Das große Reinemachen

Standards für Löschkonzepte und ihr Nutzen für die Informationssicherheit

Mit DIN 66398 und ISO/IEC 27555 existieren zwei Standards zu Löschkonzepten für personenbezogene Daten. Unser Autor erläutert, welche Hilfestellung sie auch für die Informationssicherheit bieten können, wie die Informationssicherheit übergreifende Löschkonzepte unterstützen kann und welche Synergieeffekte zwischen Informationssicherheit und Datenschutz hierbei bestehen.

Von Volker Hammer, Bensheim

Die Vorgabe des Datenschutzes, personenbezogene Daten systematisch und kontinuierlich zu löschen, stellt Organisationen vor große Herausforderungen – dasselbe gilt, wenn Datenbestände aus der Perspektive der Informationssicherheit gelöscht werden sollen. Für den Bereich personenbezogener Daten schlagen zwei Standards eine Vorgehensweise vor: die DIN 66398 [1] und die ISO/IEC 27555 [2]. Da liegt es nahe, die Bezüge zur Informationssicherheit zu prüfen und Synergieeffekte zu erschließen.

Löschaufgaben für die Informationssicherheit

Zur Pflichtaufgabe der Informationssicherheit gehört es, Datenträger zu löschen oder zu vernichten, bevor man sie entsorgt, wiederverwendet oder verkauft. Das schließt alle Arten von Datenträgern ein – zum Beispiel Festplatten, Bänder, aber auch Papier, USB-Sticks und DVDs. Um die Vernichtung oder Löschung zu gewährleisten, sind Prozesse zu etablieren, anhand derer Datenträger gesammelt und geeignet behandelt werden. Solche Regelungen lassen sich in Richtlinien festlegen, zum Beispiel für den Lebenszyklus von Datenträgern oder im Mitarbeiterhandbuch durch eine Anweisung zum Entsorgen von Papier und mobilen Datenträgern.

Vor Ort werden diese Vorgaben meist durch Schredder und Sammelbehälter umgesetzt – Dienstleister unterstützen, indem sie gesammelte Datenträger vernichten. Die DIN 66399 *„Büro- und Datentechnik – Vernichten von Datenträgern“* [3,4] definiert maximale Teilchengrößen für die Vernichtung verschiedener Arten von Datenträgern. Dafür wird über Sicherheitsstufen berücksichtigt, welchen Schutzbedarf die jeweils enthaltenen Informationen haben und welchen Aufwand ein Angreifer erbringen müsste, um die vernichteten Daten wiederherzustellen.

Die Vernichtung von Datenträgern ist aber nur ein Baustein in einem Löschkonzept: Vielmehr kann man hierunter umfassender verstehen, alle einmaligen oder regelmäßigen Aufgaben der Löschung in einer geordneten Weise zu steuern. Unter dieser Perspektive ergibt sich ein starker Bezug zum Datenschutz, der Regellöschungen für personenbezogene Daten fordert.

Für die praktische Umsetzung können Synergieeffekte für Informationssicherheit und Datenschutz erschlossen werden: Motiviert durch die Vorgaben für den Datenschutz gibt es sowohl einen nationalen als auch internationalen Standard, die eine Vorgehensweise für ein umfassendes Löschkonzept vorschlagen. Diese eignet sich auch für nicht-personenbezogene Daten und kann ebenso helfen, „klassische“ Vernichtungsaufgaben einzuordnen.

Datenschutzrechtliche Löschaufgaben für Fachprozesse

Datenschutzrechtliche Löschvorgaben sind nicht neu: Bereits das Bundesdatenschutzgesetz (BDSG) von 1990 enthielt in den §§ 20 und 35 entsprechende Regelungen. Auch die Richtlinie 95/46/EG von 1995 enthielt in Art. 6 Abs. 1e eine Vorgabe, die in den Mitgliedstaaten in nationales Recht umzusetzen war. Viele Organisationen ignorierten in der Vergangenheit jedoch die nationalen Vorschriften – die hohen Bußgelder für Verstöße gegen die DSGVO „motivieren“ jetzt offenbar stärker dazu, Maßnahmen zu ergreifen.

