvorschriften

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

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

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

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

### 7.2.3 Fristfestlegung nach Prozessanalyse

125. 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.

126. Die verantwortliche Stelle ist dann gehalten, die Vorhaltefrist für die jeweilige Datenart genau zu bestimmen, damit die Löschfrist 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.

127. Die Regellöschfrist 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.

128. Es ist sinnvoll, solche Löschfristen in den Katalog der Standardlöschfristen aufzunehmen, wenn der Katalog dadurch nicht zu sehr differenziert wird.

### 7.2.4 Ableitung von Löschfristen nach einfachen Kriterien

129. Die Abstufung der Standardlöschfristen, 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 wird, dass dies datenschutzrechtlich nicht mehr vertretbar ist. Dann sollten weitere Standardlöschfristen ergänzt werden, um eine feinere Abstufung zu erreichen.

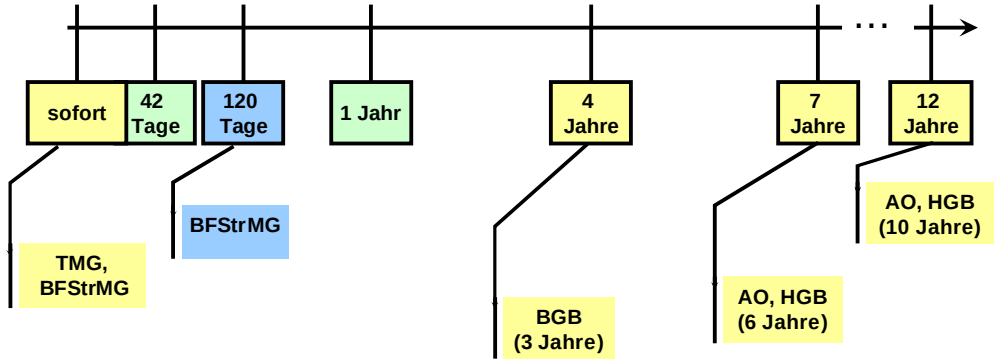
130. Soweit die Verwendung von pbD nur durch allgemeine Rechtsvorschriften geregelt ist, können Spielräume für die Festlegung von Löschfristen bestehen. Diese Spielräume können genutzt werden, um die zusätzlichen Standardlöschfristen festzulegen.

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 Standardlöschfristen müssen so festgelegt werden, dass für die zugeordneten Datenarten der Grundsatz der Erforderlichkeit auf datenschutzrechtlich vertretbare Weise eingehalten wird.

131. 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.

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

**Abbildung 3: Beispiel für einen Katalog von Standardlöschfristen (Toll Collect)**




**Legende:**
gelb unterlegt: Frist abgeleitet aus allgemeinen Gesetzen
blau unterlegt: Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
grün unterlegt: Frist frei gewählt

Die 4- und die 7-Jahresfrist ergeben sich, weil die Verjährungsfrist nach BGB bzw. die Aufbewahrungsfrist nach AO/HGB am Ende des jeweiligen Kalenderjahres beginnt. Die 12 Jahre ergeben sich für Toll Collect, weil die 10-Jahresfrist am Ende des Kalenderjahres beginnt, in dem ein Buch geschlossen wird. Das Geschäftsjahr von Toll Collect weicht allerdings vom Kalenderjahr ab, so dass Buchhaltungsdaten aus zwei Kalenderjahren für ein Buch/eine Bilanz relevant sind.

133. Durch die Löschfristen nach einfachen Kriterien kann der Fristkatalog so ergänzt werden. dass die Abstufung der Standardlöschfristen datenschutzrechtlich vertretbar ist.

## 7.3 Besonderheiten für Fristfestlegungen

### 7.3.1 Regellöschfristen und Abweichungen

134. 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 Löschfristen festzulegen, ist datenschutzrechtlich jedoch nicht vertretbar.

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

### 7.3.2 Friständerungen durch Verdichtung mit Wechsel der Datenart

136. 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

137. 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 Löschfrist 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.

BEISPIELE: Die Datenart für Daten, die zur Bearbeitung einer Reklamation benötigt werden, könnte „Reklamationsdaten" heißen. Die Löschregel 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 Löschregel könnte ebenfalls eine Frist von einem Jahr vorsehen und als Startzeitpunkt auf die Rechtskraft des Urteils abstellen.

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

### 7.3.4 Ausnahmen von Regelprozessen: Aussetzung der Löschung

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

140. 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 Löschfrist 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 Löschfrist 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."*

141. 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 Standardlöschfristen für Sicherungskopien

142. 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 Löschfrist für Teile der Daten überschritten.

143. 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 Löschfristen der Datenarten, die in der Sicherungskopie enthalten sind, aber nur um ein datenschutzrechtlich vertretbares Maß überschritten werden. Die Löschfrist der Sicherungskopie muss sich an der kürzesten Löschfrist der jeweils enthaltenen Datenarten orientieren.

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

144. Gegebenenfalls müssen die Sicherungs-Strategien und die Maßnahmen zum Wiederanlauf so angepasst werden, dass sie mit den datenschutzrechtlich vertretbaren Löschfristen 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.

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

146. 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 Löschregeln

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

148. 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.

149. 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.

150. Eine Löschregel, die nur auf einen abstrakten Startzeitpunkt abstellt, wird abstrakte Löschregel genannt.

## 8.2 Matrix der Löschklassen

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

152. 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.

