Volker Hammer

DIN 66398

Die Leitlinie Löschkonzept als Norm

Am 08.04.2016 wurde die „Leitlinie Löschkonzept" als DIN 66398 veröffentlicht. Die neue Norm beschreibt, wie ein Löschkonzept in einer Organisation etabliert werden kann. Schwerpunkt ist eine effiziente Vorgehensweise, um Löschregeln festzulegen. Der Beitrag gibt einen Überblick über die Norm.

1 Motivation

Für personenbezogene Daten ist Löschen gefordert, sobald sie für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich sind. Dies ist beispielsweise implizit der Fall, wenn die Zulässigkeit nach § 4 BDSG entfallen ist und weil nach § 3a BDSG Datenvermeidung und Datensparsamkeit gefordert sind. Explizit wird die Löschung personenbezogener Daten in den §§ 20 und 35 BDSG gefordert.[1] Die Vorgaben zur Löschung schützen die Betroffenen vor unzulässiger Verwendung ihrer Daten, wenn die zulässigen Prozesse beendet sind.

In der Praxis besteht allerdings ein großes Vollzugsdefizit für diese Löschvorgabe. Hauptsächlich findet man hierfür zwei Ursachen: Organisationen haben häufig keine Regeln definiert, nach denen Daten zu löschen sind. Außerdem sind viele IT-Systeme technisch nicht ausreichend darauf vorbereitet, Daten in Regelprozessen zu löschen. Weitere Gründe sind eher mentaler Natur:

- Oft sind Mitarbeiter aller Ebenen unsicher, was wohl passieren mag, wenn man Daten löscht. Es wird befürchtet, dass IT-Prozesse gestört oder dass bestimmte Abläufe oder Auswertungen nicht mehr möglich sein werden. Solche Schwierigkeiten können tatsächlich eintreten, wenn die Löschung nicht sorgfältig vorbereitet wird.
- Vielfach wollen sich Organisationen nicht von ihren Datenbeständen trennen, weil vage erwartet wird, dass die Daten ja noch gebraucht werden könnten. Diese Motivation beschreibt allerdings nichts anderes als unbestimmte Zwecke, die nach dem BDSG nicht zulässig sind.
- Schließlich ist es häufig schwierig, die fachlichen Zusammenhänge zu überschauen. Wenn gleiche Daten in mehreren Prozessen zu unterschiedlichen Zwecken verwendet werden, führt dies meist zu einer sehr komplexen Verzahnung organisatorischer Abläufe und zugehöriger IT-Anwendungen. In der Folge gibt es möglicherweise niemanden, der sicher bestimmen kann, wann sämtliche beteiligten Prozesse beendet sind und die Daten demzufolge gelöscht werden können.

Die genannten Schwierigkeiten führen dazu, dass Löschen als Aufgabe oft gar nicht erst betrachtet wird – weder auf der fachlichen noch auf der betriebsorganisatorischen Ebene. Löschen ist in der Tat nicht einfach. Dies rechtfertigt aber keinen Verstoß gegen Datenschutzvorgaben.

Damit alle Datenbestände gleichermaßen korrekt gelöscht werden, bedarf es einer systematischen Vorgehensweise. Diese muss für die verantwortliche Stelle entwickelt und dokumentiert werden, und zwar sinnvollerweise in einem Löschkonzept. Die DIN 66398 ist eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten". Sie bietet umfangreiche Hilfestellungen, um ein solches Löschkonzept zu erstellen und zu etablieren. Dieser Beitrag beschreibt die Entwicklung der Norm und gibt einen Überblick über die Inhalte.

2 Entwicklungsgeschichte

Die Geschichte der Norm beginnt bei der Toll Collect GmbH[2]. Dort sollte vor dem Start des Mautsystems ein unternehmensweites Löschkonzept etabliert werden.[3] Die folgenden langjährigen Erfahrungen mit der gewählten Vorgehensweise waren so positiv, dass das Deutsche Institut für Normung e. V. (DIN) darauf aufmerksam wurde. In einem DIN-INS-Projekt[4] wurde 2012 geprüft, ob die Vorgehensweise auf andere Unternehmen übertragen werden könne und ob eine Standardisierung sinnvoll sei. Diese Prü-

1 Andere deutsche Datenschutzgesetze enthalten entsprechende Vorschriften. Auch die EU Datenschutz-Grundverordnung sieht in Artikel 5 vor, dass personenbezogene Daten für legitime Zwecke erhoben werden müssen und nur in damit vereinbarer Weise weiterverarbeitet werden dürfen. Die Identifizierung der betroffenen Personen darf nur so lange möglich sein, wie es für die Zwecke, für die sie verarbeitet werden dürfen, erforderlich ist (nach *EU DSGV*).