Nach Art. 5 Abs. 1 lit. e DSGVO dürfen Daten mit Personenbezug grundsätzlich nur solange gespeichert werden, wie es für die zulässigen Zwecke erforderlich ist. Sind diese Zwecke erfüllt, sind die Daten zu löschen (Grundsatz der Speicherbegrenzung). Alternativ kann der Personenbezug durch Anonymisierung aufgehoben werden.

Anonymisierung ist in vielen Fällen aber schwieriger zu realisieren als Löschen – deshalb wird im Weiteren nur von Löschen gesprochen, auch wenn man die datenschutzrechtliche Vorgabe durch Anonymisierung erfüllen könnte.

Die zulässigen Zwecke ergeben sich aus den Fachprozessen, die generell alle einschlägigen Rechtsregeln einhalten müssen, zum Beispiel auch Aufbewahrungspflichten. Aufgrund der Vorgaben des Datenschutzes werden aus der Perspektive der Fachprozesse regelmäßig personenbezogene Daten löschfällig, weil die damit verbundenen Zwecke erfüllt sind. Da diese Vorgabe für alle personenbezogenen Daten gilt, ist das Löschen eine umfassende Aufgabe für fast jede Organisation – denn in der Praxis gibt es nur wenige Prozesse, die ohne personenbezogene Daten auskommen. Wer die Löschvorgaben der DSGVO erfüllen will, benötigt daher Regelprozesse, mit denen sich löschfällige Daten identifizieren und nachweisbar löschen lassen – denn im Sinne von Art. 5 Abs. 2 DSGVO ist der Aufsichtsbehörde gegenüber nachzuweisen, dass eine Organisation notwendige Maßnahmen ergriffen hat (Grundsatz der Rechenschaftspflicht).

Standards

Zwei Normen schlagen vor, wie Löschkonzepte aufgebaut sein können:

_____ *DIN 66398 „Leitlinie zur Ent-wicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" [1]:* Der Ursprung dieses 2016 verabschiedeten Standards waren Vorgaben für die Datenverwendung durch die Toll Collect GmbH, die in Deutschland die Lkw-Maut einzieht. Sie stand 2004 vor der Herausforderung, dem Bundesamt für Güterverkehr nachzuweisen, dass sie Mautdaten entsprechend der Rechtsvorgaben löscht. Dazu wurde ein Löschkonzept entwickelt, dessen Vorgehensweise die Normung in Deutschland aufgegriffen hat und aus dem unter Beteiligung von Industrie und Aufsichtsbehörden die DIN 66398 entstanden ist. Im Verständnis der Norm stellt eine verantwortliche Stelle in einem Löschkonzept dar, wie sie ihrer Aufgabe nachkommt, personenbezogene Daten zu löschen.

_____ *ISO/IEC 27555 „Guidelines on personally identifiable information deletion" [2]* ist ein weitgehend übereinstimmender internationaler Standard. Auf der Basis einer englischen Sprachfassung der DIN 66398 konnte ein Standardisierungsprojekt bei der ISO eingerichtet werden, dessen Ergebnis im Oktober 2021 die genannte Norm war. Die Vorgehensweise definieren beide Standards daher gleich – Unterschiede sind im Wesentlichen redaktionell. Die vielleicht wichtigste Abweichung betrifft die Definition des Löschens: Die DIN 66398 geht grundsätzlich von sicherem Löschen aus – Inhalte dürfen also nicht wiederherstellbar sein, auch wenn diese Definition durch einen Bezug auf DIN 66399 etwas relativiert wird. Dagegen definiert ISO/IEC 27555 Löschen direkt über einen risikoorientierten Ansatz: Die Wiederherstellung der Daten soll unverhältnismäßigen Aufwand erfordern (s. a. [5]).