**Abbildung 4: Beispiel für eine Matrix mit Löschklassen (Toll Collect)**

| Startzeitpunkte | Standardfristen | | | | | | |
|---|---|---|---|---|---|---|---|
| | Sofort | 42 Tage | 120 Tage | 1 Jahr | 4 Jahre | 7 Jahre | 12 Jahre |
| Ab Erhebung | | | Mautdaten | Mautdaten mit bes. Analysebedarf | | | |
| Ab Ende Vorgang | nmF, Web-Logs | Kurzzeit-Doku., Betriebs-Logs | EFN, voll erstattete Reklamationen | Vorgänge ohne Dokupflicht | Rekla- und Forderungsdaten | Handelsbriefe | Buchhaltungsdaten |
| Ab Ende Beziehung | | | | ergänzende Stammdaten | | Verträge | Kernstammdaten. |

LEGENDE:
gelb unterlegt: Frist abgeleitet aus allgemeinen Gesetzen
blau unterlegt: Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
grün unterlegt: Frist frei gewählt

ABKÜRZUNGEN: nmF = Mautdaten nicht-mautpflichtiger Fahrzeuge; EFN = Einzelfahrtennachweis

153. 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.

## 8.3 Datenarten, Löschklassen und Löschregeln

154. Die Datenarten der verantwortlichen Stelle werden den Löschklassen zugeordnet. Jede Datenart mit einer Vorhaltefirst, die nicht einer der Standardlöschfristen entspricht, wird – wenn datenschutzrechtlich zulässig – in eine Löschklasse 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 Löschfrist festgelegt wird.

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

ANMERKUNG 2: Die Frist, während der eine Datenart nach der Vorhaltefirst 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.

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

> BEISPIELE: Für einen Reparaturauftrag könnte der Startzeitpunkt die „Übergabe des reparierten Gerätes an den Kunden“ sein. Für Buchungsdatensätze und die zugehörigen buchungsbegründenden 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.

156. Die Standardlöschfristen, Löschklassen und die Zuordnung der Datenarten sollten in einem eigenständigen Dokument „Regellöschfristen“ festgelegt werden. Die Löschregeln sollen technikneutral definiert werden. Es kann sinnvoll sein, 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.

157. Primäre Zielgruppen des Dokuments Regellöschfristen sind die für den Datenschutz verantwortlichen Mitarbeiter, die Projekt-Teams, die Umsetzungsvorgaben für Systeme entwickeln sowie fachliche Anwender, die die Löschregeln von Datenarten prüfen oder als Information benötigen.

| **Tabelle 1: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Regellöschfristen“** | |
|---|---|
| Pflegeverantwortung | Verantwortlicher für Datenschutz |
| Voraussetzungen für die Freigabe von Änderungen | Review durch die betroffenen Organisationseinheiten |
| datenschutzrechtliche Freigabe durch | Verantwortlichen für Datenschutz.<br>Für große Änderungen wird empfohlen, eine zusätzliche Freigabe der Geschäftsführung einzuholen. Dadurch erhalten die Löschregeln Geltung für die verantwortliche Stelle. |

# 9 Vorgaben für die Umsetzung von Löschregeln

## 9.1 Struktur und Inhalte der Umsetzungsvorgaben

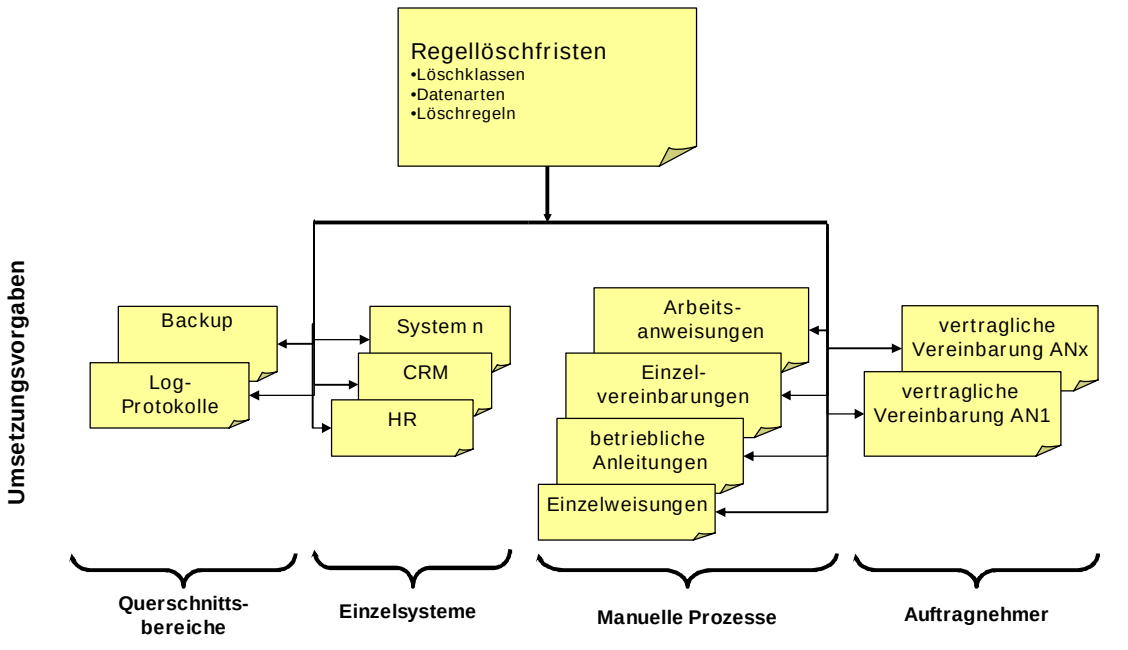
### 9.1.1 Verhältnis zwischen Regellöschfristen und Umsetzungsvorgaben

158. Das Dokument Regellöschfristen ist hinsichtlich der Löschregeln die Referenz für die Dokumente mit Umsetzungsvorgaben.