Dr. Volker Hammer

ist Mitarbeiter von Secorvo mit Arbeitsschwerpunkten in Datenschutz und Informationssicherheit. Seit 2004 berät er zu Löschkonzepten, u.a. die die Toll Collect GmbH. Er ist Editor der DIN 66398.
E-Mail: volker.hammer@secorvo.de

2 Die Toll Collect GmbH ist die Betreiberin des deutschen Mautsystems.

3 Siehe zu den Vorarbeiten bei Toll Collect *Fraenkel/Hammer DuD 2007* und *Hammer/Fraenkel DuD 2007.*

4 Das Projekt wurde im Rahmen des Programms „Innovation mit Normen und Standards" vom Bundesministerium für Wirtschaft und Technologie gefördert. Projektträger war das DIN.

fung fiel positiv aus.[5] Die Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect beschlossen daraufhin Ende 2013, ein Normungsprojekt beim DIN zu fördern.

Für den Themenbereich Datenschutz ist im DIN der Arbeitskreis 05 im DIN NIA 27 zuständig.[6] Dieser Arbeitskreis nahm im Februar 2014 den Antrag für das Normungsprojekt an. In verschiedenen Bearbeitungsschritten entstand der Text der Norm, unter anderem mit einer viermonatigen öffentlichen Kommentierungsphase von Januar bis Mai 2015 und einem anschließenden Einwender-Workshop. An den Diskussionen im DIN-INS-Projekt und im DIN-Arbeitskreis waren auch Vertreter der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein beteiligt.

Das Manuskript der Norm wurde im September 2015 vom Arbeitskreis verabschiedet und im April 2016 beim Beuth-Verlag als DIN 66398 veröffentlicht.

3 Gegenstand und Aufbau der Norm

Die DIN 66398 definiert ein Vorgehensmodell zur Entwicklung und Etablierung eines Löschkonzeptes für personenbezogene Daten (pbD).

- Die Norm beschreibt Vorgehensweisen, durch die Löschregeln festgelegt werden.
- Sie schlägt weiter vor, wie die Umsetzung der Löschregeln gesteuert werden kann.
- Für die Dokumentation des Löschkonzepts empfiehlt sie eine Struktur.
- Schließlich gibt die Norm auch Empfehlungen, wie das Löschkonzept etabliert und fortgeschrieben werden kann.

Konkrete Löschregeln und Löschfristen kann die Norm allerdings nicht festlegen. Da diese von den jeweils einschlägigen datenschutzrechtlichen Vorschriften und den zulässigen Zwecken der Verarbeitung bei der verantwortlichen Stelle abhängen, müssen die Regeln durch die verantwortliche Stelle festgelegt werden. Hauptadressat der Norm ist deshalb die verantwortliche Stelle. Die Norm kann außerdem organisationsübergreifende Synergie-Effekte erschließen – dazu unten Näheres.

In den ersten drei Kapiteln spezifiziert die Norm den Anwendungsbereich, Begriffe und Abkürzungen. Gerade auch formale Festlegungen wie die Begriffsdefinitionen sind für Löschprojekte hilfreich: Da zwangsläufig Akteure aus unterschiedlichen Disziplinen zusammenarbeiten müssen, helfen erprobte Begriffe bei der Verständigung zwischen Fachanwendern, Entwicklern, Administratoren und Mitarbeitern aus der Rechtsabteilung und dem Datenschutz.

Kapitel Vier der Norm gibt einen Überblick über die Vorgehensweise. Hier finden sich auch Hinweise, wie einschlägige datenschutzrechtliche Vorschriften im Löschkonzept zu berücksichtigen sind. Es werden außerdem die zentralen Begriffe erläutert, darunter Löschen, Datenart, Löschregel, Vorhaltefrist, Standardlöschfrist und Regellöschfrist. Außerdem werden im Hinblick auf Löschen die Bezüge der Datenbestände in Produktion, Archiven und Backups dargestellt.

Die Kapitel Fünf bis Neun vertiefen einzelne Aspekte. Sie beschreiben:

- wie Datenarten gebildet werden,
- wie Löschfristen festgelegt werden,
- welche Löschklassen entstehen und wie die Datenarten in diese Klassen eingeordnet werden,
- wie Umsetzungsvorgaben für die Löschung strukturiert werden und welche Inhalte sie haben,
- und schließlich, welche Verantwortlichkeiten geregelt werden müssen, um das Löschkonzept fortzuschreiben und zu pflegen.

Vier Anhänge bieten Informationen zu Fragen aus dem Kontext eines Löschkonzepts: zur Organisation eines Projekts „Löschkonzept", zum Verhältnis zwischen Anonymisieren und Löschen, zu Vorgaben für die Sicherheit von Löschmechanismen und zur Bedeutung des datenschutzrechtlichen Sperrens bei Aufbewahrungsfristen über eine fachliche Verwendung hinaus.

Im folgenden Abschnitt werden die Kernaspekte der Norm skizziert.

4 Inhalte der DIN 66398

Die in der Norm empfohlene Vorgehensweise gründet auf zwei Säulen. Deren erste ist das Prinzip „Für jede Datenart genau eine Löschregel". Dazu wird der Datenbestand der verantwortlichen Stelle in Datenarten aufgeteilt. Eine *Datenart* umfasst einen Bestand, der für einen rechtlichen oder fachlichen Zweck verwendet wird, unabhängig davon, wie die konkreten Datenobjekte aufgebaut sind und wo sie gespeichert oder verarbeitet werden.