Beide Standards wurden von den Löschvorgaben des Datenschutzrechts motiviert und sind deshalb auf ein Löschkonzept für personenbezogene Daten ausgerichtet. Die Vorgehensweise zum Etablieren eines Löschkonzepts lässt sich aber auch auf andere Datenbestände übertragen. Wenn etwa die Informationssicherheit für eigene Daten Löschregeln benötigt, lassen sich diese ohne Bruch in ein Lösch-

konzept entsprechend der Standards integrieren.

Kernelemente der Standards

Die DSGVO verlangt von Organisationen, den Nachweis zu erbringen, dass personenbezogene Daten regelgerecht gelöscht werden. Die in beiden Standards empfohlene Vorgehensweise erreicht genau das: Hat man das Löschkonzept etabliert, liegen Dokumente vor, mit denen dieser Nachweis gegenüber der Aufsichtsbehörde geführt werden kann.

Katalog der Löschregeln

Löschen ist auch deshalb eine große Herausforderung, weil in Organisationen oft nicht klar ist, nach welchen Regeln gelöscht werden soll – ohne diese lassen sich jedoch keine passenden Mechanismen implementieren. Eine zentrale Aufgabe für jedes Löschprojekt ist es deshalb, *Löschregeln* bereitzustellen. Die Standards empfehlen, diese in einem Katalog zu sammeln:

_____ Er soll das zentrale Nachschlagewerk sein, wenn eine Löschregel gesucht wird.

_____ Im Regelkatalog sollen die Löschregeln so begründet werden, dass sie für die Beteiligten in der Organisation und die Aufsichtsbehörde nachvollziehbar sind.

_____ Löschregeln sollen im Regelkatalog *technikunabhängig* definiert werden – was letztlich bedeutet, dass weder das Speichermedium (z. B. Papier, CD, Video-Band oder Festplatte) noch die Art der Speicherung (z. B. PDF, analoges Audio-Signal, Datensatz in einer Datenbank oder strukturierte Speicherung) für diese Beschreibung eine Rolle spielen sollen. So kann man Techniksysteme austauschen, ohne dass sich die Löschregel ändert. Und für konkrete Datenbestände, die unter Umständen an mehreren Stellen gespeichert sind, lässt sich jeweils die gleiche Löschregel anwenden, die bei technikneutraler Formulierung aber nur einmal begründet werden muss.

Löschregeln sollen eindeutig sein. Die Basis für ihre Definition sind gemäß Datenschutzgesetzgebung die zulässigen Zwecke. Die Vorgehensweise der Standards empfiehlt deshalb, die Datenbestände einer Organisation in sogenannte *Datenarten* aufzuteilen. Datenarten sind ein logisches Konstrukt: Jede kann verschiedene Datenobjekte enthalten. Zentrale Anforderung ist aber, dass dies nur Datenobjekte sind, die für die gleichen Zwecke verwendet werden.

Beispiele für Datenarten

_____ Die Datenart „Buchhaltungsdaten“ enthält insbesondere alle Rechnungen, Quittungen, Zahlungsanweisungen an die Bank und Bankbelege wie Kontoauszüge.

_____ Die Datenart „Bewerbungsakte“ umfasst alle personenbezogenen Unterlagen, die in einem konkreten Bewerbungsverfahren entstehen, allem voran die Bewerbungsunterlagen, den Schriftverkehr mit dem Bewerber, die Notizen aus dem Bewerbungsgespräch oder gegebenenfalls Unterlagen eines Assessment-Centers.

_____ Für die Außensicherung von Gebäuden könnte man die Datenart „Bilddaten für den Objektschutz“ definieren.

_____ Im Bereich der Überwachung von IT-Systemen fallen beispielsweise Datenarten an wie „Log-Protokolle zu Seitenabrufen auf Webservern“, „Log-Protokolle auf Applikationsebene“ oder „Log-Protokolle mit Buchhaltungsrelevanz“. Da diese Protokolle jeweils unterschiedlichen Zwecken dienen, sind sie als getrennte Datenarten festzulegen.