159. Die Löschregeln 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.

**Abbildung 5: Verhältnis zwischen Regellöschfristen und Umsetzungsvorgaben**




160. Die Gesamtheit der Umsetzungsvorgaben soll alle Bestände an pbD der verantwortlichen Stelle abdecken.

161. Die Umsetzungsvorgaben sollen in die Dokumentationsstruktur der verantwortlichen Stelle eingeordnet werden. In den weiteren Abschnitten dieses Kapitels werden Hinweise dazu und zur Verantwortung für die Pflege und die Freigabe der Umsetzungsempfehlungen gegeben.

### 9.1.2 Inhalt von Umsetzungsvorgaben

162. 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 Löschregel ist anzuwenden? Welche technischen Bedingungen bilden den Auslöser der Frist?
- Durch welchen Mechanismus wird die Löschung durchgeführt?
- Soweit Löschmechanismen konfigurierbar sind: Welche Parameter sind mit welchen Werten zu verwenden, um die zu löschenden Daten zu bestimmen?
- Wer ist für den Start und die Überwachung des Mechanismus verantwortlich?
- Wie ist die Durchführung von Löschmaßnahmen zu dokumentieren?

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

164. Es ist häufig nicht notwendig, die Vorhaltefrist der einzelnen Datenarten in jedem IT-System auszunutzen. Deshalb können den Umsetzungsvorgaben gegebenenfalls kürzere Löschfristen definiert werden, als nach den Regellöschfristen 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

165. Löschmaßnahmen müssen in Querschnittsbereichen umgesetzt werden. Oft können die Vorgaben einheitlich geregelt werden. Insbesondere für die folgenden Bereiche können einheitliche Regeln naheliegen.

166. 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 Löschfristen 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.

167. 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.

168. 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 Löschfristen 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.

169. 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.

170. Die Umsetzungsvorgaben für Querschnittsbereiche haben Richtliniencharakter. Sie sollten daher in die Richtlinien-Struktur der verantwortlichen Stelle eingeordnet werden.

171. Zielgruppe der Dokumente sind die für den jeweiligen Querschnittsbereich verantwortlichen Entscheidungsträger sowie die Mitarbeiter, die die Richtlinie umsetzen müssen.

| **Tabelle 2: Empfehlungen für Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Querschnittsbereiche“** | |
|---|---|
| Pflegeverantwortung | Verantwortlicher für Datenschutz (soweit keine Zuständigkeit anderer Organisationseinheiten besteht) |
| Voraussetzungen für die Freigabe von Änderungen | Review durch betroffene Organisationseinheiten |
| datenschutzrechtliche Freigabe durch | Verantwortlicher für Datenschutz. |

172. Es kann notwendig sein, dass nachgewiesen wird, welche Datenträger durch Löschen freigegeben und welche vernichtet wurden. Ergänzend zu den Umsetzungsvorgaben im Querschnittsbereich **„**Rückbau von Systemen“ ist es dann sinnvoll, ein „**Bestandsverzeichnis der Datenträger“** zu führen und die Dokumentation der Löschung oder Vernichtung vorzusehen:

| **Tabelle 3: Empfehlungen für Pflegeverantwortung „Bestandsverzeichnis der Datenträger“** | |
|---|---|
| Pflegeverantwortung für das Bestandsverzeichnis | für die Löschung bzw. Vernichtung der Datenträger verantwortliche Organisationseinheit |

## 9.3 Umsetzungsvorgaben für einzelne IT-Systeme

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

174. Die Umsetzungsvorgaben für einzelne IT-Systeme beschreiben, welche Löschmechanismen 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.

175. Es ist sinnvoll, in den Umsetzungsvorgaben für einzelne System 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 Löschfrist für eine Datenart gegenüber der Regellöschfrist 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 Löschmechanismus berücksichtigen.

176. Häufig werden durch einen Löschmechanismus 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.

BEISPIELE: 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.

177. Primäre Zielgruppe dieser Umsetzungsvorgaben sind die Administratoren sowie die Anwender, die die Prozesse gestalten, in denen die jeweiligen Datenbestände verwendet werden.

178. Es bietet sich an, die Umsetzungsvorgaben für einzelne IT-Systeme jeweils als eigenständiges Systemlöschkonzept zu dokumentieren. In diesem Fall können die Löschmechanismen unabhängig von anderen betrieblichen Anforderungen dargestellt werden. Es ist aber auch möglich, die entsprechenden Informationen in die System- und Betriebshandbücher der Systeme zu integrieren.

| **Tabelle 4: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für einzelne IT-Systeme“** | |
|---|---|
| Pflegeverantwortung | für das System betrieblich verantwortliche Organisationseinheit |
| Voraussetzungen für die Freigabe von Änderungen | Review durch weitere betroffene Organisationseinheiten |
| datenschutzrechtliche Freigabe durch | Verantwortlicher für Datenschutz. |

ANMERKUNG 1: Die Pflegeverantwortung sollte der betrieblich verantwortlichen Organisationseinheit zugewiesen werden, weil sie in einem geordneten IT-Management den besten Überblick über Änderungen am jeweiligen System hat. Sie kann außerdem Wechselwirkungen zwischen Umsetzungsvorgaben zur Löschung und anderen betrieblichen Abläufen bewerten. Schließlich muss die betrieblich verantwortliche Organisationseinheit dafür Sorge tragen, dass die freigegebenen Vorgaben auch umgesetzt werden.

ANMERKUNG 2: Andere Organisationseinheiten sollten verpflichtet werden, die betrieblich verantwortliche Organisationseinheit bei der Pflege zu unterstützen. Beispielsweise sollten die für die Systementwicklung und Systembeschaffung verantwortlichen Organisationseinheiten verpflichtet sein, die notwendigen Informationen bereitzustellen, die nach technischen Änderungen für die Pflege der Umsetzungsvorgabe benötigt werden.

ANMERKUNG 3: In den Review-Prozess müssen insbesondere die Anwender des jeweiligen Systems einbezogen werden, damit sie die fachlichen Auswirkungen von Löschregeln bewerten können.