Die zweite Säule ist die klare Trennung der Dokumentation technikunabhängiger Löschregeln von den Umsetzungsvorgaben, die das Löschen in Prozessen steuern

4.1 Keine Löschung ohne Regeln

Wie eingangs benannt besteht eine der Hürden für die Löschung personenbezogener Daten im Fehlen von Löschregeln. Wie aber sollen Löschregeln gebildet werden?

Eine Löschregel definiert, welche Daten zu welchem Zeitpunkt gelöscht werden sollen. Wie beschrieben soll für jede Datenart genau eine Löschregel definiert werden. Diese Löschregel besteht aus zwei Angaben: der sogenannten Regellöschfrist und einem Startzeitpunkt, ab dem die Regellöschfrist läuft. Unter der *Regellöschfrist* wird die Frist verstanden, nach der die Datenobjekte einer Datenart gelöscht sein müssen, wenn sie im Regelprozess verarbeitet werden. Da eine Regellöschfrist alleine keinen Termin für die Löschung festlegt, muss ein Startzeitpunkt für den Lauf der Frist durch ein geeignetes Ereignis bestimmt werden. Das kann beispielsweise das Datum eines Protokoll-Eintrags, der Zeitpunkt eines Vertragsschlusses oder der Termin einer Kündigung sein. Ein Datenobjekt muss gelöscht sein, wenn die Regellöschfrist bezogen auf den jeweiligen Startzeitpunkt erreicht wurde.

Für die Löschregel muss die datenschutzrechtliche Zulässigkeit gegeben sein: Datenobjekte der Datenart müssen durch Anwendung von Startzeitpunk und Regellöschfrist im Sinne des Datenschutzes ‚rechtzeitig' gelöscht werden. Es gilt daher, mit

5 *Hammer/Schuler 2012*. Dieses Dokument ist eine Vorversion zur Norm.

6 Der DIN NIA 27 ist ein Arbeitsgremium des ‚Normenausschusses Informationstechnik und Anwendungen'. Der Aufgabenbereich von NIA 27 sind ‚IT-Sicherheitsverfahren' und umfasst Normen für generische Methoden und Techniken für die IT-Sicherheit. Aufgabenbereich des Arbeitskreises 05 im NIA 27 sind Normen im Bereich ‚Identitätsmanagement und Datenschutz-Technologien'. Andere Arbeitskreise im NIA 27 arbeiten z.B. mit an der ISO/IEC 27000-Serie oder an kryptographischen Verfahren.

Abb. 1 | Matrix von Löschklassen am Beispiel von Toll Collect.[7]

Startzeitpunkte	Standardlöschfristen: Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
ab Erhebung			Mautdaten	Mautdaten mit besonderem Analysebedarf			
Ende des Vorgangs	Web-Logs, nmF	Kurzzeit-Doku, Betriebs-Logs	Voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Reklamations- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
Ende der Beziehung zum Betroffenen				ergänzende Stammdaten		Verträge	Kernstammdaten

Die gesetzlich motivierten Fristen von 4, 7 und 12 Jahren entstehen, weil die Rechtsvorschriften die Frist erst ab einer Jahresgrenze definieren. Das laufende Kalenderjahr wurde in diesen Fällen zur Standardlöschfrist hinzugerechnet.

Legende

allgemeine Gesetze	spezielle Gesetze	frei gewählt

der Löschregel eine geeignete Kombination von Regellöschfrist und Startzeitpunkt zu bestimmen. Dazu bietet die Norm eine überaus effiziente Vorgehensweise an: die Verwendung von sogenannten Löschklassen.[8]

Löschklassen

Löschklassen werden jeweils aus einer Standardlöschfrist und einem von drei Typen von Startzeitpunkten gebildet.

Standardlöschfristen werden verwendet, um Löschfristen, die vergleichsweise nahe beieinander liegen, in einer Frist zusammenzufassen. Die Standardlöschfristen reduzieren die Komplexität des Löschkonzepts und erleichtert die spätere Umsetzung, ohne die Aufbewahrung zu löschender Datenobjekte datenschutzrechtlich unangemessen lange zu verzögern. Die Norm schlägt drei Schritte vor, in denen Standardlöschfristen identifiziert werden. Dazu werden wenige, möglichst typische Datenarten als Stellvertreter ausgewählt, die für unterschiedliche Zwecke verwendet werden.

