

DIN 66398**DIN**

ICS 35.020; 03.160

Einsprüche bis 2015-05-09

Entwurf

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

Guideline for development of a concept for data deletion of personal identifiable information with derivation of deletion periods

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-01-09 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 52 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

Seite

Vorwort	5
Einleitung.....	6
1 Anwendungsbereich	8
2 Begriffe	8
3 Abkürzungen	11
4 Grundlagen eines Löschkonzepts	11
4.1 Allgemeines	11
4.2 Anwendung einschlägiger datenschutzrechtlicher Vorschriften	12
4.3 Was bedeutet „Löschen“?	13
4.4 Für jede Datenart eine Löschregel	14
4.4.1 Datenarten	14
4.4.2 Löschregeln	14
4.4.3 Vorhaltefrist und Regellöschfrist	14
4.4.4 Behandlung nicht-produktiver Datenbestände: Archive und Sicherungskopien	16
4.4.5 Standardlöschfristen, Startzeitpunkte, Löschregeln und Löschklassen	17
4.4.6 Löschen in Sondersituationen	17
4.5 Dokumentenstruktur im Löschkonzept	18
5 Datenarten bilden.....	18
5.1 Datenbestände, Zwecke und Datenarten	18
5.2 Datenarten systematisch erfassen	19
5.3 Gestaltungskriterien für die Bildung von Datenarten	19
5.3.1 Hinweise aus der Praxis	19
5.3.2 Orientierung an Rechtsvorgaben	19
5.3.3 Orientierung an Verwendungszwecken	19
5.3.4 Orientierung an der Sensitivität von Daten	20
6 Löschfristen festlegen	20
6.1 Standardlöschfristen verwenden	20
6.2 Fristfestlegungen	21
6.2.1 Übersicht über die Vorgehensweisen zur Fristdefinition	21
6.2.2 Unmittelbare Fristen aus Rechtsvorschriften	22
6.2.3 Fristfestlegung nach Prozessanalyse	22
6.2.4 Ableitung von Löschfristen nach einfachen Kriterien	22
6.3 Besonderheiten für Fristfestlegungen	23
6.3.1 Regellöschfristen und Abweichungen	23
6.3.2 Friständerungen durch Verdichtung mit Wechsel der Datenart	23
6.3.3 Wechsel der Datenart für Sonderfälle	24
6.3.4 Ausnahmen von Regelprozessen: Aussetzung der Löschung	24
6.3.5 Abweichungen von Standardlöschfristen für Sicherungskopien	24
7 Löschklassen	25
7.1 Abstrakte Startzeitpunkte – abstrakte Löschregeln	25
7.2 Matrix der Löschklassen	25
7.3 Datenarten, Löschklassen und Löschregeln	26
8 Vorgaben für die Umsetzung von Löschregeln	27
8.1 Struktur und Inhalte der Umsetzungsvorgaben	27
8.1.1 Verhältnis zwischen Regellöschfristen und Umsetzungsvorgaben	27
8.1.2 Inhalt von Umsetzungsvorgaben	28
8.2 Umsetzungsvorgaben für Querschnittsbereiche	30

8.3	Umsetzungsvorgaben für einzelne IT-Systeme	32
8.4	Einzelmaßnahmen zur Löschung von Datenbeständen.....	33
8.4.1	Allgemeine Hinweise zu Umsetzungsvorgaben für Einzelmaßnahmen	33
8.4.2	Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag	33
8.4.3	Umsetzungsvorgaben für Datenbestände in regelmäßigen manuellen Prozessen	34
8.4.4	Umsetzungsvorgaben für Kopien personenbezogener Daten für Sonderverwendungen	35
8.4.5	Umsetzungsvorgaben für Restbestände in IT-Systemen.....	36
8.4.6	Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten	36
8.5	Umsetzungsvorgaben für Auftragnehmer	37
9	Aufbau- und Ablauforganisation: Verantwortung und Prozesse für das Löschen von personenbezogenen Daten	38
9.1	Organisatorische Einbettung	38
9.2	Leitung der Organisation.....	39
9.3	Rolle des Ansprechpartners für Datenschutz	39
9.3.1	Pflegeverantwortung für Dokumente	39
9.3.2	Prozesse beim Ansprechpartner für Datenschutz	39
9.3.3	Freigabe-Beteiligungen.....	39
9.4	Verantwortung für Umsetzungsvorgaben.....	40
9.4.1	Organisationseinheiten mit Verantwortung für Bestände mit personenbezogenen Daten.....	40
9.4.2	Weitere Aufgaben im Zusammenhang mit Umsetzungsvorgaben.....	41
9.4.3	Organisationseinheit Change-Management	42
9.4.4	Organisationseinheiten mit Verantwortung zur Steuerung von Auftragnehmern.....	42
9.5	Allgemeine Meldepflichten	43
	Anhang A (informativ) Hinweise für ein Projekt „Löschkonzept“	44
	Anhang B (informativ) Hinweise zur Anonymisierung personenbezogener Daten.....	46
	Anhang C (informativ) Hinweise zu Vorgaben für die Sicherheit von Löschmechanismen	48
	Anhang D (informativ) Hinweise zur Sperrung von Datenbeständen	50
	Literaturhinweise	52