ANMERKUNG 4: Die datenschutzrechtliche Freigabe muss durch den Verantwortlichen für Datenschutz erfolgen, damit er veränderte Umsetzungsvorgaben auf Konformität mit dem Datenschutz prüfen kann. Wenn die Umsetzungsvorgabe zum Löschen ein eigenständiges Dokument ist, lässt sich der Freigabeprozess in der Regel effizienter gestalten, als wenn die Umsetzungsvorgaben Teil eines System- oder Betriebshandbuchs sind.

## 9.4 Einzelmaßnahmen zur Löschung von Datenbeständen

### 9.4.1 Allgemeine Hinweise zu Umsetzungsvorgaben für Einzelmaßnahmen

179. 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 berücksichtig werden.

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

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

### 9.4.2 Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag

182. Für den allgemeinen Bürobetrieb können Löschregeln festgelegt werden, beispielsweise zur Behandlung von Dokumenten abgeschlossener Projekte oder für E-Mails. Diese Umsetzungsvorgaben sollten in ein bestehendes Mitarbeiterhandbuch integriert werden. Es ist sinnvoll, dort auch über sichere Entsorgungsmöglichkeiten für Dateien, Papierdokumente und Datenträger zu informieren.

183. Zielgruppe sind alle Mitarbeiter der verantwortlichen Stelle.

| **Tabelle 5: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag“** | |
|---|---|
| Pflegeverantwortung | Organisationseinheit mit Verantwortung für die Pflege des Mitarbeiterhandbuchs |
| Voraussetzungen für die Freigabe von Änderungen | gemäß der Regeln der verantwortlichen Stelle für dieses Mitarbeiterhandbuch |
| Freigabe durch | gemäß der Regeln der verantwortlichen Stelle für dieses Mitarbeiterhandbuch. Der Verantwortliche für Datenschutz ist an der Freigabe zu beteiligen |

### 9.4.3 Umsetzungsvorgaben für Datenbestände in manuellen Prozessen

184. Bestände mit pbD, die in regelmäßigen manuellen Prozessen verwendet werden, müssen ebenfalls innerhalb der Regellöschfristen gelöscht werden.

185. Es bietet sich an, die entsprechenden Arbeitsaufgaben in Arbeitsanweisungen festzulegen.

186. Zielgruppe der Arbeitsanweisung sind die jeweils am manuellen Prozess beteiligten Mitarbeiter und die Leiter der entsprechenden Organisationseinheiten.

| **Tabelle 6: Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Datenbestände in manuellen Prozessen“** | |
|---|---|
| Pflegeverantwortung | Organisationseinheit, die den jeweiligen manuellen Prozess verantwortet |
| Voraussetzungen für die Freigabe von Änderungen | Review durch die Organisationseinheiten, die am jeweiligen manuellen Prozess beteiligt ist bzw. die Ergebnisse abnimmt |
| Freigabe durch | Organisationseinheit, die den jeweiligen manuellen Prozess verantwortet. Der Verantwortliche für Datenschutz ist an der Freigabe zu beteiligen, wenn Löschregeln betroffen sind. |

### 9.4.4 Umsetzungsvorgaben für Datenabzüge für Sonderverwendungen

187. 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 dem Verantwortlichen für den Datenschutz vereinbart wurde.

188. Es bietet sich an, die entsprechenden Aufgaben für die Löschung in Einzelvereinbarungen mit dem Verantwortlichen für Datenschutz festzulegen. Die Vereinbarungen können z. B. im Rahmen eines vorhandenen Change-Managements erstellt und abgearbeitet werden.

189. Zielgruppe der jeweiligen Vereinbarungen sind die an der Durchführung der Sonderverwendung beteiligten Mitarbeiter sowie der Leiter der verantwortlichen Organisationseinheit.

| **Tabelle 7: Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Datenabzüge für Sonderverwendungen“** | |
|---|---|
| Pflegeverantwortung | Organisationseinheit, die die Sonderverwendung beantragt |
| Voraussetzungen für die Freigabe von Datenabzügen | Review durch die Organisationseinheiten, die verantwortlich für die Daten sind (Daten-Owner, fachliche Anwender), durch die Organisationseinheiten, die an der Sonderverwendung beteiligt sind, sowie ggf. die Organisationseinheiten für IT-Betrieb und Informationssicherheit |
| datenschutzrechtliche Freigabe durch | Verantwortlicher für Datenschutz |

190. Es ist sinnvoll, für die Nachverfolgung von Ausnahmeregelungen für Umsetzungsvorgaben oder Datenabzüge eine Übersicht über diese Fälle zu führen. Die Rückkehr zum Regelbetrieb oder die Löschung der Datenabzüge kann in dieser Übersicht nach einer entsprechen-

den Rückmeldung der jeweils verantwortlichen Organisationseinheit dokumentiert werden.

| Tabelle 8: Empfehlungen für Pflegeverantwortung und Freigaberegeln „Übersicht über Ausnahmeregelungen“ | |
|---|---|
| Pflegeverantwortung | Verantwortlicher für Datenschutz |
| Voraussetzungen für den jeweiligen Rückbau-Vermerk | entsprechende Rückmeldung von der verantwortlichen Organisationseinheit |
| Freigabe durch | nicht erforderlich |

### 9.4.5 Umsetzungsvorgaben für Restbestände in IT-Systemen

191. Die Umsetzungsvorgaben für Querschnittsbereiche und für die einzelnen IT-Systeme decken die automatisierte Regelverarbeitung ab. Die dort festgelegten Mechanismen erfassen aber möglicherweise nicht alle pbD, die zu löschen sind. Die verantwortliche Stelle muss daher sicherstellen, 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.