Definition von Löschregeln

Für alle Datenarten werden Löschregeln definiert, die jeweils aus einer Regellöschfrist und einem Startzeitpunkt bestehen, ab dem diese Frist gerechnet wird. Die Regellöschfrist gibt die Obergrenze der

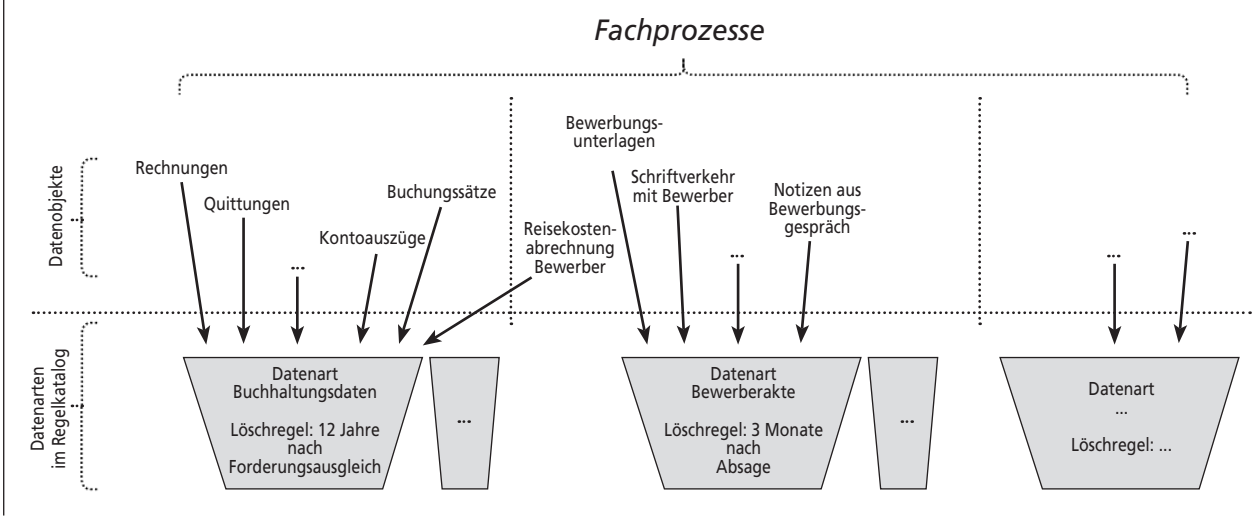


Abbildung 1: Beispielhafte Zuordnung von Datenobjekten zu Datenarten – im Fachprozess „Bewerbungsverfahren“ könnte eine weitere Datenart „Aufzeichnung aus Assessment-Center“ lauten.

Verwendung an: Wenn die Daten im Regelprozess verarbeitet werden und die Regellöschfrist abgelaufen ist, müssen sie gelöscht sein.

Das Vorgehen mittels Datenarten ermöglicht es, die vielfältigen Datenbestände einer Organisation in vergleichsweise wenigen Gruppen zusammenzufassen. Jede Datenart bildet einen logischen Container – das reduziert die Zahl der Löschregeln: Man benötigt nur eine Löschregel für „Buchhaltungsdaten“ und nicht mehrere unterschiedliche für die verschiedenen Datenobjekte. Prinzipiell kann eine Datenart Datenobjekte aus mehrere Fachabteilungen enthalten und wird nur einmal definiert – diese Wiederverwendung reduziert die Zahl der Datenarten weiter.

Dadurch, dass in einer Datenart nur Datenobjekte mit gleichen Zwecken gesammelt werden, ergibt sich, dass sie der gleichen Löschregel unterliegen. Für eine klare Strukturierung der Datenarten empfehlen die Standards daher auch, für jede Datenart genau eine Löschregel zu definieren. Will man innerhalb einer Datenart die Löschregel differenzieren, also beispielsweise Bewerberakten je nach Einwilligung in ein Pooling früher oder später löschen, soll die Datenart aufgeteilt werden.