Tabellen

Tabelle 1 — Verwendete Abkürzungen	11
Tabelle 2 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der Dokuments „Regellöschfristen“	27
Tabelle 3 — Empfehlungen für Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Querschnittsbereiche“	31
Tabelle 4 — Empfehlungen für Pflegeverantwortung „Bestandsverzeichnis der Datenträger“	31
Tabelle 5 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für einzelne IT-Systeme“	33
Tabelle 6 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Datenobjekte im Arbeitsalltag	34
Tabelle 7 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Datenbestände in regelmäßigen manuellen Prozessen	34
Tabelle 8 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Kopien personenbezogener Daten für Sonderverwendungen“	35
Tabelle 9 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Übersicht über Ausnahmeregelungen“	35
Tabelle 10 — Empfehlungen für Pflegeverantwortung und Freigaberegeln „Umsetzungsvorgaben für Restbestände in IT-Systemen“	36

Tabelle 11 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für unzulässige Bestände mit personenbezogenen Daten“	37
Tabelle 12 — Empfehlungen für die Pflegeverantwortung und Freigaberegeln der „Umsetzungsvorgaben für Auftragnehmer“	38
Tabelle 13 — Empfehlungen für die Pflegeverantwortung der „Übersicht über IT-Systeme und andere Bestände mit pbD“	41
Tabelle 14 — Empfehlungen für die Pflegeverantwortung der „Handlungsbedarfe aus Umsetzungsvorgaben“	42

Bilder

Bild 1 — Beispiel für Fristabschnitte für einen Auftrag im Löschkonzept	15
Bild 2 — Mögliche Standardlöschfristen eines TK-Dienstleisters	23
Bild 3 — Beispielhafte Matrix von Löschklassen für einen TK-Dienstleister	26
Bild 4 — Verhältnis zwischen Regellöschfristen und Umsetzungsvorgaben	28
Bild A.1 — Aufteilung in Projektphasen	45

Vorwort

Dieses Dokument wurde vom DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. Das DIN sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Einleitung

In sehr vielen Geschäftsprozessen und IT-Anwendungen werden personenbezogene Daten (pbD) verwendet. Sie unterliegen 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 vorsehen. So enthält Artikel 6 der EU-Datenschutzrichtlinie von 1995 [RiLi 95/46/EG] eine Löscho- und Anonymisierungsvorgabe. Sie war in allen nationalen Datenschutzgesetzen der EU-Länder umzusetzen.

Wenn einschlägige datenschutzrechtliche Vorschriften 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.

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

- es notwendig ist, unbestimmte Rechtsbegriffe auszulegen, um Löschregeln zu bilden;
- es verantwortlichen Stellen schwerfällt, für Datenbestände das Ende der Verwendung in Prozessen und damit konkrete Löschfristen festzulegen;
- viele Personen daran beteiligt sind, die Löschregeln festzulegen und die Löschrmechanismen in IT-Systemen und anderen Abläufen zu implementieren, und die Beteiligten dies nur können, wenn sie die Löschregeln verstehen; oder
- es an klaren Vorstellungen fehlt, wie die korrekte Umsetzung der Löschregeln überprüft und gegebenenfalls nachgewiesen werden kann.

Um eine rechtskonforme Löschung von pbD sicherzustellen, ist es in der Praxis für die verantwortliche Stelle unabdingbar, ein Regelwerk zu entwickeln und Verantwortung zuzuweisen. Die Etablierung eines solchen Löschkonzepts ist eine komplexe und umfangreiche Aufgabe. Die Erfolgsaussichten für dessen Entwicklung können verbessert werden, wenn die verantwortliche Stelle auf einen bewährten Vorschlag zur Vorgehensweise und zur Gestaltung zurückgreifen kann.

In dieser Norm wird eine Vorgehensweise für die Entwicklung und Etablierung eines Löschkonzepts vorgeschlagen. Der Vorgehensweise liegt die Annahme zugrunde, dass die durchgängige Löschung von pbD einen tragfähigen Kompromiss zwischen rechtlichen Vorgaben und praktischen Anforderungen erfordert.

Grundlegende Datenschutzkenntnisse werden bei Anwendern dieser Norm vorausgesetzt.

Ziele dieser Norm

Diese Norm unterstützt verantwortliche Stellen dabei, ihre rechtlichen Pflichten zur Löschung personenbezogener Daten zu erfüllen. Als Leitlinie gibt sie Empfehlungen für die Inhalte, den Aufbau und die Zuordnung von Verantwortung in einem Löschkonzept für pbD. Die Vorgehensweise und die Strukturierungsvorschläge sind für alle verantwortlichen Stellen geeignet.

Diese Norm richtet sich an Personen, die datenschutzrechtliche Löschkonzepte entwickeln, z. B. Projektverantwortliche oder den Ansprechpartner für Datenschutz.

Löschklassen

Ein Löschkonzept kann nur dann mit akzeptablem Aufwand etabliert werden, wenn alle Beteiligten die Löschregeln nachvollziehen können und die Komplexität der Regeln überschaubar bleibt. Einfache Regeln sind daher der Schlüssel zum Erfolg. Diese Norm empfiehlt aus diesem Grund die Verwendung standardisierter Löschrufen und sogenannter Löschklassen, die gegebenenfalls organisationspezifisch angepasst werden. Diese Löschklassen reduzieren die Komplexität und bilden den Kern des Löschkonzepts. Durch die Einordnung personenbezogener Daten in Löschklassen werden ihnen implizit Löschregeln zugeordnet.