192. Das Löschkonzept sollte regeln, wer für die Identifikation und Löschung solcher Datenbestände verantwortlich ist.

193. Es bietet sich an, identifizierte Bestände in betrieblichen Prozessen zu löschen. Die Umsetzungsvorgaben, die regelmäßig durchgeführt werden müssen, könnten in entsprechenden betrieblichen Arbeitsanleitungen getroffen werden. Einmalige Arbeiten können z. B. im Rahmen eines vorhandenen Change-Managements festgelegt und abgearbeitet werden.

194. Im Regelfall sollte für diese Datenbestände geklärt sein, dass sie zu löschen sind. Primäre Zielgruppe der betrieblichen Arbeitsanleitungen sind daher die betrieblich verantwortlichen Mitarbeiter. Wenn Unsicherheit über die fachliche Verwendung der Restbestände besteht, kann es notwendig sein, die anwendenden Organisationseinheiten in einen Review-Prozess einzubinden.

| Tabelle 9: Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Restbestände in IT-Systemen“ | |
|---|---|
| Pflegeverantwortung | für die Löschung verantwortliche Organisationseinheit |
| Voraussetzungen für die Freigabe von Änderungen | ggf. Review durch die betroffenen Organisationseinheiten |
| datenschutzrechtliche Freigabe durch | Verantwortlicher für Datenschutz |

### 9.4.6 Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten

195. Wenn festgestellt wird, dass Bestände mit pbD nach den einschlägigen Rechtsvorschriften durch die verantwortliche Stelle unzulässigerweise gespeichert werden, sind diese zu löschen. Im Regelfall sind unverzüglich betriebliche Löschmaßnahmen zu ergreifen. Wenn ein Betroffener ein Löschbegehren für Datenobjekte stellt, die sich auf ihn beziehen, und diese unzulässigerweise gespeichert sind, sind diese ebenfalls zu löschen.

196. Die eingesetzten IT-Systeme und Prozesse müssen die Möglichkeit bieten, dass nach einer entsprechenden Mitteilung des Verantwortlichen für den Datenschutz die Löschung unverzüglich umgesetzt wird. Nach der Mitteilung könnten die Umsetzungsvorgaben in betrieblichen Einzelweisungen gegeben werden, z. B. durch den Daten-Owner. Die Weisungen können z. B. im Rahmen eines vorhandenen Change-Managements erstellt und abgearbeitet werden.

197. Primäre Zielgruppe der betrieblichen Einzelweisungen sind die betrieblich verantwortlichen Mitarbeiter.

| **Tabelle 10: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“** | |
|---|---|
| Pflegeverantwortung | Vorgabe für die Einzelweisung: Verantwortlicher für Datenschutz<br>Steuerung der betrieblichen Umsetzung: Organisationseinheit mit Verantwortung für den unzulässigen Datenbestand |
| Voraussetzungen für die Freigabe von Änderungen | entfällt, da rechtlich unzulässiger Datenbestand und gesetzliche Löschpflicht |
| datenschutzrechtliche Freigabe durch | implizit durch die Mitteilung des Verantwortlichen für Datenschutz an den Prozessverantwortlichen für die Löschung. |

## 9.5 Umsetzungsvorgaben für Auftragnehmer

198. Die verantwortliche Stelle muss auch sicherstellen, dass die Regellöschfristen auch für ihre Datenbestände eingehalten werden, die bei Auftragnehmern verarbeitet werden.

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

200. Zielgruppe dieser Umsetzungsvorgaben sind die für die Umsetzung beim Auftragnehmer verantwortlichen Mitarbeiter.

| **Tabelle 11: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Auftragnehmer“** | |
|---|---|
| Pflegeverantwortung | Vertragliche Vereinbarungen: die für Vertragsgestaltungen bei der verantwortlichen Stelle zuständige/n Organisationseinheit/en, z.B. Recht, Einkauf<br>Einzelweisungen: für die Steuerung des Auftragnehmers verantwortliche Organisationseinheit der verantwortlichen Stelle |
| Voraussetzungen für die Freigabe von Änderungen | ggf. Review durch weitere betroffene Organisationseinheiten oder den Verantwortlichen für Datenschutz. |

| Tabelle 11: Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Auftragnehmer“ | |
|---|---|
| Freigabe durch | in Sonderfällen: verantwortliche Organisationseinheit nach Rücksprache mit dem Verantwortlichen für Datenschutz. |

# 10 Management-System: Verantwortung und Prozesse für das Löschen von personenbezogenen Daten

## 10.1 Allgemeine Einbettung in ein Management-System

201. Im Löschkonzept der verantwortlichen Stelle 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.

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

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

204. Durch die Festlegungen für das Löschkonzept oder seine Umsetzung können Organisationseinheiten betroffen sein, die pbD für ihre Geschäftsprozesse verwenden. Sie müssen an der Gestaltung geeignet beteiligt werden, z. B. in Form von Review-Aufforderungen.

## 10.2 Rolle des Verantwortlichen für Datenschutz

### 10.2.1 Pflegeverantwortung für Dokumente

205. Er wird empfohlen, folgende Verantwortung beim Verantwortlichen für Datenschutz anzusiedeln:

- Pflege des Dokuments „Löschkonzept“
  Auslöser für Änderungen sind Entscheidungen der verantwortlichen Stelle, Verantwortung oder Dokumentationsstruktur des Löschkonzepts anzupassen.
- Pflege des Dokuments „Regellöschfristen“
  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 der Dokumente mit Umsetzungsvorgaben für Querschnittsbereiche
  Auslöser für Änderungen sind Änderungen betrieblicher Anforderungen oder Prozesse.