- Zunächst werden Datenarten identifiziert, für die sich Fristen **unmittelbar aus Rechtsvorschriften** ergeben. Beispiele hierfür sind die Verjährungsfrist von 3 Jahren nach § 195 BGB, die Aufbewahrungsfrist von 6 Jahren für Handelsbriefe und 10 Jahren für Buchhaltungsdaten und Buchungsbelege nach § 147 AO und § 257 HGB. Daraus ergeben sich die ersten Standardlöschfristen: Aus den identifizierten Fristen verwendet man als Standardlöschfristen so wenige wie möglich, aber so viele wie datenschutzrechtlich nötig.
- Für manche Datenarten können die Standardlöschfristen aus dem ersten Schritt datenschutzrechtlich unzureichend sein, beispielsweise weil es sich um besondere Arten personenbezogener Daten handelt oder weil gesetzlich enge Fristen gefordert sind, die aber unbestimmt sind. Für ausgewählte Datenarten aus dieser Gruppe werden daher **Prozessanalysen** durchgeführt. Dazu wird geprüft, wie lange die einzelnen Schritte des Geschäftsprozesses dauern, in dem die jeweilige Datenart verwendet wird. Grundlage für die Standardlöschfrist ist die Summe über die maximalen Laufzeiten der Schritte. Eine solche Analyse ist aufwändig. Sie kann aber rechtlich gefordert sein, um eine enge Frist zu bestimmen. Wenn möglich, werdennur wenige Prozesse analysiert, um weitere Standardlöschfristen zu bestimmen.
- In den beiden ersten Schritten werden bereits einige Standardlöschfristen festgelegt. Die Abfolge dieser Standardlöschfristen kann aber große Abstände aufweisen. Dann kann folgende Situation auftreten: Für manche verbleibenden Datenarten kann einerseits der Zweck verhindern, dass sie zu einer frühen Standardlöschfrist gelöscht werden. Andererseits kann die nächste größere Standardlöschfrist datenschutzrechtlich nicht mehr vertretbar sein, weil sie einen zu großen Abstand aufweist. Bei Bedarf werden solche Lücken dann durch **frei gewählte Standardlöschfristen** unterteilt. In Abb. 1 sind die Fristen 42 Tage und 1 Jahr frei gewählt.

Ziel ist es, mit wenigen Standardlöschfristen auszukommen. In allen drei Schritten wird daher geprüft, ob Differenzierungen nötig sind und ob nahe beieinander liegende Fristen zu einer zusammengefasst werden können.

Löschregeln benötigen außerdem *Startzeitpunkte*. Die Startzeitpunkte lassen sich nach drei wesentlichen Typen einteilen. Diese Typen von Startzeitpunkten abstrahieren von konkreten Ereignissen und werden in der Norm verwendet, um Löschklassen zu bilden. Zwei Typen sind naheliegend: Der Lauf der Löschfrist beginnt mit dem Zeitpunkt der **Erhebung** oder mit dem **Ende eines Vorgangs.** Ein spezielles Ereignis ist das Ende der Beziehung zum Betroffenen. Dieses Ereignis ist ein Spezialfall von „Ende eines Vorgangs". Dieser Typ von Startzeitpunkt hat allerdings besondere Bedeutung, weil für alle bis dahin aufbewahrten Datenarten spätestens jetzt die Löschfrist starten muss. Das **Ende der Beziehung zu einem Betroffenen** wird daher als dritter abstrakter Startzeitpunkt verwendet.

Löschklassen werden nun gebildet, indem eine Matrix der aus den vorigen Arbeitsschritten festgelegten Standardlöschfristen und den Typen von Startzeitpunkten aufgespannt wird. Jede Zelle der Matrix entspricht einer Löschklasse und wird definiert durch eine Kombination aus Standardlöschfrist und Startzeitpunkt. Ein Beispiel für eine Matrix mit Löschklassen zeigt Abb. 1

Datenarten in Löschklassen

Im nächsten Schritt werden die Datenarten in die Löschklassen eingeordnet.

7 Abb. in Anlehnung an DIN 66398.

8 Das Konzept der Löschklassen wurde im Löschkonzept von Toll Collect entwickelt: *Hammer/Fraenkel DuD 2011.*

Für viele Datenarten besteht ein gutes Grundverständnis dafür, welchen datenschutzrechtlich zulässigen Zwecken sie dienen. Daraus ergibt sich, wie lange man Daten zur fachlichen Verwendung, für fachliche Dokumentationserfordernisse und aus rechtlichen Aufbewahrungspflichten aufbewahren muss und darf (Vorhaltefrist). Mit diesen Kenntnissen kann die verantwortliche Stelle die Datenarten in die oben festgelegten Löschklassen einordnen. Dabei wird für jede Datenart eine Löschklasse gewählt, deren Typ von Startzeitpunkt und Standardlöschfrist der Vorhaltefrist der jeweiligen Datenart entspricht oder deren Standardlöschfrist nur wenig größer ist.

Ein gewisser „Abstand" zwischen Vorhaltefrist und Standardlöschfrist ist in vielen Fällen datenschutzrechtlich akzeptabel. Bestehen im Einzelfall Bedenken, dass der Abstand zu einer zu späten Löschung führen würde, muss versucht werden, eine andere Kombination von Standardlöschfrist und Startzeitpunkt zu wählen.[9] In manchen Fällen führt eine Prüfung auch dazu, dass für die Datenart nur eine kürzere Vorhaltefrist notwendig ist und sie deshalb in eine Löschklasse mit kürzerer Frist eingeordnet werden kann. Zeigt sich während der Zuordnung, dass in einer Datenart unterschiedliche Fristen für die Löschung angebracht wären, ist dies ein starkes Indiz dafür, dass die Datenobjekte auf zwei oder mehr Datenarten aufgeteilt werden sollten und dann in unterschiedliche Löschklassen eingeordnet werden.