Nutzen

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 personenbezogener Daten zu erfüllen.
- Die Umsetzung von Löschrufen erfordert, dass Geschäftsprozesse hinreichend geklärt werden. Komplexe Abläufe können oftmals effizienter gestaltet werden.
- Die Datenhaltung wird systematisiert und konsolidiert. Weil auch Altbestände in die Löschung einbezogen werden sollten, werden diese Bestände bereinigt. Dies reduziert den Aufwand und die Kosten für die Datenmigration bei Systemwechseln erheblich.
- 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 Erhebung der Bestände mit pbD und der verbundenen Löschrufen erhält der Ansprechpartner für Datenschutz wertvolle Detailinformationen zur Systemdokumentation.
- Die Diskussion um Löschregeln und die konstruktive Gestaltung von Geschäfts- und IT-Prozessen verbessert das Datenschutzverständnis innerhalb der verantwortlichen Stelle.

In dieser Norm werden zentrale Begriffe definiert, die zur Festlegung von Löschregeln benötigt werden.

Einsatzgebiet dieser Norm

Vorrangiges Einsatzgebiet dieser Norm ist die Entwicklung eines Löschkonzepts mit Löschregeln und deren Umsetzung durch eine verantwortliche Stelle.

Bei der Konzeption von Geschäftsprozessen werden Löschanforderungen auf der Grundlage der definierten Löschregeln frühzeitig berücksichtigt. Für Systementwicklungs- und Systembeschaffungsprozesse können ebenfalls Löschanforderungen definiert werden.

Diese Norm gibt zudem Software-Herstellern Hinweise darauf, wie IT-Systeme gestaltet sein sollten, um die verantwortlichen Stellen bei der rechtskonformen Löschung von pbD zu unterstützen („Privacy by Design“).

Darüber hinaus bietet diese Norm 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.

1 Anwendungsbereich

Diese Norm definiert ein Vorgehensmodell zur Entwicklung und Etablierung eines Löschkonzeptes für personenbezogene Daten (pbD). Dazu gehören:

- Vorgehensweisen, durch die Löschrregeln für personenbezogene Datenbestände festgelegt werden;
- eine Übersicht über notwendige Umsetzungsvorgaben innerhalb der verantwortlichen Stelle;
- Vorschläge für die Struktur der durch das Löschkonzept vorgegebenen Dokumentation; und
- Empfehlungen, nach denen das Löschkonzept etabliert, umgesetzt und fortgeschrieben und die Verantwortung für die entsprechenden Aufgaben zugewiesen werden sollten.

Diese Norm legt keine konkreten Löschrregeln und Löschrfristen fest. Diese hängen von den jeweils einschlägigen datenschutzrechtlichen Vorschriften 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 dieser Norm.

Wenn die Norm angewandt wird, sind im Regelfall einschlägige datenschutzrechtliche Vorschriften zu berücksichtigen. Deren Interpretation und Übertragung auf das Löschkonzept der verantwortlichen Stelle liegt außerhalb des Gegenstands dieser Norm.

Außerhalb des Gegenstands dieser Norm liegen auch die technischen Mechanismen des Löschsens, wie beispielsweise das Löschen durch Überschreiben von Datenbankwerten, das Löschen von Datensätzen oder das Löschen ganzer Tabellen oder Dateien. Das Sicherheitsniveau von Löschrmechanismen wird ebenfalls nicht betrachtet.

Diese Norm bezieht sich auf das Löschen personenbezogener Daten. Allerdings kann die Vorgehensweise grundsätzlich auch auf andere Datenbestände übertragen werden.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

Ansprechpartner für Datenschutz

Person in der verantwortlichen Stelle, die auf die Einhaltung einschlägiger datenschutzrechtlicher Vorschriften hinwirkt

Anmerkung 1 zum Begriff: In Deutschland ist dies regelmäßig der betriebliche Datenschutzbeauftragte. Unabhängig von der Bestellung eines betrieblichen Datenschutzbeauftragten hat die Geschäftsführung nach den gesetzlichen Vorgaben des BDSG die Pflicht, die einschlägigen datenschutzrechtlichen Vorschriften zu erfüllen. 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 Ansprechpartner für Datenschutz zugeordnet werden.

Anmerkung 2 zum Begriff: Welche konkreten Pflichten für die verantwortliche Stelle bestehen, einen Ansprechpartner für Datenschutz zu benennen, ergibt sich aus den einschlägigen datenschutzrechtlichen Vorschriften und ist nicht Gegenstand dieser Leitlinie.

2.2

Anonymisierung

Prozess, durch den pbD derart irreversibel verändert werden, dass ein Betroffener nicht mehr direkt oder indirekt identifiziert werden kann

Anmerkung 1 zum Begriff: Um pbD zu anonymisieren werden beispielsweise einzelne Werte 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 demnach nicht mehr unter deren Löschrvorgaben. Anonymisierung ist häufig schwer zu erreichen. Die Anforderungen an Anonymisierung ergeben sich aus den einschlägigen datenschutzrechtlichen Vorschriften. Weitere Hinweise gibt Anhang B

[QUELLE: ISO 29100:2011, Begriff 2.2]

2.3

Aufbewahrungsfrist

Zeitraum, innerhalb dessen die Objekte einer Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein müssen

Anmerkung 1 zum Begriff: Eine Aufbewahrungsfrist trägt zur Vorhaltefrist bei.

2.4

Auftragnehmer

Dienstleister, der personenbezogene Daten im Auftrag der verantwortlichen Stelle und ausschließlich nach deren Vorgaben verarbeitet

Anmerkung 1 zum Begriff: Auftragnehmer werden im Sinne der jeweils einschlägigen datenschutzrechtlichen Vorschriften verstanden. In Deutschland ist dies § 3 (8) und § 11 BDSG.

2.5

Betroffener

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

Anmerkung 1 zum Begriff: Einschlägige datenschutzrechtliche Vorschriften können sich auch auf andere Schutzsubjekte als natürliche Personen beziehen, beispielsweise juristische Personen.