206. Für die genannten Dokumente ist der jeweilige Änderungs- und Freigabeprozess festzulegen.

### 10.2.2 Weitere Prozesse beim Verantwortlichen für Datenschutz

207. Der Verantwortliche für Datenschutz soll außerdem Eigentümer der folgenden Prozesse sein:

- **Löschen von unzulässigen Bestände mit pbD** (Abschnitt 9.4.6). Für den Prozess ist festzulegen, wie der Verantwortliche für Datenschutz die Löschung unzulässig erhobener oder gespeicherter pbD veranlassen kann. Es sollte festgelegt werden, welche Organisationseinheit die Löschung umsetzen muss und dass sie dem Verantwortlichen für Datenschutz über den Vollzug berichtet.
- **Datenschutz-Audit für Löschmaßnahmen**. Für den Prozess ist festzulegen, wie die Planung und die Durchführung von Datenschutz-Audits erfolgen sollen. Es wird empfohlen, dem Verantwortlichen für Datenschutz auch das Recht einzuräumen, die jeweils für die Umsetzungsvorgaben verantwortliche Organisationseinheit aufzufordern, ein Audit durchzuführen und über das Ergebnis zu berichten.

  ANMERKUNG: Aus den in den Umsetzungsvorgaben geforderten Angaben lassen sich auf einfache Weise Prüfbedingungen für Audits ableiten.

### 10.2.3 Freigabe-Beteiligungen

208. Der Verantwortliche für Datenschutz muss an der Freigabe der folgenden Dokumente beteiligt sein:

- Umsetzungsvorgaben für Löschmaßnahmen (siehe Kap. 9). Es wird empfohlen, die Erstellungs- und Pflegeprozesse für die jeweiligen Umsetzungsvorgaben in vorhandene Prozesse einzubetten, z. B. Betrieb, Change-Management und Einkauf.
  Die Prozesse müssen sicherstellen, dass der Verantwortliche für Datenschutz neuen Dokumenten und relevanten Änderungen zustimmen muss.
- Anforderungsdokumente für Systembeschaffungen und Systementwicklungsprojekte. Die Erstellungs- und Pflegeprozesse müssen sicherstellen, dass der Verantwortliche für Datenschutz prüfen kann,
  - ob pbD im jeweiligen System verwendet und deshalb Löschmechanismen realisiert werden müssen,
  - ob die in den Anforderungen definierten Löschmechanismen ausreichend sind und den Löschregeln entsprechen und
  - ob gegebenenfalls gefordert werden muss, dass Löschungen im Einzelfall möglich sind (Abschnitt 9.4.6).

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

## 10.3 Verantwortung und Prozesse im Zusammenhang mit Umsetzungsvorgaben

### 10.3.1 Organisationseinheiten mit Verantwortung für Bestände mit personenbezogenen Daten

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

- Umsetzungsvorgaben der Löschregeln für den jeweiligen Datenbestand mit dem Verantwortlichen für Datenschutz 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 den Verantwortlichen für Datenschutz in die Freigabe einzubinden.

### 10.3.2 Weitere Aufgaben im Zusammenhang mit Umsetzungsvorgaben

210. Die verantwortliche Stelle soll sicherstellen, dass jeder Bestand mit pbD geeigneten Umsetzungsvorgaben unterliegt. Um die Datenbestände den Verantwortlichen zuzuordnen, benötigt die verantwortliche Stelle eine **Liste der IT-Systeme und anderer Datenbestände**. Unter andere Datenbestände können z. B. manuell oder bei Auftragnehmern geführte Datenbestände fallen. Diese Liste und die Zuordnung der Verantwortlichen muss gepflegt werden.

| **Tabelle 12: Empfehlungen für die Pflegeverantwortung der „Übersicht über IT-Systeme und andere Bestände mit pbD“** | |
|---|---|
| Pflegeverantwortung | Organisationseinheit, die den IT-Betrieb steuert |
| Aufnahme von Ergänzungen und Änderungen | bspw. im Zusammenhang mit Release-Planungen oder aus sonstigen Hinweisen |
| Freigabe durch | nicht erforderlich |

211. In manchen Fällen können Löschmaßnahmen nicht sofort realisiert werden, beispielsweise weil eine Fehlerbehebung oder eine Weiterentwicklung eines IT-Systems notwendig ist. Die verantwortliche Stelle muss einen Überblick über solche **Handlungsbedarfe** haben, damit sie diese priorisieren und nachverfolgen kann. Dazu muss entschieden werden, ob die Handlungsbedarfe in den jeweiligen Umsetzungsvorgaben ausgewiesen oder an einer Stelle gesammelt werden.

| Tabelle 13: Empfehlungen für die Pflegeverantwortung der „Handlungsbedarfe aus Umsetzungsvorgaben“ | |
|---|---|
| Pflegeverantwortung | ENTWEDER:<br>• Pflege der detaillierten Handlungsbedarfe in den Umsetzungsvorgaben durch die für den Datenbestand verantwortliche Organisationseinheit und<br>• Pflege einer Übersichtsliste, die auf die entsprechenden Umsetzungsvorgaben verweist; die Verantwortung für die Pflege ist zuzuweisen.<br>ODER<br>• Pflege der detaillierten Handlungsbedarfe in einer Gesamtliste; die Verantwortung für die Pflege ist zuzuweisen. |
| Aufnahme von Handlungsbedarfen | insbesondere im Zusammenhang mit den Freigabeprozessen für Umsetzungsvorgaben aus Kapitel 9. |
| Vermerk über Erledigung von Handlungsbedarfen | nach Bestätigung durch die verantwortliche Organisationseinheit, dass der Handlungsbedarf erledigt wurde |

ANMERKUNG: Der Verantwortliche für Datenschutz sollte über die Aufnahme und Erledigung von Handlungsbedarfen informiert werden.

### 10.3.3 Organisationseinheit Change-Management

212. Die Veränderungen im IT-Betrieb und betriebliche Aufgaben aus besonderem Anlass sollten bei der verantwortlichen Stelle durch ein Change-Management gesteuert werden.

