Volker Hammer

Löschen nach Regeln

Standardisierungsmöglichkeiten für ein Löschkonzept

1 Motivation

In sehr vielen Geschäftsprozessen und IT-Anwendungen werden personenbezogene Daten verwendet. Diskutiert man mit Anwendern oder Entscheidungsträgern über das Löschen derartiger Daten, so scheinen die Hürden unüberwindlich. So wird beispielsweise vorgebracht: Technisch sei es ungeheuer schwierig oder eine Löschung gar nicht vorgesehen. Oder: Es gäbe niemanden, der entscheiden könne, dass Prozesse abgeschlossen sind und nicht doch noch eine Nachfrage oder Prüfung durch Finanzamt oder Wirtschaftsprüfer erfolgt. Und immer wieder: Man wisse ja auch nicht, ob die Daten nicht doch für eine – noch neu zu entwickelnde – statistische Auswertung, Marketingmaßnahme oder andere Idee benötigt würden.

Viele Anwender wollen Daten schlichtweg nicht löschen. Die personenbezogenen Daten unterliegen aber dem Datenschutzrecht, das auch Löschvorgaben enthält: Sie dienen dem Schutz der Betroffenen, denn nach dem Löschen ist eine unzulässige oder unerwünschte Verwendung der Daten nicht mehr möglich. Die §§ 20 Abs. 2 Nr. 2 und 35 Abs. 2 Nr. 3 BDSG fordern die Löschung personenbezogener Daten, wenn ihre Verarbeitung nicht mehr erforderlich ist. Damit wird § 4e BDSG konkretisiert, denn § 4e Nr. 7 BDSG statuiert die Pflicht der verantwortlichen Stelle, Regelfristen für die Löschung personenbezogener Daten festzulegen. Spezialgesetze können außerdem für bestimmte Datenarten hinsichtlich der Löschung engere Vorgaben als das BDSG treffen.

In der Fachöffentlichkeit ist man sich weitgehend einig, dass bezüglich des Löschens ein großes Vollzugsdefizit besteht – allerdings begleitet von einer gewissen Hilflosigkeit. Die Toll Collect GmbH[1] zeigt jedoch, wie es gehen kann: Sie realisierte schon zum Mautstart ein Löschkonzept für die Mautdaten. Dieses Konzept wurde in den vergangenen Jahren überaus erfolgreich auch für alle anderen Datenbestände mit Personenbezug weiterentwickelt und umgesetzt. Wichtige Elemente der Vorgehensweise wurden schon 2007 veröffentlicht.[2] Aus Kontakten mit dem Deutsches Institut für Normung e. V. (DIN) ergab sich schließlich die Frage, ob die verfolgte Vorgehensweise nicht auf andere Organisationen übertragbar sei. Im Rahmen des Programms „Innovation mit Normen und Standards – INS“ wurde daher ein Projekt durchgeführt (kurz *DIN/INS-Projekt*), um die Standardisierbarkeit des Ansatzes zu prüfen.[3]

2 Unterstützung für das Löschen personenbezogener Daten?

Die oben beschriebenen Bedenken werden selbstverständlich nicht nur aus Bequemlichkeit vorgebracht oder weil interne Blockaden überwunden werden müssen. Auch objektiv verlangt die rechtskonforme Umsetzung der Löschgebote eine höchst komplexe Subsumption für die Bestimmung der Fristen, die den Wegfall der Erforderlichkeit für die Speicherung festlegen. Das sichere und systematische Löschen personenbezogener Daten ist für eine verantwortliche Stelle schwierig, denn:

- für die Fristbestimmung müssen unbestimmte Rechtsbegriffe ausgelegt werden,
- das Ende von Prozessen, in denen die Daten benötigt werden, muss identifiziert werden, um konkrete Löschzeitpunkte festlegen zu können, und
- die Löschmechanismen müssen in den betroffenen IT-Systemen und Prozessen implementiert werden.

Allgemeine und unspezifische Aufforderungen zum Löschen werden in einer verantwortlichen Stelle kaum erfolgreich sein – sie führen allenfalls zufällig und in Einzelfällen zum Erfolg. Angesichts der Komplexität kann die Aufgabe wohl nur nach systematischer Analyse und mit Hilfe klar strukturierter Regeln gelöst werden.

Welche Hilfestellungen sind möglich?