2.6

Datenart

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

2.7

Datenbestand

Menge an pbD der verantwortlichen Stelle

Anmerkung 1 zum Begriff: Zu den Beständen zählen regelmäßig auch pbD, die nicht elektronisch gespeichert sind.

2.8

Datenobjekte

Elemente, die Daten enthalten, wie z. B. Dateien, Dokumente, Datensätze oder Attribute

Anmerkung 1 zum Begriff: 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“.

2.9

Löschung

Prozess, durch den pbD derart irreversibel verändert werden, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können

Anmerkung 1 zum Begriff: In der Regel ist "sicheres Löschen" gefordert. Sicheres Löschen meint, dass der Aufwand für die Rekonstruktion der Daten entweder unmöglich oder nur mit erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist. Für die Wahl der Verfahren ist der Schutzbedarf der Daten zu berücksichtigen (vgl. auch [DIN 66399] Teil 1).

Anmerkung 2 zum Begriff: Wenn die einschlägigen datenschutzrechtlichen Vorschriften dies zulassen, können personenbezogene Daten auch anonymisiert werden, statt sie zu löschen. Weitere Hinweise gibt Anhang B.

2.10

Löschfrist

Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden sollte

Anmerkung 1 zum Begriff: Eine besondere Gruppe von Löschfristen bilden die →Regellöschfristen.

2.11**Löschklasse**

Kombination aus einer Standardlöschfrist und einem abstraktem Startzeitpunkt für den Fristlauf

Anmerkung 1 zum Begriff: In einer Löschklasse werden alle Datenarten zusammengefasst, die der gleichen Löschfrist und dem gleichen abstrakten Startzeitpunkt unterliegen. Im Unterschied zur (konkreten) Löschregel für eine Datenart wird in der (abstrakten) Löschklasse nur auf den abstrakten Startzeitpunkt, nicht aber auf eine konkrete Bedingung für den Start des Fristlaufs abgestellt (siehe auch Abschnitt 7).

2.12**Löschkonzept**

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

2.13**Löschregel**

Kombination aus Löschfrist und konkreter Bedingung für den Startzeitpunkt des Fristlaufs

2.14**Personenbezogene Daten (pbD)**

Einzelangaben über persönliche oder sachliche Verhältnisse eines bestimmten oder bestimmbaren Betroffenen

Anmerkung 1 zum Begriff: Hier wurde der Begriff in Anlehnung an § 3 Abs. 1 BDSG definiert. Die Definitionen anderer Rechtsvorschriften können davon abweichen und sind zu verwenden, wenn sie einschlägig sind (siehe hierzu auch 4.2).

2.15**Regellöschfrist**

maximaler Zeitraum, nach dessen Ablauf eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle gelöscht werden sollte

Anmerkung 1 zum Begriff: Zu den Randbedingungen der Fristfestlegung siehe 5.3.3.

2.16**Standardlöschfristen**

vereinheitlichte Löschfristen für die verantwortliche Stelle

2.17**Verantwortliche Stelle**

Person oder Organisation, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt

Anmerkung 1 zum Begriff: Die verantwortliche Stelle ist Adressat der einschlägigen datenschutzrechtlichen Vorschriften. Jeder Datenbestand ist insofern einer verantwortlichen Stelle zugeordnet. Wer dies ist, ist aus den einschlägigen Rechtsvorschriften abzuleiten. Hier wurde die Definition der verantwortlichen Stelle nach § 3 Abs. 3 BDSG verwendet. Für die Etablierung eines Löschkonzepts ist die Definition nach den einschlägigen datenschutzrechtlichen Vorschriften zu verwenden.

Anmerkung 2 zum Begriff: Diese Leitlinie kann auch angewendet werden, wenn datenschutzrechtlich künftig das „Shared-Data-Konzept“ zugelassen wird. In diesem Fall nutzen verschiedene verantwortliche Stellen einen Datenbestand gemeinsam. Diese Stellen sind dann dafür verantwortlich, die Vorgehensweise zur Löschung untereinander abzustimmen, beispielsweise dadurch, dass eine Stelle die Koordination für die Festlegung der Löschregeln übernimmt.

2.18**Vorhaltefrist**

Zeitraum, innerhalb dessen die Objekte einer Datenart in der verantwortlichen Stelle aufgrund der fachlichen Verwendung oder gesetzlicher Aufbewahrungspflichten mindestens verfügbar sein sollten

Anmerkung 1 zum Begriff: Zu den Randbedingungen der Fristfestlegung siehe 4.4.3.

3 Abkürzungen

Tabelle 1 — Verwendete Abkürzungen

Abs.	Absatz
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
CRM	Customer Relationship Management
DIN	Deutsches Institut für Normung e.V.
DMS	Dokumentenmanagementsystem
HGB	Handelsgesetzbuch
ISO	International Standardization Organisation
IT	Informationstechnologie
pbD	personenbezogene Daten
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz

4 Grundlagen eines Löschkonzepts

4.1 Allgemeines

Diese Leitlinie bezieht sich auf das Löschen von personenbezogenen Daten (pbD). Die einschlägigen datenschutzrechtlichen Vorschriften fordern von der verantwortlichen Stelle, dass sie die Löschung personenbezogener Daten sicherstellt.

Diese Leitlinie beschreibt, wie ein Löschkonzept für pbD in einer Organisation etabliert werden kann und welche Festlegungen dafür getroffen und dokumentiert werden sollten. In einem Löschkonzept legt die verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von pbD erfüllt. Dies gelingt nur mittels eines strukturierten und geregelten Vorgehens. Die verantwortliche Stelle sollte dafür insbesondere festlegen,

- welche Löschregeln für welche Datenbestände gelten;
- wie aus den Löschregeln die Umsetzung der Löschung 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.