213. Die für das Change-Management verantwortliche Organisationseinheit muss sicherstellen, dass der Verantwortliche für Datenschutz zur datenschutzrechtlichen Freigabe von Aktivitäten aufgefordert wird, die zur Aussetzung der Löschung von pbD führen oder besondere Aktivitäten zum Löschen von pbD erfordern. Letzteres ist beispielsweise der Fall, wenn Kopien von Datenbeständen außerhalb von Regelprozessen verwendet werden sollen.

214. Die Prozesse des Change-Managements sind entsprechend anzupassen.

### 10.3.4 Organisationseinheiten mit Verantwortung zur Steuerung von Auftragnehmern

215. Die Verantwortung für die Steuerung von Auftragnehmern sollte in der verantwortlichen Stelle eindeutig zugewiesen sein.

216. Die für die Verträge mit Auftragnehmern verantwortlichen Organisationseinheiten müssen sicherstellen, dass neben anderem auch die Umsetzung von Löschmaßnahmen vertragliche vereinbart wird.

217. Die für die Steuerung von Auftragnehmern verantwortlichen Organisationseinheiten müssen sicherstellen, dass die vertraglichen Regelungen und weitere Weisungen beim Auftragnehmer umgesetzt werden.

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

# 11 Bibliographie


| | |
|---|---|
| [CSEC 2006] | Communications Security Establishment Canada (2006): Clearing and Declassifying Electronic Data Storage Devices (ITSG-06), Communications Security Establishment Canada (CSEC), 2006 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg06-eng.pdf). |
| [ISO/IEC 29001] | ISO/IEC 29100 - International Organization for Standardization / International Electrotechnical Commission (2011): ISO/IEC 29100 - Information technology - Security techniques - Privacy framework, ISO/IEC, 2011. |
| [ISO/IEC N11279] | ISO/IEC JTC 1/SC 27/WG 5: Terms of Reference – Study Period on documentation of data deletion principles for personally identifiable information |
| [ISO/IEC N11686] | ISO/IEC JTC 1/SC 27/WG 5: Report on ToR N11279 – SP: Concept for Deletion of PII |
| [ISO/IEC N11750] | ISO/IEC JTC 1/SC 27/WG 5: Meeting report for WG 5 Study Period on Data deletion principles for personally identifiable information in organizations |
| [NIST SP 800-88] | NIST SP 800-88 - National Institute of Standards and Technology (2006): NIST Special Publication 800-88 - Guidelines for Media Sanitization, National Institute of Standards and Technology, Gaithersburg, USA, 2006 (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf; Stand: 30.07.2012). |
| [Fraenkel/ Hammer 2007] | Fraenkel, R. / Hammer, V. (2007): Rechtliche Löschvorschriften, DuD 12/2007, 899 ff. |
| [Hammer/ Fraenkel 2007] | Hammer, V. / Fraenkel, R. (2007): Löschkonzept, DuD 12/2007, 905 ff. |
| [Hammer/ Fraenkel 2011] | Hammer, V. / Fraenkel, R. (2011): Löschklassen - standardisierte Fristen für die Löschung personenbezogener Daten, DuD 12/2011, 890 ff. |


# 12 Hinweise für die Weiterarbeit an einem internationalen Standard

219. Dieser Text stellt eine Leitlinie vor, die als Grundlage für eine Weiterentwicklung zu einem Standard dienen kann. In den Diskussionen über den Entwurf entstanden Anregungen, die für die weitere Arbeit in einem Standardisierungsprojekt relevant sein können. Folgende Hinweise wurden in dieser Dokumentversion noch nicht berücksichtigt:

- Je nach Ausrichtung eines Standards ist zu prüfen, welche Textabschnitte als normative Vorgabe (MUSS) oder als Empfehlung (SOLLTE/KANN) zu formulieren sind.
- Es sollte geprüft werden, ob für die Leitlinie der Grundsatz der Erforderlichkeit aus dem Datenschutzrecht vorausgesetzt werden soll oder vorausgesetzt werden muss. Verantwortliche Stellen, deren Datenbestände nicht dem Grundsatz der Erforderlichkeit unterliegen, wären dann nicht Teil der primären Zielgruppe.
- Es sollte geprüft werden, ob inhaltliche Bezüge zu Standards aus den Bereichen Records Management (ISO TC 46/SC11) und Document Management (ISO TC 171) bestehen.
- Der abstrakte Startzeitpunkt „Ende der Beziehung zum Betroffenen“ ist möglicherweise auch ein spezieller Statuswechsel im Identity Management. Es sollte geprüft werden, ob sich daraus Bezüge zu Standards des Identity Managements ergeben.

- Gegebenenfalls ist zu berücksichtigen, dass es nicht in jeder Organisation einen Verantwortlichen für Datenschutz gibt und dass auch verantwortliche Stellen ohne einen solchen ein Löschkonzept etablieren können und sollen.
- Die Definition des Begriffs „Löschen“ sollte mit bestehenden Standards abgeglichen werden, z. B. DIN 33858 und 32757, ISO 12036, 12037, IT Grundschutzkataloge, § 303a StGB.
- Möglicherweise sollten Grafiken oder Beispiele im Text für einen Standard abstrakt gestaltet werden, z. B. die Grafiken für die Vorhaltefrist und Regellöschfrist und die Matrix der Löschklassen. Konkrete Beispiele wären dann eventuell in einen Anhang zu verlagern.
- Es muss sprachlich klargestellt sein, dass der Verantwortliche für den Datenschutz nicht für die Einhaltung des Datenschutzes verantwortlich ist.