Können die Löschregeln zwischen Organisationen übertragen werden? Im Allgemeinen wohl kaum. Denn das Prinzip der „Erforderlichkeit“ des BDSG stellt auf die zulässigen Verwendungszwecke der verantwortlichen Stelle ab – und die sind so verschieden wie es Unternehmen und Behörden sind. Geschäftsprozesse, Verträge mit Kunden oder Arbeitnehmern, gesetzliche Pflichten oder Aufgaben, die Größe der Organisation oder ihre Technikausstattung unterscheiden sich. All diese Faktoren haben Einfluss auf den richtigen Zeitpunkt der Löschung und auf die daraus resultierenden Löschregeln. Allgemeine, direkt übertragbare Regeln wird es daher nur in gleich gelagerten Anwendungsfeldern wie beispielsweise der Personalverwaltung geben können.

Im DIN/INS-Projekt zum Löschkonzept war daher zu untersuchen, nach welchem Schema eine Organisation ihr Löschkonzept entwickeln kann und welche Aspekte des Löschens von personenbezogenen Daten dabei zwischen Organisationen übertragen werden können. Für diese Aspekte war zu prüfen, ob Hilfestellungen gegeben werden können, um die rechtlichen Pflichten in Organisationen umzusetzen.

Ziel: organisationsspezifisches Löschkonzept

Organisationsweites Löschen muss als eine kontinuierliche Aufgabe verstanden werden. Geschäftsprozesse und die IT-Landschaft sind heute so dyna-

misch, dass die Löschregeln und die Verantwortlichkeiten für die Umsetzung immer wieder zu überprüfen, zu ergänzen und anzupassen sind. Um eine rechtskonforme, geordnete Löschung von personenbezogenen Daten sicherzustellen, müssen verantwortliche Stellen ein Regelwerk entwickeln und Verantwortung für die Aufgaben der Löschung zuweisen. Dieses Regelwerk wird als Löschkonzept bezeichnet.

Zwar müssen konkrete Löschregeln aus den spezifischen Gegebenheiten in der Organisation abgeleitet werden; die Vorgehensweise, um sie festzulegen, ist aber übertragbar. Bei der Toll Collect konnten in den vergangenen Jahren hierzu zentrale Erkenntnisse gewonnen werden. Diese sollten im Rahmen des Projekts mit andern Vertretern der Fachöffentlichkeit diskutiert und verallgemeinert werden.

Mit übertragbaren Hilfestellungen, so die Erwartung, verbessern sich in jeder Organisation die Erfolgsaussichten für die Entwicklung eines konkreten Löschkonzepts wesentlich. Wenn die verantwortliche Stelle auf eine bewährte Vorgehensweise zurückgreifen kann, kann sie Fehlversuche vermeiden.

Die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“[4], im Weiteren kurz: *Leitlinie*, gibt Hilfestellungen für die Kernaufgaben in Löschprojekten. Mit ihrer Hilfe kann ein Löschkonzept effizient erstellt werden. Die Leitlinie ist das Ergebnis des DIN/INS-Projekts, das von intensiven Diskussionen mit Datenschützern aus Industrie und Aufsichtsbehörden begleitet wurde.[5]

3 Die Leitlinie Löschkonzept

In einem Löschkonzept legt eine verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von personenbezogenen Daten erfüllen will. 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, Anforderungen an Prozesse und Verantwortung für die Etablierung, Fortschreibung und Umsetzung des Löschkonzepts.

3.1 Löschregeln festlegen

Ein Löschkonzept kann nur dann mit akzeptablem Aufwand etabliert werden, wenn alle Beteiligten die Löschregeln nachvollziehen können und die Komplexität der Umsetzung überschaubar bleibt. Einfache Regeln sind daher der Schlüssel zum Erfolg.

Kern eines Löschkonzepts ist es, die Löschregeln festzulegen. Eine Löschregel enthält eine Löschfrist und eine Bedingung für den Startzeitpunkt des Fristlaufs. Die Löschregeln werden jeweils für Datenarten bestimmt. In den Datenarten werden einzelne Bestände von personenbezogenen Daten, die in der verantwortlichen Stelle für die gleichen Zwecke verwendet werden, zusammengefasst.[6] Beispielsweise könnten bei einem Telekommunikations-Provider als Datenarten Stammdaten, Standortdaten, Verkehrsdaten, Abrechnungsdaten und Einzelverbindungsnachweise unterschieden werden. Die Bestände einer Datenart werden hinsichtlich der Löschung gleich behandelt.