Diese Festlegungen bilden das Löschkonzept der verantwortlichen Stelle. Dieses Kapitel stellt die Bausteine eines Löschkonzepts im Überblick vor. In den weiteren Kapiteln werden die einzelnen Bausteine detailliert beschrieben.

Diese Leitlinie unterstützt die effiziente Etablierung eines Löschkonzepts folgendermaßen:

- Die wesentlichen Elemente eines Löschkonzepts werden beschrieben und es werden Vorschläge zu ihrer Etablierung gemacht.
- Es werden Begriffsdefinitionen zur Vereinfachung der Kommunikation zwischen Datenschutzverantwortlichen, fachlichen Anwendern, Administratoren, Software-Entwicklern und anderen Beteiligten bereitgestellt.
- Die empfohlene Vorgehensweise zielt darauf, dass die verantwortliche Stelle wenige und einfache Löschregeln definiert, um bessere Verständlichkeit und Umsetzbarkeit zu erreichen.
- Die Vorgehensweise erlaubt es auch vorhandene Ressourcen effizient zu nutzen.
- Die empfohlene Dokumentationsstruktur grenzt inhaltliche Bereiche klar ab und ist deshalb gut zu pflegen, wenn Geschäftsprozesse oder IT-Systeme geändert werden.

Die in dieser Leitlinie beschriebene Vorgehensweise basiert auf den folgenden grundlegenden Schritten:

- Im ersten Schritt werden mit Hilfe exemplarischer Datenarten möglichst wenige Standardfristen für die Löschung von pbD ausgewählt. Sie bilden in der Kombination mit drei abstrakten Startzeitpunkten die Löschklassen der verantwortlichen Stelle.
- Im zweiten Schritt werden alle Arten pbD möglichst vollständig in die Löschklassen eingeordnet. Dadurch lassen sich die Löschregeln systematisch ableiten. Diese Aufgabe wird typischerweise in mehreren Runden iterativ vervollständigt.
- Aus der resultierenden Sammlung der Löschregeln werden anschließend die Umsetzungsvorgaben für konkrete Datenbestände abgeleitet und implementiert.

Diese Effizienz kann nur erreicht werden, wenn die Komplexität des Löschkonzepts im Rahmen der einschlägigen datenschutzrechtlichen Vorschriften so weit wie möglich reduziert wird.

Das Löschkonzept dient der Umsetzung ausgewählter datenschutzrechtlicher Verpflichtungen der verantwortlichen Stelle. Es ist daher als Teil des Datenschutzkonzepts der verantwortlichen Stelle zu verstehen.

Die weiteren Abschnitte dieses Kapitels geben einen Überblick über die zentralen Begriffe und die in dieser Leitlinie vorgeschlagenen Vorgehensweisen. Einige Hinweise zur Organisation eines Projekts „Löschkonzept“ gibt Anhang A.

4.2 Anwendung einschlägiger datenschutzrechtlicher Vorschriften

Die Vorgaben zur Löschung von pbD ergeben sich für eine verantwortliche Stelle aus den einschlägigen datenschutzrechtlichen Vorschriften und gegebenenfalls aus weiteren rechtlich bindenden Vorgaben.

Zu den einschlägigen datenschutzrechtlichen Vorschriften zählen z. B. Gesetze oder Verordnungen. Unter „einschlägig“ werden in dieser Leitlinie alle Vorschriften verstanden, auf deren Grundlage personenbezogene Datenbestände erhoben und verwendet werden und gelöscht werden sollten oder müssen. Dazu gehören sowohl Vorschriften, die sich ausschließlich auf den Datenschutz beziehen, als auch solche, die z. B. ergänzende oder spezielle datenschutzrechtliche Vorschriften, Zulässigkeitsgrundlagen für die Verarbeitung oder Aufbewahrungspflichten enthalten. Da sich die einschlägigen datenschutzrechtlichen Vorschriften länderspezifisch, nach Datenarten und verantwortlicher Stelle unterscheiden können, führen sie für vergleichbare Datenbestände in verschiedenen Ländern gegebenenfalls zu unterschiedlichen Löschregeln.

ANMERKUNG Zu den Rechtsvorschriften zählen in Deutschland auch Betriebs- oder Dienstvereinbarungen

Für die Ableitung von Löschregeln können neben den einschlägigen datenschutzrechtlichen Vorschriften auch weitere rechtliche Vorgaben relevant sein, z. B. Verträge. Solche Regelungen können zwischen den beteiligten Parteien vereinbart werden, aber nur, soweit sie sich im Rahmen der einschlägigen datenschutzrechtlichen Vorschriften bewegen. Im weiteren Text dieser Leitlinie wird deshalb nur noch von einschlägigen datenschutzrechtlichen Vorschriften gesprochen, auch wenn diese durch weitere rechtliche Vorgaben konkretisiert werden können. Es ist Aufgabe der verantwortlichen Stelle bei der Anwendung der Leitlinie zu prüfen, ob sie solche weiteren Rechtsvorgaben zu beachten hat.

Diese Leitlinie beschreibt nur eine Vorgehensweise, nach der Löschregeln entwickelt und angewandt werden können. Es ist Aufgabe der verantwortlichen Stelle, die für sie einschlägigen datenschutzrechtlichen Vorschriften und weiteren rechtlichen Vorgaben zu identifizieren und beim Gebrauch dieser Leitlinie anzuwenden. Die verantwortliche Stelle sollte dabei auch prüfen, welchen Empfehlungen dieser Leitlinie sie folgt, um die einschlägigen datenschutzrechtlichen Vorschriften zum Löschen umzusetzen und an welchen Stellen sie von dieser Leitlinie abweicht. Die gewählte Vorgehensweise sollte dokumentiert werden.