Zusammenfassung von Regeln zu Löschklassen

Es liegt nahe, die Löschregeln aus der Analyse von Fachprozessen abzuleiten. Das ist manchmal auch zwingend der Fall – würde man diese Prozessanalyse aber für alle Datenarten durchführen, müssten dafür gewaltige Ressourcen aufgewendet werden. Die Standards schlagen einen effizienteren Weg vor, der in vielen Fällen aussichtsreich ist – dieser sei hier nur angedeutet: Anhand von einzelnen repräsentativen Datenarten kann man sogenannte *Löschklassen* bilden. Diese werden durch eine Standardfrist und einen der drei abstrakten Startzeitpunkte ab Erhebung, ab dem Ende eines Vorgangs im Lifecycle der Datenart oder ab dem Ende der Beziehung zum Betroffenen definiert (vgl. Abb. 2). Diese Löschklassen helfen dann dabei, Datenarten einzuordnen und Löschregeln schnell zu definieren.

Standardlöschfristen

abstrakte Startzeitpunkte	Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
ab Erhebung			Mautdaten	Mautdaten mit besonderem Analysebedarf			
ab Ende eines Vorgangs	Web-Logs, nicht-maut-pflichtige Fahrzeuge	Kurzzeit-Doku, Betriebs-Logs	voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Reklamations- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
ab Ende der Beziehung zum Betroffenen				ergänzende Stammdaten		Verträge	Kernstammdaten

Legende: Frist aufgrund … | allgemeiner Gesetze | bereichsspezifischer Gesetze | freier Entscheidung

Abbildung 2: Beispielhafte Matrix von Löschklassen mit ausgewählten Stellvertretern für Datenarten – Standardfristen und Datenarten entstammen hier dem frühen Löschkonzept der Toll Collect (s. a. [6])

Umsetzungsvorgaben – Mechanismen für bestimmte Anwendungsbereiche

Wie beschrieben, sind Löschregeln im Regelkatalog technikunabhängig definiert. Um tatsächlich zu löschen, muss eine Organisation aber Mechanismen implementieren – diese sollen in sogenannten *Umsetzungsvorgaben* dokumentiert werden. Dabei handelt es sich um einen Sammelbegriff für verschiedene Dokumente, in denen man konkret beschreibt, wie bestimmte Datenobjekte gelöscht werden. Jede Umsetzungsvorgabe bezieht sich auf einen bestimmten Gegenstandsbereich und die Datenarten, die dort verwendet werden:

_____ Ein Systemlöschkonzept definiert für ein IT-System (oder ein großes Modul einer Anwendung), wie die Löschung in den einzelnen Tabellen, für Dateien oder andere Datenstrukturen implementiert wird.

_____ Eine Arbeitsanweisung beschreibt für Dateien oder andere Datenobjekte unter manueller Verwaltung, wie löschfällige Bestände aufgeräumt werden.

_____ Eine datenschutzrechtliche Weisung trifft Vorgaben für einen Dienstleister.

_____ Richtlinien können die Umsetzung in Querschnittsbereichen regeln, zum Beispiel einheitlich für Backups, Log-Files oder die Entsorgung von IT-Komponenten.

Umsetzungsvorgaben greifen dabei auf die Löschregeln des Katalogs zurück. Jede Umsetzungsvorgabe soll für ihren Geltungsbereich insbesondere darstellen, wie man im Löschmechanismus Startzeitpunkt und Regellöschfrist bestimmt, wer dafür verantwortlich ist, Löschläufe zu starten und wie und wo die einzelnen Löschläufe dokumentiert werden.