Mit diesem Schritt sammelt die verantwortliche Stelle in jeder Zelle der Matrix die Datenarten mit gleichem Typ von Startzeitpunkt und gleicher Standardlöschfrist. In einer Spalte der Matrix sind alle Datenarten mit gleicher Standardlöschfrist angeordnet. Das schafft gute Vergleichsmöglichkeiten, um die Zuordnung der Datenart zu Löschklassen zu überprüfen und fachliche Abhängigkeiten zu berücksichtigen.

Alle Löschregeln der verantwortlichen Stelle sollen in einem Dokument „Löschregeln" zusammengestellt werden. Dort müssen die Löschregeln ausformuliert werden. Für jede Datenart wird dazu die Standardlöschfrist der Löschklasse als Regellöschfrist übernommen. Außerdem muss der Startzeitpunkt definiert werden, indem eine konkrete Bedingung identifiziert wird. Beispiel: Der Typ des Startzeitpunktes „Ende eines Vorgangs" wird konkretisiert durch „Zeitpunkt des Vertragsschlusses". Das Dokument „Löschregeln" bildet den Katalog der Regeln für die verantwortliche Stelle.

4.2 Keine Löschung ohne Implementierung

Die Löschregeln werden im Katalog technikunabhängig beschrieben, also ohne Blick auf die Speicherorte, die Verarbeitungsprozesse und die Verantwortlichen für den jeweiligen Datenbestand. Um die Löschung erfolgreich umzusetzen, müssen die Regeln auf konkrete Maßnahmen übertragen und Verantwortliche zur Löschung verpflichtet werden. In der DIN 66398 wird vorgeschlagen, dazu sogenannte *Umsetzungsvorgaben* zu verwenden. Umsetzungsvorgaben können als eigenständige Dokumente erstellt oder in bestehende Dokumente der verantwortlichen Stelle aufgenommen werden. Die Norm schlägt vor, Umsetzungsvorgaben nach folgenden Kriterien zu bilden:

- In Richtlinien können die Löschmaßnahmen für übergreifende Aspekte festgelegt werden, beispielsweise für Backups oder Einträge in IT-Protokollen.
- Systemspezifische Umsetzungsvorgaben beschreiben die Löschmaßnahmen für alle Datenarten in einem IT-System. Die Maßnahmen könnten z. B. im jeweiligen Betriebshandbuch ergänzt werden.
- Umsetzungsvorgaben können auch für manuelle Prozesse notwendig sein, z. B. als Teil von Arbeitsanweisungen.
- Schließlich sind auch Dienstleister geeignet zu verpflichten, beispielsweise über vertragliche Vereinbarungen im Dienstleistungsvertrag oder über ADV-Weisungen.

Eine Umsetzungsvorgabe nach dieser Struktur umfasst eine oder mehrere Datenarten und legt für diese die Implementierung der Löschregeln fest. In der Umsetzungsvorgabe werden daher zunächst die Datenarten aufgeführt, für die diese Umsetzungsvorgabe gilt. Für diese Datenarten werden die Löschregeln aus dem Katalog der Löschregeln entnommen und für die Umsetzung konkretisiert. Für die Datenarten in einem IT-System sind dazu jeweils unter anderem die folgenden Entscheidungen zu treffen:

- Soll die Regellöschfrist ausgenutzt werden oder kann die Datenart schon früher gelöscht werden? Dies kann beispielsweise der Fall sein, wenn sie in mehreren Systemen verarbeitet, aber nur in einem archiviert wird.
- Welches sind die konkreten Bedingungen im System, durch die der Startzeitpunkt identifiziert wird? Beispiel: Für den Zeitpunkt des Vertragsschlusses könnte ein konkretes Attribut mit dem entsprechenden Datum verwendet werden.
- Mit welchem Mechanismus wird gelöscht?
- Wie wird der Löschlauf dokumentiert?

Mit den Umsetzungsvorgaben wird der Regelbetrieb organisiert. Was aber tun, wenn Daten länger benötigt werden oder technische Störungen auftreten?