Aus den einschlägigen datenschutzrechtlichen Vorschriften ist beispielsweise die Definition für personenbezogene Daten abzuleiten. Z. B. können neben natürlichen Personen auch andere Schutzsubjekte unter die datenschutzrechtlichen Löschvorschriften fallen. In dieser Leitlinie wird dennoch durchgängig nur vom Betroffenen gesprochen. Werden von den einschlägigen datenschutzrechtlichen Vorschriften andere Schutzsubjekte eingeschlossen, sind deren Datenbestände auch im Löschkonzept zu behandeln.

Aus den einschlägigen datenschutzrechtlichen Vorschriften ist auch abzuleiten, welche Eigenschaften der technischen oder organisatorischen Maßnahmen für die Umsetzung gefordert sind. Z. B. ist abzuleiten, welche Bedingungen für die Anonymisierung personenbezogener Daten zu erfüllen sind, damit Datenbestände aus dem Geltungsbereich der einschlägigen datenschutzrechtlichen Vorschriften herausfallen und weiter gespeichert werden dürfen (siehe auch Anhang B).

Soweit weitere rechtliche Vorgaben zwischen der verantwortlichen Stelle und anderen Stellen vereinbart werden, sollte auf Standardlöschfristen (vgl. Abschnitt 6.1.) und bestehende Löschregeln zurückgegriffen werden. Dadurch wird vermieden, dass die Komplexität der Löschregeln für die verantwortliche Stelle erhöht wird. Vertragspartner können eigene Fristen allerdings nur im Rahmen der Spielräume festlegen, die die einschlägigen datenschutzrechtlichen Vorschriften eröffnen. Im Falle der Auftragsdatenverarbeitung ist der Auftraggeber für die Festlegung der Löschfristen verantwortlich.

Sofern sich Widersprüche zwischen dieser Leitlinie, den einschlägigen datenschutzrechtlichen Vorschriften und weiteren rechtlichen Vorgaben ergeben, haben zunächst die einschlägigen datenschutzrechtlichen Vorschriften und in deren Rahmen die weiteren rechtlichen Vorgaben Vorrang vor dieser Leitlinie.

Löschregeln für die Auftragsdatenverarbeitung

Die einschlägigen datenschutzrechtlichen Vorschriften verlangen, dass Verträge, andere Vereinbarungen und Weisungen zur Auftragsdatenverarbeitung vom Auftragnehmer umzusetzen sind. Vorgaben des Auftraggebers dürfen deshalb vom Auftragnehmer nicht in eigener Weise interpretiert werden, um Löschregeln für die pbD des Auftraggebers abzuleiten. Im Falle der Auftragsdatenverarbeitung verantwortet alleine der Auftraggeber die Festlegung der Löschregeln (siehe dazu auch Abschnitt 8.5). Er bestimmt, welche einschlägigen datenschutzrechtlichen Vorschriften wie umzusetzen sind. Wenn der Auftraggeber seine Löschregeln auf Wunsch des Auftragnehmers anpasst, darf er dies nur, wenn es nach den einschlägigen datenschutzrechtlichen Vorschriften für den Auftraggeber zulässig ist.

4.3 Was bedeutet „Löschen“?

Datenobjekte, die Personenbezug aufweisen, gelten als gelöscht, wenn sie nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet werden können. Löschen wird z. B. durch das physische Überschreiben von Datenobjekten erreicht. Datenobjekte können auch gelöscht werden, indem der Datenträger, auf dem sie enthalten sind, geeignet zerstört oder vernichtet wird. Welche Verfahren für die Löschung oder Vernichtung einzusetzen sind, richtet sich nach der Sensitivität der Daten, den Datenträgern und den einschlägigen datenschutzrechtlichen Vorschriften. Die Auswahl der Verfahren ist nicht Gegenstand dieser Leitlinie. Weiterführende Hinweise gibt Anhang C.

Datenobjekte können auch anonymisiert werden, statt sie zu löschen: 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 Vorzug zu geben. Weitere Hinweise gibt Anhang B.

ANMERKUNG Anonymisierte Daten unterliegen zwar nicht mehr den Löschvorgaben des Datenschutzes. Sie können aber weiterhin einer Vertraulichkeitsklasse der verantwortlichen Stelle unterliegen. Aus den Vertraulichkeitsklassen können sich ebenfalls Löschregeln ergeben.

Im Weiteren wird nur noch der Begriff „Löschen“ verwendet. Die Umsetzungsalternativen „Vernichten von Datenträgern“ und „Anonymisieren von Daten“ sind dabei eingeschlossen.

4.4 Für jede Datenart eine Löschregel

4.4.1 Datenarten

Jeder Teil des Datenbestandes, der für einen einheitlichen fachlichen Zweck verwendet wird, bildet eine Datenart, unabhängig davon wo die Daten im Einzelfall gespeichert werden. Da die Datenarten in der verantwortlichen Stelle in der Regel für unterschiedliche Zwecke verwendet werden, können sich auch unterschiedliche Regeln für die Löschung ergeben.