Datenarten sind meist einfach zu bestimmen. Die genaue Festlegung der „Erforderlichkeit“ als Voraussetzung für eine Löschfrist ist dagegen oft mit sehr großem Aufwand verbunden. Da die Etablierung eines Löschkonzepts an diesem Aufwand scheitern kann,[7] sind besonders hierfür geeignete Ansätze gefordert. Die Leitlinie schlägt dazu die folgenden Vorgehensweisen vor:

- Verwendung von **Standardfristen**. Eine zu differenzierte Landschaft von Löschfristen ist für die Beteiligten in einer Organisation nicht handhabbar. Die Leitlinie geht deshalb von der Annahme aus, dass ein rechtlich vertretbarer Kompromiss zwischen den Löschvorgaben der Rechtsnormen und der Praktikabilität von Löschprozessen gefunden werden muss.[8]
- **Varianten für die Analyse von Löschfristen**. Die Leitlinie geht davon aus, dass Rechtsvorschriften unterschiedlich große Gestaltungsspielräume einräumen, um Löschfristen zu bestimmen: Für wenige Datenbestände kann die Frist aus den Rechtsvorgaben entnommen werden. Spezifische Rechtsvorschriften ohne konkrete Fristvorgabe oder Datenbestände mit hoher Sensitivität erfordern eine enge Fristregelung und daher eine genaue und gegebenenfalls aufwändige Analyse. Ist dagegen nur allgemein die Erforderlichkeit zu beachten, können in vielen Fällen Standardlöschfristen anhand einfacher Kriterien abgeleitet werden. Durch die Varianten können die Aufwände zur Fristanalyse wesentlich verringert werden.
- **Löschklassen** für die Zuordnung von Löschregeln zu Datenarten. Aus den Standardfristen und drei Typen von Startzeitpunkten[9] ergeben sich sogenannte Löschklassen. Die Erfahrungen zeigen, dass die Zuordnung von Löschregeln mit Hilfe der Löschklassen sehr effizient möglich ist und eine übersichtliche Struktur von Datenarten und Löschregeln ergibt.

Es bietet sich an, die Löschklassen in einer Matrix darzustellen. In der Praxis zeigt sich, dass ggf. nicht alle möglichen Kombinationen von Standardfristen und Startzeitpunkten als Löschklassen benötigt werden (siehe Abb. 1). Dadurch wird das Löschkonzept der verantwortlichen Stelle weiter vereinfacht.

Die Leitlinie gibt außerdem eine Reihe von Hinweisen, wie „Nebenbestände“ von Daten behandelt werden können. Beispiele sind die Löschung von Kopien für die Datensicherung, das Löschen in Archiven, Datenabzüge außerhalb von Regelprozessen oder das Vorhalten von Datenbeständen mit Fehlern.

3.2 Vorgaben für die Umsetzung von Löschregeln

Sind die Löschregeln festgelegt, gilt es, sie umzusetzen. Dies soll durch konkrete Umsetzungsvorgaben erfolgen. Sie richten sich an die Mitarbeiter, die für die Datenbestände verantwortlich sind. Nach der Leitlinie können folgende Umsetzungsvorgaben unterschieden werden:

- Umsetzungsvorgaben für Querschnittsbereiche; dazu gehören beispielsweise

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

Beispiel: Löschklassen bei Toll Collect

Legende:

Hellgrau unterlegt	Frist abgeleitet aus allgemeinen Gesetzen
Dunkelgrau unterlegt	Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
Mittelgrau unterlegt	Frist frei gewählt

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

In den Zellen der Matrix sind beispielhaft Datenarten aus dem Kontext des Mautsystems angegeben. Für andere verantwortliche Stellen ergeben sich möglicherweise andere – ggf. auch zusätzliche – Standardfristen und andere Datenarten.[10]

die Maßnahmen zur Behandlung von Protokollen oder Sicherungskopien.
- Umsetzungsvorgaben für einzelne IT-Systeme; diese sind für IT-Systeme festzulegen und zu implementieren, in denen die eigentliche Datenhaltung erfolgt.
- Einzelmaßnahmen zur Löschung von Datenbeständen. Darunter fallen u. a. Anweisungen zum Löschen im allgemeinen Bürobetrieb, Arbeitsanleitungen für die Löschung von Datenbeständen in manuellen Prozessen und die Steuerung der Löschung für einzelne Datenabzüge außerhalb der Regelprozesse.
- Umsetzungsvorgaben für Auftragnehmer; diese müssen durch Verträge und Weisungen geregelt werden.