Für IT-Anwendungen legt man dabei die technischen Parameter fest: Welches Attribut in oder zu einem Datenobjekt liefert den konkreten Wert für den Startzeitpunkt? In welchem Konfigurationsparameter lässt sich der Wert für die Regellöschfrist einstellen? So wird die Bedingung festgelegt, die im Löschlauf die löschfälligen Datenobjekte identifiziert – diese liefert im Übrigen auch genau diejenigen Informationen, die ein Auditor benötigt, um am System zu prüfen, ob das Löschen korrekt ausgeführt

wird und der Datenbestand aufgeräumt ist.

Wenn ein System in mehreren Tabellen unterschiedliche Datenarten speichert (z. B. Buchhaltungsdaten und Kernstammdaten), können diese je nach Implementierung auch von einem Mechanismus gelöscht werden. Entscheidend ist, dass die Löschregel je Datenart geeignet in der Technik abgebildet ist.

Über die Umsetzungsvorgaben lässt sich überdies auch definieren, welches Sicherheitsniveau für den Löschmechanismus gefordert und wie dieses zu erreichen ist. In manchen Fällen kann es außerdem notwendig sein, spezielle Maßnahmen vorzubereiten, die nach Recovery-Situationen einen wiedereingespielten löschfälligen Bestand in der Produktion aufräumen.

Empfehlungen und Praxis

Aus den bisher beschriebenen Kernelementen ergibt sich eine klare, logische Dokumentationsstruktur für das Löschkonzept: Durch eine Organisationsanweisung wird der Regelkatalog verbindlich verabschiedet und die Verantwortlichkeiten auf der Umsetzungsebene werden geregelt – unterschiedliche Dokumente beschreiben die Maßnahmen auf der Umsetzungsebene (vgl. Abb. 3).

Beispielhafte Eckdaten zu Regelkatalogen

Jede Organisation benötigt ihren eigenen Regelkatalog, denn sie ist selbst für ihre Datenhaltung verantwortlich, verwendet ihre eigenen Prozesse und unterliegt vielleicht auch spezifischen rechtlichen Vorgaben. Mittelständische Unternehmen (auch größere) haben oft ein konzentriertes Produktportfolio. Ein Regelkatalog, der die Datenarten der Kern-, Management- und Unterstützungsprozesse abdeckt, kann etwa 140 Datenarten umfassen und einen Umfang in der Größenordnung von 300 Seiten haben. Er ist ein konsolidiertes Nachschlagewerk – jede Fachabteilung benötigt allerdings nur einen Ausschnitt daraus.

Iterative Identifizierung von Datenarten

Grundsätzlich werden Datenarten mit ihren Löschregeln iterativ identifiziert: Die Beteiligten im Löschprojekt prüfen, wie sie einen Datenbestand in Datenarten aufteilen, beispielsweise für eine Fachabteilung.

Ein Beispiel: Im Rechnungswesen kann auffallen, dass man zwischen den Datenarten „Buchhaltungsdaten“, welche die eigentlichen Buchungsbelege enthalten, und „Stammdaten der Kunden“ unterscheiden muss. Denn Buchhaltungsbelege sind einem Konto zugeordnet und werden typischerweise nach der Aufbewahrungspflicht der Abgabenorgdnung (§ 147 AO) 10 Jahre nach Ende des Kalenderjahres löschfällig. Als Löschregel ergibt sich beispielsweise 12 Jahre nach Forderungsausgleich. Das Konto für die Belege wird aber aus den Stammdaten gebildet: Diese kann man daher erst löschen, wenn die letzten Buchhaltungsdaten gelöscht wurden und die Beziehung zum Kunden beendet ist. Als Löschregel könnte sich ergeben 12 Jahre nach Ende der Beziehung. In den Stammdaten der Kunden sind aber möglicherweise sensitive Merkmale enthalten, etwa eine Bankverbindung. In der Diskussion der Datenart stellen die Beteiligten fest, dass es keine Zwecke gibt, die dafür eine lange Aufbewahrung nach dem Ende der Kundenbeziehung rechtfertigen. Demnach könnte man zwischen den Datenarten „Kernstammdaten Kunde“ (12 Jahre für das Konto) und „erweiterte Stammdaten Kunde“ (Löschregel 1 Jahr nach Ende der Beziehung) unterscheiden.