4.3 Keine Regel ohne Ausnahme

Der Begriff „Regellöschfrist" legt nahe, dass es auch Abweichungen vom Regelprozess geben kann. Damit ein Löschkonzept in der Praxis bestehen kann, muss es Sonderfälle abdecken können. Die DIN 66398 enthält daher auch Vorschläge für verschiedene fachliche Anforderungen und Situationen des IT-Betriebs, die dem Löschkonzept die notwendige Flexibilität verschaffen:

- Gelegentlich werden einzelne Datenobjekte länger benötigt, beispielsweise für einen Rechtsstreit. Das kann im Löschkonzept abgebildet werden, indem für diese ausgewählten Bestände eine eigene Datenart definiert wird. Datenobjekte, die beispielsweise als Beweismittel verwendet werden sollen, fallen dann in diese Datenart und unterliegen einer anderen Löschregel. Sie können dann z. B. gekennzeichnet und von Löschung ausgenommen werden, bis der Rechtsstreit beendet ist. Solche Ausnahmen werden dann in Umsetzungsvorgaben berücksichtigt.
- Wenn Datenbestände länger gespeichert werden sollen, um beispielsweise statistische Auswertungen zu erlauben, kann unter Umständen durch Vergröberung oder Aggregation von Werten eine andere Zulässigkeitsgrundlage erreicht und dann für die umgewandelten Bestände die Datenart gewechselt werden. Auch für solche „veränderten" Datenarten können die Löschmaßnahmen in Umsetzungsvorgaben beschrieben werden.
- Im Falle von Störungen des IT-Betriebs oder Fehlern im Datenbestand wird vorgeschlagen, die Löschmechanismen befristet

9 Wenn die Zuordnung einer Datenart nicht möglich ist, kann selbstverständlich auch geprüft werden, ob eine weitere Standardlöschfrist eingeführt wird oder eine Löschregel außerhalb des Schemas der Löschklassen definiert wird. Solche Ausnahmen sollen aber vermieden werden, weil dadurch die Komplexität des Löschkonzepts erhöht wird.

auszusetzen. Das Aussetzen der Löschung und die Wiederaufnahme des Regelbetriebs können beispielsweise über das Change-Management gesteuert werden.

- Schließlich können wenige Spezialfälle von Löschungen auch direkt über das Change-Management angewiesen werden, beispielsweise wenn ein Betroffener ein berechtigtes Löschbegehren stellt.[10]

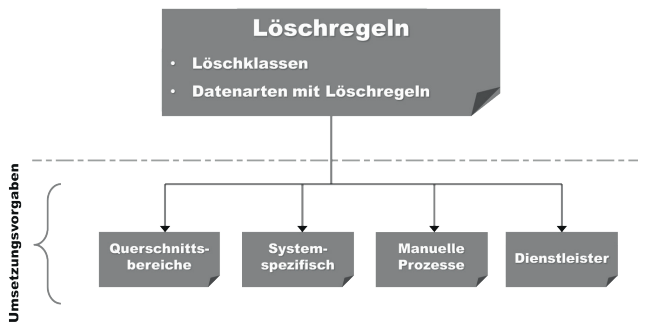
Diese Abweichungen von den Regelprozessen der Verarbeitung unterliegen zwar dem Vorbehalt der datenschutzrechtlichen Zulässigkeit, aber sie schaffen die Voraussetzungen für ein umfassendes Löschkonzept, das auch Sondersituationen mit definierten Prozessen behandelt.

4.4 Kein Konzept ohne Dokumentation

Die Dokumentationen von Löschregeln und Umsetzungsvorgaben sollen voneinander getrennt werden. Aus der Perspektive der Norm ergibt sich damit die logische Dokumentationsstruktur in Abb. 2.

Das einzige eigenständige „Pflichtdokument" nach den Empfehlungen der Norm ist der Katalog der Löschregeln. Alle anderen Inhalte können in bestehende Dokumente der verantwortlichen Stelle integriert werden, wenn sich dies anbietet.

Abb. 2 | Dokumentationsstruktur eines Löschkonzepts.[11]



4.5 Keine Kontinuität ohne Verantwortliche

Die DIN 66398 fordert, dass ein einmal erstelltes Löschkonzept gemäß der Entwicklung von Recht, Fachprozessen und IT-Systemen fortgeschrieben wird. Die Norm benennt deshalb Aufgaben, für die die Verantwortlichkeiten festgelegt werden müssen. Dazu gehören die Pflege des Katalogs der Löschregeln und die Entwicklung und Fortschreibung von Umsetzungsvorgaben.

In der Norm werden außerdem Informationspflichten und Freigabebeteiligungen empfohlen, damit die datenschutzrechtliche Zulässigkeit von Löschregeln durch den Datenschutzbeauftragten geprüft werden kann, z. B. bei Dokumentänderungen, einigen Aktivitäten des Change-Managements oder bei Systembeschaffungen.

10 Treten bestimmte Fälle dieser Art häufiger auf, bietet es sich an, eine Datenart mit Löschregel zu definieren. Die relevanten Datenobjekte können dann beispielsweise in einem Prozess gekennzeichnet und mit einer Löschmaßnahme im Regelbetrieb behandelt werden.

11 Abb. nach DIN 66398.

5 Chancen durch die neue Norm

5.1 Löschen wird einfacher

Die DIN 66398 verschafft den Organisationen, die sie anwenden, große Vorteile: Wesentliche Vorarbeiten, mit denen ein Löschprojekt erst konzipiert werden müsste, stehen zum Projektbeginn fertig zur Verfügung. Erfahrungen mit der Vorgehensweise müssen nicht teuer gewonnen, sondern können schnell genutzt werden.