3.3 Verantwortung, Prozesse und Dokumentationsstruktur

Um ein Löschkonzept erfolgreich und dauerhaft zu etablieren, sind weitere Elemente notwendig, die ebenfalls in der Leitlinie beschrieben werden. Zunächst sind für die Aufgaben im Löschkonzept die Verantwortlichen festzulegen, z. B. in der folgenden Weise:
- **Betrieblicher Datenschutzbeauftragter** (bDSB): Pflege der Dokumente Löschkonzept, Regellöschfristen und Umsetzungsvorgaben für Querschnittsbereiche, sowie Datenschutz-Audits zum Löschen.
- **Für Datenbestände verantwortliche Mitarbeiter**: Umsetzungsvorgaben mit dem bDSB abstimmen und betrieblich überwachen.
- **IT-Entwicklung**: Löschanforderungen durchgängig in allen relevanten Entwicklungs- und Beschaffungsprozessen berücksichtigen.
- **Change-Management**: Freigabe von betrieblich relevanten Änderungen durch den bDSB sicherstellen.

Die Prozesse, in denen Löschmaßnahmen als Umsetzungsvorgabe definiert, implementiert und überwacht werden, sind festzulegen. Dafür sollen möglichst bereits vorhandene Prozesse angepasst werden. Auch die Fortschreibung des Löschkonzepts und der Regellöschfristen sind festzulegen. Formale Festlegungen für Verantwortung und Prozesse sind notwendig. Mindestens genauso wertvoll ist aber ein konstruktives Klima, in dem der Datenschutzbeauftragte, die fachlichen Anwender und die betrieblich Verantwortlichen zusammenarbeiten.[11]

In der Leitlinie werden auch Empfehlungen für die Dokumentationsstruktur gegeben. Demnach entstehende Dokumente sind das Löschkonzept selbst sowie das Dokument „Regellöschfristen“. In letzterem werden die Löschklassen und die Datenarten mit ihren Löschregeln beschrieben. Alle weiteren Dokumente sollen wie vergleichbare Dokumente in der Dokumentenlandschaft der verantwortlichen Stelle eingeordnet werden, beispielsweise Umsetzungsvorgaben für Querschnittsbereiche als Richtlinien. Wo es sich anbietet, können Inhalte auch in bestehenden Dokumenten ergänzt werden, beispielsweise Umsetzungsvorgaben für Einzelsysteme in System- oder Betriebshandbüchern oder Löschregeln für Papierakten in Mitarbeiter-Handbüchern.

Ein Löschkonzept zu etablieren, stellt eine verantwortliche Stelle vor einige Herausforderungen. Daher gibt die Leitlinie auch Hinweise für ein Projekt „Löschkonzept“.

3.4 Abgrenzung der Leitlinie

Die Leitlinie ist fokussiert auf die Elemente eines Löschkonzepts und den Prozess der Einführung. Folgende Aspekte werden nicht betrachtet:
- Konkrete Löschregeln und Löschfristen. Diese hängen von den jeweils einschlägigen Rechtsvorschriften und den zulässigen Zwecken der Verarbeitung durch die jeweilige verantwortliche Stelle ab.
- Technische Mechanismen zur Löschung und deren Sicherheitsniveau. Dazu liegen bereits eine Reihe von Standards und Anleitungen vor, die den Umgang mit klassifizierten Informationen regeln.
- Daten, die keinen Personenbezug aufweisen. Allerdings kann die Vorgehensweise grundsätzlich auch auf solche Datenbestände übertragen werden.

4 Nutzen der Leitlinie

Die Leitlinie bietet umfangreichen Nutzen. Unternehmen, die personenbezogene Daten verarbeiten, können für ihr eigenes Löschkonzept auf einer Vorgehensweise für effiziente Löschprojekte aufsetzen. Sie können damit die Löschung personenbezogener Daten rechtskonform gestalten.

Daneben bietet ein Löschkonzept für die verantwortliche Stelle viele weitere Vorteile. Der Lebenszyklus von Daten wird für die Definition der Löschregeln vom Ende, nämlich vom Zeitpunkt ihrer Beseitigung her gedacht. Dadurch entstehen Anregungen, Prozesse „aufzuräumen“. Das gilt auch für die zu löschenden Datenbestände: Damit Löschfunktionen umgesetzt werden können, müssen Datenschiefstände bereinigt werden. Datenbestände werden verkleinert – das kommt der Performanz von Datenbanken zu Gute. Und schließlich sparen Migrationsprojekte viel Aufwand, wenn sie sich nicht um historische Formate, Altbestände oder andere Restbestände kümmern müssen, die inzwischen gelöscht werden konnten.

Techniker werden der Frage der Löschung in Beschaffungs- und Entwicklungsprojekten sowie im Betrieb höheren Stellenwert einräumen. Die Anforderungen an Produkte und Dienstleister können klar strukturiert formuliert werden.