Löschanforderungen in neuen IT-Projekten

Löschkonzepte sollten nachhaltig etabliert werden. Deshalb empfiehlt es sich dringend, Löschanforderungen in den Anforderungen für neue IT-Systeme oder Prozessanpassungen von vornherein mit zu berücksichtigen. Beschaffungs- und Implementierungsprozesse sollte man entsprechend anpassen – als Liefergegenstand kann beispielsweise die Beschreibung der Umsetzung gefordert werden.

Bestehende Dokumentation ergänzen

Umsetzungsvorgaben können zwar auch als eigenständige Dokumente erstellt werden – in der Regel ist es aber sinnvoller, sie in bestehende Dokumente zu integrieren. So soll ein Systemlöschkonzept den Administratoren darstellen, wie der

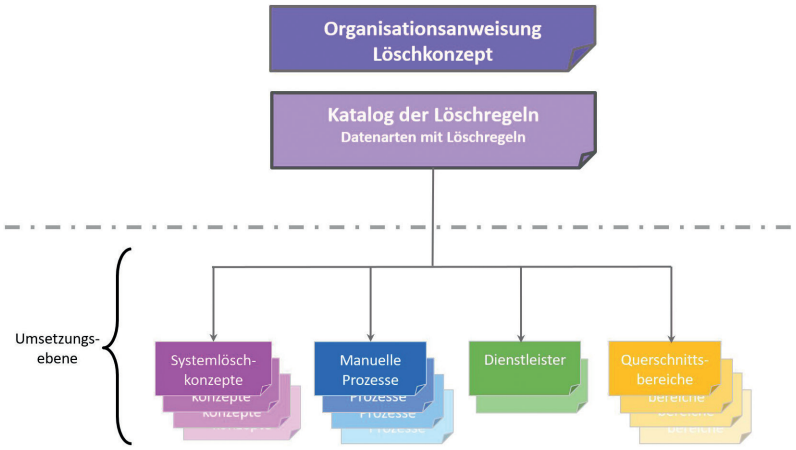


Abbildung 3: Dokumentationsstruktur eines Löschkonzepts in Anlehnung an DIN 66398 und ISO/IEC 27555

Löschmechanismus zu konfigurieren und zu verwenden ist. Daher kann man es auch gut als Kapitel in ein Betriebshandbuch integrieren.

Für ein effizientes Löschen in manuellen Prozessen muss in der Regel die Ablage der Datenobjekte gut aufgebaut sein. Für den „Löschlauf" braucht es dann nur wenige Schritte: die löschfälligen Datenobjekte identifizieren, einen geeigneten Mechanismus zum Überschreiben anwenden und die Maßnahme dokumentieren. Das alles lässt sich gut in bestehende Arbeitsanweisungen integrieren – gesteuert wird die regelmäßige Ausführung dann zum Beispiel über eine Wiedervorlage.

Verankerung und Pflege des Löschkonzepts

Schließlich empfehlen die Standards auch noch, dass die Vorgehensweise und die Verantwortlichkeiten für die Pflege des Regelkatalogs in der Organisation klar geregelt ist. Das kann etwa in einer Organisationsanweisung oder der Datenschutz-Leitlinie erfolgen. Dort lässt sich auch festlegen, welche Führungsebene dafür verantwortlich ist, dass Löschmechanismen implementiert werden. So könnte man zum Beispiel Bereichsleitern zuschreiben, dass sie innerhalb ihrer Datenbestände auch für die Löschung sorgen müssen.

Datenarten für die Informationssicherheit

Für die Definition von Datenarten im Regelkatalog ist die Informationssicherheit eine Fachabteilung von vielen: Sie benötigt bestimmte (oft auch personenbezogene) Datenbestände für ihre spezifischen Zwecke. Im Rahmen der Regelbildung wird dann geklärt, welche Regellöschfrist für welche Datenbestände der Informationssicherheit datenschutzrechtlich vertretbar ist; gegebenenfalls werden auch andere Zwecke der Organisation für die Daten berücksichtigt.