Mit einem Löschkonzept schafft die verantwortliche Stelle die Voraussetzungen, um die datenschutzrechtlichen Löschvorgaben einzuhalten. Den Vorschlägen der DIN 66398 liegt die Annahme zugrunde, dass die durchgängige Löschung personenbezogener Daten einen tragfähigen Kompromiss zwischen rechtlichen Vorgaben und praktischen Anforderungen erfordert. Diesen Kompromiss muss die verantwortliche Stelle für ihre Bestände selbst finden. Dabei muss sie die Zulässigkeit nach den für sie einschlägigen Rechtsvorschriften beachten. Wenn Standardlöschfristen genutzt werden können, können Löschregeln mit sehr hoher Effizienz festgelegt werden.

Umsetzungsvorgaben bieten außerdem eine sehr gute Grundlage, um Audit-Pläne zu erstellen. Aus den Vorgaben können Prüfbedingungen sehr einfach abgeleitet werden.

Werden die in der Norm vorgeschlagenen Prozesse etabliert, kann dies auch dazu beitragen, den Datenschutz insgesamt besser im Unternehmen zu verankern.

5.2 Projekt „Löschkonzept"

Um in einer verantwortlichen Stelle ein Löschkonzept gemäß DIN 66398 zu etablieren, ist es in der Regel sinnvoll, ein eigenes Projekt „Löschkonzept" durchzuführen. Aufgabe eines solchen Projekts ist es, die in der Norm vorgeschlagene Vorgehensweise auf das Unternehmen zu übertragen. Meist wird es hilfreich sein, in zwei Phasen vorzugehen: zunächst die Definition der Löschregeln vorzunehmen und danach eine Umsetzungsphase anzuschließen.

In der ersten Projektphase sollte der Katalog der Löschregeln möglichst vollständig erstellt werden. Dazu sind erfahrungsgemäß mehrere Abstimmungsrunden mit Fachverantwortlichen, Juristen, Technikern und Datenschützern notwendig. Ein möglichst vollständiger, präziser Katalog ist jedoch unverzichtbar um Überraschungen bei der späteren Umsetzung zu vermeiden.

Für die Arbeiten in der Umsetzungsphase können dann Prioritäten bezüglich der Reihenfolge gesetzt werden, die sich beispielsweise an der Sensitivität der Datenarten, an Abhängigkeiten zwischen Systemen oder an Zeitpunkten für anstehende Release-Wechsel orientieren.

Sind die ersten Umsetzungsaufgaben abgeschlossen, sollten die Regelprozesse der Organisation angepasst werden. Hiervon sind zum Beispiel die Prozesse des Change-Managements und zur System-Beschaffung betroffen, in die Löschregeln als Anforderungen einfließen. Der Datenschutzbeauftragte muss in diese Prozesse geeignet eingebunden werden – sowohl um die Anwendung bestehender Löschregeln zu prüfen als auch um bei Bedarf neue Datenarten mit ihren Löschregeln in den Katalog aufzunehmen.

Bei günstigem Verlauf des Projekts entwickelt sich in der Organisation mit der Zeit eine „Löschkultur": Umsetzungsvorgaben zu Löschregeln sind in IT-Projekten selbstverständlich. Vom IT-Betrieb werden technische Mechanismen erwartet und in Regelprozessen gestartet und überwacht.

5.3 Mehr als nur Datenschutz

Neben den positiven Effekten für den Datenschutz tritt vielfach weiterer Nutzen für die Organisation ein: Mit dem Blick auf das Löschen von Daten können Geschäftsprozesse manchmal präzisiert und optimiert werden. Es werden klarere Vorgaben für die Datenhaltung getroffen und überflüssige Bestände abgebaut. Durch eine bessere Übersicht über (zu schützende) Datenbestände können überflüssige Angriffsziele reduziert und Maßnahmen der Informationssicherheit besser gesteuert werden.

Im Zuge der Umsetzung von Löschregeln bietet es sich in manchen Fällen an, Systeme und IT-Prozesse zu entkoppeln, zu konsolidieren oder rückzubauen. Für den IT-Betrieb können sich dadurch Performance-Gewinne und eine verbesserte Stabilität ergeben. Bereinigte Datenbestände reduzieren auch die Kosten künftiger System-Migrationen. Ein Löschkonzept mit seinen Dokumenten nach DIN 66398 ist schließlich auch in Mitbestimmungsverfahren hilfreich.[12]

6 Ausblick

Löschregeln für Branchen
Die DIN 66398 bietet auch Chancen über die Grenzen der jeweiligen verantwortlichen Stelle hinaus. Wenn mehrere Unternehmen einer Branche die Vorgehensweise der Norm anwenden, kann ein gemeinsamer „Basiskatalog" von Löschklassen und Löschregeln entstehen. Dieser reduziert den Aufwand für die Unternehmen der Branche, Löschkonzepte zu entwickeln.