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

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

4.4.2 Löschregeln

Personenbezogene Daten sollten nicht nur nach Einzelfallentscheidungen, sondern durchgängig nach sinnvollen Regeln gelöscht werden. Im Löschkonzept entwickelt die verantwortliche Stelle deshalb Regeln, wann die einzelnen Datenarten zu löschen sind. Für jede Datenart wird eine datenschutzkonforme Löschregel definiert. Jede Löschregel enthält eine Löschfrist und einen Startzeitpunkt, ab dem die Frist zu laufen beginnt.

Die einschlägigen datenschutzrechtlichen Vorschriften 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 Zweckbindung („Use, Retention and Disclosure Limitation“) und Datensparsamkeit („Data Minimization“) anzuwenden. Danach sind pbD so früh wie möglich zu löschen.

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“.

4.4.3 Vorhaltefrist und Regellöschfrist

4.4.3.1 Löschen im Regelprozess

Für jede Datenart ist zu klären, wie lange sie in Geschäftsprozessen benötigt wird. Der Zeitraum, innerhalb dessen sie auf Grund der fachlichen Verwendung oder gesetzlicher Aufbewahrungspflichten **mindestens** verfügbar zu halten ist, wird als **Vorhaltefrist** bezeichnet. Sie setzt sich zusammen aus dem Zeitraum, in dem eine Datenart aktiv in Geschäftsprozessen verwendet wird und dem Zeitraum, in dem die Datenart für fachliche Zwecke der verantwortlichen Stelle noch aufbewahrt werden sollte oder aus rechtlichen Vorgaben noch aufzubewahren ist. In beiden Fällen sind die Grenzen der Aufbewahrung durch die einschlägigen datenschutzrechtlichen Vorschriften zu beachten.

Rechtliche Aufbewahrungspflichten sind Teil des Verwendungsprozesses in der verantwortlichen Stelle. Sie ergeben sich, wenn in einschlägigen datenschutzrechtlichen Vorschriften Aufbewahrungsfristen für bestimmte Datenarten festgelegt sind. Aufbewahrungsfristen können sich außerdem aus vertraglichen Vereinbarungen ergeben.

Auch eigene fachliche Zwecke können dazu führen, dass eine verantwortliche Stelle Datenarten für einen Zeitraum nach dem Ende der aktiven Verwendung aufbewahren will.

BEISPIEL Zu rechtlichen Aufbewahrungspflichten zählen beispielsweise die Vorgaben des Steuerrechts für Handelsbriefe und Buchhaltungsunterlagen. Zu fachlichen Zwecken zählen z. B. Garantiezusagen oder potenzielle Rückrufaktionen.

Die einschlägigen datenschutzrechtlichen Vorschriften können besondere Maßnahmen fordern, wenn Datenobjekte nur noch gespeichert werden, um Aufbewahrungspflichten zu erfüllen. Beispielsweise kann in diesem Fall gefordert werden, dass die Daten gesperrt werden. Die Daten dürfen in diesem Fall nur noch für die Zwecke genutzt werden, für die sie aufbewahrt werden.

ANMERKUNG 1 Beispielsweise ist im BDSG nach § 35 Abs. 3 Nr. 1 die Sperrung für Daten gefordert, die nur noch wegen rechtlicher Vorgaben gespeichert werden und deshalb nicht gelöscht werden können. Aus der engeren Zweckbegrenzung ergibt sich implizit, dass nur noch Benutzer Zugriff erhalten dürfen, die mit den Zwecken befasst sind, aus denen die Aufbewahrungspflicht resultiert.

In solchen Fällen kann es sinnvoll sein, im Rahmen der Löschregeln auch Regeln für die Sperrung von Datenarten festzulegen. Weitere Hinweise zu diesem Aspekt gibt Anhang D. Sperrregeln werden hier nicht weiter betrachtet.

Die verschiedenen Zeiträume der Verwendung ergeben zusammen die Vorhaltefrist. Um der Definition der Vorhaltefrist oben zu entsprechen, ist jede Datenart mindestens an einem definierten Ort bis zum Ende der Vorhaltefrist verfügbar zu halten.

Nach dem Ende der jeweiligen Vorhaltefrist werden die Daten in der verantwortlichen Stelle nicht mehr benötigt. Datenschutzrechtlich ist dann gefordert, dass die Daten innerhalb einer vertretbaren Frist gelöscht werden. Die Summe aus Vorhaltefrist und der datenschutzrechtlich vertretbaren Frist für die Gestaltung der Löschräume definiert die längste Löschrfrist bei der Verarbeitung der Daten im Regelprozess. Diese Frist wird als **Regellöschrfrist** bezeichnet. Datenobjekte sollten nach Ablauf ihrer Regellöschrfrist in allen Systemen der verantwortlichen Stelle gelöscht sein. Dies schließt die Löschung bei Auftragnehmern der verantwortlichen Stelle ein.

In Bild 1 wird dargestellt, wie mit den verschiedenen Fristabschnitten im Lebenszyklus eines Auftrags eine Regellöschrfrist gebildet wird. Im Beispiel beginnt der Lauf der Vorhalte- und der Regellöschrfrist für den Auftrag 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 Abgabenordnung (AO) und Handelsgesetzbuch (HGB) aufbewahrt.