# 13 Workshops, Konferenzen und Unterstützung

220. Diese Leitlinie ist wesentlich auch durch die Vorarbeiten bei Toll Collect (vgl. [Fraenkel/ Hammer 2007], [Hammer/ Fraenkel 2007], [Hammer/ Fraenkel 2011]) und durch den inhaltlichen Austausch mit Gesprächspartnern zustande gekommen. Das Projektteam bedankt sich bei allen Gesprächspartnern für die intensiven und fruchtbaren Diskussionen! Die Toll Collect GmbH stellte die Räumlichkeiten für die Durchführung der Projekt-Workshops zur Verfügung. Vielen Dank!

221. Wir bedanken uns auch bei Herrn Grahle und Herrn Uhlherr vom DIN für die stets konstruktive und hilfreiche Unterstützung zu Fragen der Gestaltung von Standards und zur Projektabwicklung.

## 13.1 Workshops des DIN/INS-Projekts

### 13.1.1 Kickoff-Workshop

222. Die Bausteine und der Gliederungsaufbau der Leitlinie wurden am 28. Juni 2012 in den Räumen der Toll Collect GmbH in Berlin in einem Kickoff-Workshop diskutiert. Teilnehmer des Workshops waren:

| | |
|---|---|
| Herr Manuel Cebulla | TÜV Informationstechnik GmbH |
| Herr Walter Ernestus | Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit |
| Herr Hanno Fischer | Blancco GmbH |
| Herr Reinhard Fraenkel | Toll Collect GmbH |
| Herr Christian Graf von der Schulenburg | Verlagsgesellschaft Madsack GmbH & Co. KG |
| Herr Roman Grahle | DIN e.V. |
| Frau Ljerka Grahovac | Deutsche Bahn AG |

| | |
|---|---|
| Frau Michaela Luncke | Toll Collect GmbH |
| Frau Chris Newiger | Deutsche Bahn AG |
| Herr Hermann-Josef Schwab | SAP AG |
| Herr Martin Uhlherr | DIN e.V. |
| Herr Carsten Welp | Deutsche Post Adress GmbH |

### 13.1.2 Review-Workshop

223. Der Entwurf der Leitlinie wurde am 16. Oktober 2012 in den Räumen der Toll Collect GmbH in Berlin in einem Review-Workshop diskutiert. Teilnehmer des Workshops waren:

| | |
|---|---|
| Herr Bernd-Rainer Boschek | Daimler AG |
| Herr Reinhard Fraenkel | Toll Collect GmbH |
| Herr Christian Graf von der Schulenburg | Verlagsgesellschaft Madsack GmbH & Co. KG |
| Frau Ljerka Grahovac | Deutsche Bahn AG |
| Frau Michaela Luncke | Toll Collect GmbH |
| Herr Jan Schallaböck | Unabhängiges Landeszentrums für Datenschutz Schleswig-Holstein |
| Herr Hermann-Josef Schwab | SAP AG |
| Herr Martin Uhlherr | DIN e.V. |
| Herr Dr. Stefan Weiß | Swiss Reinsurance Company Ltd. |
| Herr Carsten Welp | Deutsche Post Adress GmbH |

224. Die Teilnehmer des Review-Workshops stellten fest, dass die hier vorgestellte Leitlinie als Ausgangspunkt für ein internationales Standardisierungsprojekt gut geeignet ist.

225. Wertvolle Kommentare zur Review-Fassung erhielten wir außerdem von Herrn Manuel Cebulla (TÜV Informationstechnik GmbH).

## 13.2 ISO/IEC Study Period

226. Parallel zum DIN/INS-Projekt war von Vertretern des DIN in der ISO/IEC JTC 1/SC 27/WG 5 eine „Study Period on documentation of data deletion principles for personally identifiable information“ etabliert worden ([ISO/IEC N11279]). Dr. Volker Hammer von Secorvo übernahm die Rolle des Rapporteurs. Der Report basierte wesentlich auf den Ergebnissen des DIN/INS-Projekts und wurde im Oktober 2012 vorgestellt ([ISO/IEC N11686], [ISO/IEC N11750]).

| Termin und Ort | Veranstaltung |
|---|---|

| | |
|---|---|
| 25. Oktober 2012, Rom | 14th meeting of ISO/IEC JTC 1/SC 27/WG 5: Report on “Study Period on a concept for deletion of personal data by which organisations can support implementation of the respective privacy principles of ISO/IEC 29100 Privacy Framework on Documentation of data deletion for PII in organizations” |

In der WG 5 stieß die vorgestellte Vorgehensweise auf großes Interesse. Die Study Period wurde um 6 Monate verlängert. Es bestehen daher sehr gute Chancen, dass bei ISO/IEC ein internationales Standardisierungsprojekt zum Thema „Leitlinie für ein Löschkonzept für personenbezogene Daten“ aufgesetzt werden kann. Voraussetzung ist allerdings, dass die Ressourcen für einen Editor zur Verfügung stehen.

Herzlichen Dank an Prof. Kai Rannenberg (Goethe Universität Frankfurt) und Herrn Jan Schallaböck (Unabhängiges Landeszentrums für Datenschutz Schleswig-Holstein) für die konstruktive und unkomplizierte Unterstützung bei den Arbeiten während der Study Period.

## 13.3 Weitere Präsentationen

Das Thema des Projekts und die in der Leitlinie vorgeschlagene Vorgehensweise wurden außerdem in den folgenden Workshops vorgestellt:

| Termin und Ort | Veranstaltung |
|---|---|
| 21. August 2012, Berlin | Gemeinsamer Workshop des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und des DIN e.V. "Entwicklung von Datenschutznormen insbesondere in ISO/IEC JTC 1/SC 27/WG 5 Information Technologies – Security Techniques – Identity management and privacy technologies“ |
| 22. August 2012, Berlin | Sitzung des DIN NIA 27-AK-05 |