5 Ausblick

Wenn viele Unternehmen die gleiche Vorgehensweise und die gleichen Begriffe verwenden, könnten sich mittel- bis langfristig branchenspezifisch übertragbare Datenarten und Löschregeln etablieren. Würden diese von den Aufsichtsbehörden akzeptiert, ergäbe sich für die jeweils verantwortliche Stelle hohe Rechtssicherheit im Hinblick auf ihre Löschpflichten. Die Aufsichtsbehörden verfolgen die Arbeiten daher mit Interesse.

Für die Entwicklung neuer Infrastrukturen, beispielsweise E-Mobility oder Smart Grid, werden Datenschutzaspekte einen hohen Stellenwert besitzen. Mit Hilfe der Leitlinie könnten die beteiligten Akteure bereits in sehr frühen Phasen einheitliche Löschregeln für die personenbezogenen Datenbestände festlegen.

Eignung für die internationale Standardisierung

Der Nutzen der Leitlinie für den Datenschutz wäre noch größer, wäre sie als internationaler Standard etabliert. Der Stellenwert von Löschfunktionalitäten in Produkten würde erhöht. Hersteller, die die Umsetzung eines Löschkonzepts systematisch unterstützen, könnten Marktvorteile erwarten. Die Begriffsbildung in einem Standard würde auch die Kommunikation zwischen Kunden und Auftraggebern wie auch intern beim Hersteller erleichtern. Derzeit bemühen wir uns deshalb, auf der Basis der Leitlinie ein internationales Standardisierungsprojekt bei ISO zu etablieren.

6 Referenzen

Für wertvolle Hinweise zu diesem Beitrag danke ich Herrn Reinhard Fraenkel und Frau Karin Schuler.

[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.
[Fraenkel/ Hammer 2007]	Fraenkel, R. / Hammer, V. (2007): Rechtliche Löschvorschriften, DuD 12/2007, 899 ff.; http://www.secorvo.de/publikationen/rechtliche-loeschvorschriften-fraenkel-hammer-2007.pdfa
[Hammer/ Fraenkel 2007]	Hammer, V. / Fraenkel, R. (2007): Löschkonzept, DuD 12/2007, 905 ff.; http://www.secorvo.de/publikationen/loeschkonzept-hammer-fraenkel-2007.pdf
[Hammer/ Fraenkel 2011]	Hammer, V. / Fraenkel, R. (2011): Löschklassen - standardisierte Fristen für die Löschung personenbezogener Daten, DuD 12/2011, 890 ff.; http://www.secorvo.de/publikationen/loeschklassen-hammer-2011.pdf.
[Hammer/ Schuler 2012]	Hammer, V. / Schuler, K. (2012): Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Secorvo, Karlsruhe, 2012; http://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf.

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

2 [Fraenkel/ Hammer 2007], [Hammer/ Fraenkel 2007], [Hammer/ Fraenkel 2011]. Zu Erfahrungen bei der Umsetzung eines Löschkonzeptes siehe auch Fraenkel in diesem Heft.

3 Das Programms „Innovation mit Normen und Standards“ wird vom Bundesministerium für Wirtschaft und Technologie gefördert. Projektträger ist das DIN.

4 [Hammer/ Schuler 2012]

5 Beteiligt waren z. B. Daimler AG, Deutsche Bahn AG, TÜV Informationstechnik GmbH, SAP AG, Swiss Reinsurance Company Ltd., der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und das Unabhängige Landeszentrums für Datenschutz Schleswig-Holstein.

6 Die Datenarten sind mindestens so aufzuteilen, wie es rechtlich unterschiedliche Verwendungszwecke gibt. Es spricht aber nichts dagegen, weitere fachliche Aspekte zu berücksichtigen und eine feinere Aufteilung vorzunehmen. Dadurch kann z. B. dem Sprachgebrauch der Anwender für ihre Datenbestände Rechnung getragen werden.

7 [Hammer/ Fraenkel 2011]

8 Selbstverständlich können keine beliebigen Kompromisse gewählt werden. Beispielsweise ist im Falle einer Auswahlentscheidung zwischen zwei Fristen die kürzere zu wählen. Die Wahl von Standardlöschfristen muss auch vor der Aufsichtsbehörde vertreten werden können.

9 Die Typen sind: Zeitpunkt der „Erhebung der Daten“, „Ende eines Vorgangs“ und „Ende der Beziehung zum Betroffenen“.

10 Die Grafik wurde übernommen aus [Hammer/ Schuler 2012].

11 Siehe dazu auch Fraenkel in diesem Heft.