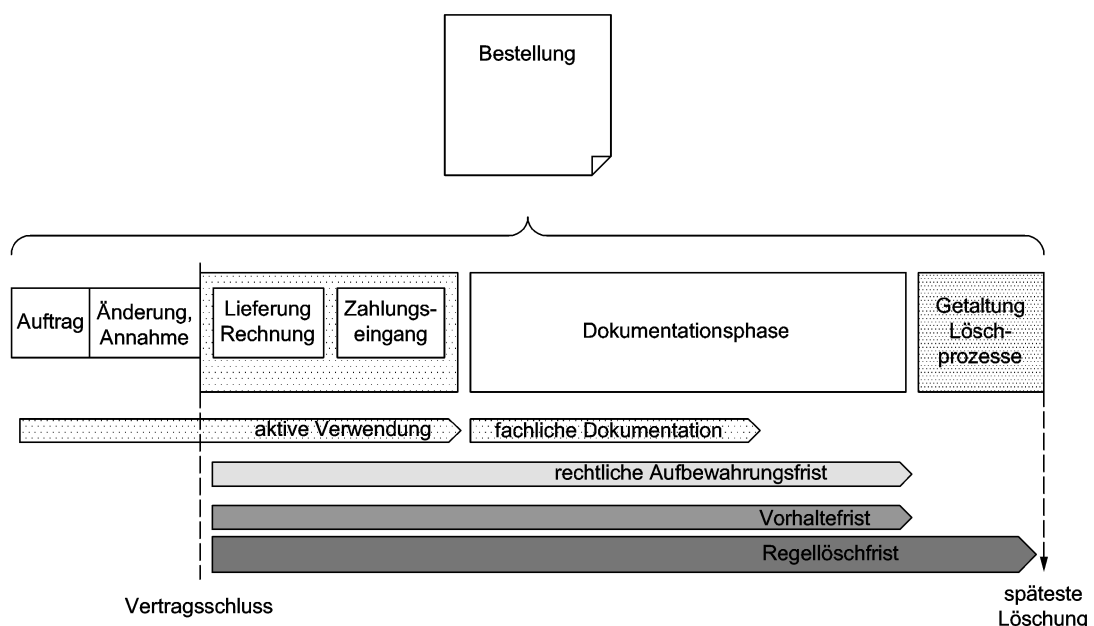


Bild 1 — Beispiel für Fristabschnitte für einen Auftrag im Löschrkonzept

ANMERKUNG 2 Im Beispiel in Bild 1 ist die Vorhaltefrist für den Auftrag kürzer als die Regellöschfrist. Je nach Datenart und Löschrufen der verantwortlichen Stelle können Vorhaltefrist und Regellöschfrist auch gleich lang sein. Die Rechnung und die Buchung des Zahlungseingangs fallen in jeweils eigene Datenarten und haben deshalb eigene Löschrufen.

Die zulässigen Verwendungszwecke bestimmen die Vorhaltefrist und die Regellöschfrist. Wenn die Rechtslage Spielräume für die Fristen zur Verwendung einer Datenart einräumt, können diese im Verwendungs- und Löschrufen genutzt werden. Es ist Aufgabe der verantwortlichen Stelle, abzuschätzen und datenschutzrechtlich zu verantworten, welche Spielräume bestehen und wie lange nach dem Ende der Vorhaltefrist die Löschung erfolgen kann.

Wenn rechtliche Spielräume bestehen, können diese genutzt werden, um die Löschrufen auf einfache Weise zu bilden. Durch die Spielräume ist es gegebenenfalls möglich, für viele Datenarten Standardlöschrufen zu verwenden und auf eine genaue Fristanalyse zu verzichten (siehe Abschnitt 6.1). Dann können Löschrufenklassen zur Festlegung der Löschrufen benutzt werden (siehe Abschnitt 7).

Wenn die einschlägigen datenschutzrechtlichen Vorschriften 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 Abschnitt 7.3.

ANMERKUNG 3 Durch den Zeitraum zwischen dem Ende der Vorhaltefrist und dem Ende der Regellöschfrist werden die Löschrufen und die Umsetzung von Löschrufenmaßnahmen im Systembetrieb praktikabler.

4.4.3.2 Sonderfälle

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 datenschutzrechtlichen Vorschriften zulässig ist (Abschnitt 6.3.2). Zur Behandlung von Störfällen kann die Löschung zeitweise ausgesetzt werden (Abschnitt 6.3.4).

4.4.4 Behandlung nicht-produktiver Datenbestände: Archive und Sicherungskopien

4.4.4.1 Archive und Sicherungskopien

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

Archive dienen dazu, Daten langfristig vorzuhalten. Daten werden in Archive verlegt, wenn keine Veränderungen mehr vorgenommen werden, jedoch aus zulässigen Gründen gefordert ist, dass sie weiter aufbewahrt werden. Ein Archiv kann unterschiedliche Datenarten mit unterschiedlichen Löschrufen enthalten. Die einschlägigen datenschutzrechtlichen Vorschriften können fordern, dass archivierte Daten gesperrt werden (siehe Anhang D).

Sicherungskopien (Backup) dienen der Wiederherstellung von Systemen und Datenbeständen nach Störungen und dürfen daher nicht verändert werden. Ein Löschrufen von Daten innerhalb von Backups ist in der Praxis kaum möglich und widerspricht dem Zweck einer Sicherung. Sicherungskopien benötigen jedoch für ihren Zweck nur eine geringe Vorhaltezeit. Mit kurzen Löschrufen für die Backup-Generationen kann dann Löschrufenvorgaben entsprochen werden. Sicherungskopien dürfen nicht als Archive missbraucht werden.

Es wird dringend empfohlen, zwischen Sicherungskopien und Archiven klar zu trennen. Die pbD in Archiven unterliegen den Löschrufen der jeweiligen Datenarten und sollten nach diesen Regeln im Archiv gelöscht werden. Für die Löschung von Sicherungskopien sollten dagegen eigene Fristen festgelegt werden, die bezüglich der Regellöschfristen der im Backup enthalten „gemischten“ Daten verhältnismäßig sind (siehe Abschnitt 6.3.5).