Ein solcher Branchenkatalog kann überdies Anreiz für Hersteller sein, passende Löschmechanismen in ihren Produkten zu implementieren. Dies würde den Beschaffungs- und Pflegeaufwand für Löschmechanismen in den verantwortlichen Stellen weiter reduzieren.

Löschen nach der Grundverordnung
Wenn 2018 die Datenschutz-Grundverordnung der EU in Kraft tritt, ändern sich zwar Rechtsvorgaben. Aber auch die Regeln der Grundverordnung fordern zulässige Zwecke (Art. 6) und setzen die Prinzipien der Zweckbindung und Datenminimierung (Art. 5). Löschpflichten entstehen zusätzlich durch Artikel 17 „Recht auf Löschung". Indirekt dürfte auch das „Recht auf Datenübertragbarkeit" zu Löschanforderungen führen. Löschen ist daher auch unter dem Regime der Grundverordnung geboten. Da die DIN 66398 eine allgemeine Vorgehensweise beschreibt, lässt sich diese auch unter den Vorgaben der Grundverordnung anwenden. In Artikel 24 der Grundverordnung wird zudem gefordert, dass der Verantwortliche den Nachweis erbringen kann, dass die Verarbeitung gemäß der Verordnung erfolgt. Ein Löschkonzept nach DIN 66398 kann ein wichtiges Element für solche Nachweise sein.

Löschen international
Die DIN 66398 ist zwar eine deutsche Norm. Sie beschreibt aber eine allgemeine Vorgehenswiese, die darauf abstellt, dass Organisationen ihre Löschregeln nach den für sie einschlägigen Rechtsvorschriften bilden. Es spricht daher vieles dafür, dass auch Organisationen außerhalb von Deutschland oder Unternehmen, die international tätig sind, ihr Löschkonzept nach der Norm erstellen. Um die DIN 66398 auch international zugänglich zu machen, wird im Rahmen des Normungsprojekts derzeit noch eine englische Sprachfassung erarbeitet.

Löschen als gute IT-Praxis!
Die in der Norm vorgeschlagene Vorgehensweise baut eine große Hürde für das Löschen von pbD ab: Sie zeigt konstruktiv und praxisgerecht, wie Löschregeln definiert und Löschkonzepte etabliert werden können. Dies und die positiven (Neben-)Wirkungen können Organisationen bewegen, Löschen als gute IT-Praxis aufzugreifen. Tun dies viele, wird das offensichtliche Vollzugdefizit beim Löschen reduziert. Dann hätte die neue Norm ihren Zweck erfüllt.

Dank

Diese Norm zu erstellen, war ein großes Projekt und ich bedanke mich ganz herzlich bei allen, die es unterstützt haben. Die Voraussetzung schuf die Toll Collect GmbH, indem sie gestattete, das Thema Löschen so offen und öffentlich zu diskutieren. Ohne die Förderunternehmen wäre ein Normungsprojekt nicht möglich gewesen. Meine Kollegin Karin Schuler, die Diskussionspartner aus den Förderunternehmen, den DIN-INS-Workshops und dem DIN-AK haben mit viel Engagement am Text mitgewirkt. Ein Besonderer Dank geht an Reinhard Fraenkel, ohne dessen Unterstützung, Begleitung und hartnäckiges Suchen nach guten Lösungen weder Löschkonzept, noch Leitlinie oder DIN-Norm entstanden wären. Danke!

Quellen und weiterführende Materialien

[1] DIN 66398:2016-05 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth-Verlag, 2016.
[2] EU DSGV – Datenschutz-Grundverordnung der Europäischen Union in der Fassung des Rats der Europäischen Union 5419/16 vom 06.04.2016 (deutsche Fassung).
[3] Fraenkel, R., Hammer, V. (2007): Rechtliche Löschvorschriften, in: DuD 12/2007, S. 899 ff., Download unter: www.secorvo.de > Publikationen > Fachartikel > 2007.
[4] Hammer, V., Fraenkel, R. (2007): Löschkonzept, DuD 12/2007, S. 905 ff., Download unter: www.secorvo.de > Publikationen > Fachartikel > 2007.
[5] Hammer, V., Fraenkel, R. (2011): Löschklassen – standardisierte Fristen für die Löschung personenbezogener Daten, DuD 12/2011, S. 890 ff., Download unter: www.secorvo.de > Publikationen > Fachartikel > 2011.
[6] Hammer, V., Schuler, K. (2012): Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, 2012, Download unter: www.secorvo.de > Publikationen > Fachartikel > 2012. Dieses Dokument ist eine Vorversion zur Norm.
[7] Hammer, V. / Schuler, K. (2016): Löschen nach Regeln – die neue Norm hilft, CuA – Computer und Arbeit, 1/2016, 30 ff.; Download unter www.Secorvo.de > Publikationen > Fachartikel > 2016.

Eine Übersicht zu den Inhalten der DIN 66398 und weiterführende Hinweise gibt auch die Website http://DIN-66398.de.

12 *Hammer/Schuler CuA 2016.*