Zu den relevanten Datenarten gehören manche der schon oben erwähnten Beispiele, unter anderem aber auch spezifische Sicherheitslogs aus Firewalls, Meldungen von IDS-Sensoren oder die Dokumentation von Berechtigungsänderungen. Die Unterlagen, die benötigt werden, um eine Anomalie in den Log-Protokollen daraufhin zu prüfen, ob zum Beispiel ein Angriff vorliegt und welche Schäden er verursacht hat, könnte man etwa in einer weiteren Datenart „Vorfalls-Akten" erfassen – für diese könnte eine längere Regellöschfrist geboten sein als für ansonsten unauffällige Protokolldaten.

Für manche Datenbestände können auch Zielkonflikte bestehen – etwa zwischen den Interessen der Informationssicherheit (viel und lange aufheben) und des Datenschutzes (möglichst früh löschen und nur ausgewählte Daten verarbeiten). Die Vorgehensweise im Regelkatalog führt dazu, dass entsprechende Argumente offengelegt und Kompromisse gefunden und dokumentiert werden.

Daneben könnten in der Informationssicherheit auch Löschregeln für Bestände hilfreich sein, die als Betriebsgeheimnisse eingestuft werden, aufgrund vertraglicher Regelungen als vertraulich zu behandeln sind oder dem Geheimschutz unterliegen.

Synergieeffekte

Die gemeinsame Motivation von Datenschutz und Informationssicherheit besteht darin, dass gelöschte Daten nicht abfließen und auch nicht auf andere Art missbraucht werden können – ein Löschkonzept hilft, das systematisch zu erreichen.

Wie gesagt, eignet sich die beschriebene Vorgehensweise nicht nur für den Datenschutz, sondern ist generell für Löschkonzepte nutzbar – sie kann also im Besonderen auch die Löschaufgaben der Informationssicherheit abdecken. Solche Aufgaben werden beispielsweise im IT-Grundschutz-Kompendium unter CON.6 *„Löschen und Vernichten"* [7] formuliert. Auch die neue ISO/IEC 27002:2022 (vgl. S. 30) definiert ein Control zum Löschen – unter 8.10 wird gefordert: „Information stored in information systems, devices or in any other storage media should be deleted when no longer required." Am Ende dieses Controls wird auf ISO/IEC 27555 hingewiesen.

An der Entwicklung eines Löschkonzepts sind viele Personen beteiligt: oberes Management, Projektleiter, Fachexperten, Datenschützer, IT-Spezialisten, IT-Sicherheitsbeauftragte und Entwickler. Beide Standards bieten für die Kommunikation erprobte Begriffe an, die eine gute Verständigung ermöglichen.

In der Diskussion von Datenarten und für die Umsetzung stellen sich in jeder Organisation eine Reihe von praktischen Fragen: Wie sollen Backups gelöscht werden, die löschfällige Daten enthalten? Wie kann man einzelne Datenobjekte von der Löschung ausnehmen, beispielsweise weil sie noch als Beweismittel in einem Rechtsstreit benötigt werden? Wie lässt sich eine Kontrolle von Ausnahmen bei der Regellöschung erreichen, die beispielsweise durch Datenabzüge oder bei Technikfehlern auftreten? Die Standards enthalten Vorschläge, wie sich diese Themen konsistent im Rahmen der Vorgehensweise behandeln lassen. Auch die eingangs genannten Richtlinien zum Entsorgen von Datenträgern oder von Papier fügen sich nahtlos in die Ebene der Umsetzungsvorgaben für Querschnittsaufgaben ein.

Die Standards empfehlen eine allgemeingültige und erprobte Vorgehensweise. Darüber hinaus bietet sich mit einem Löschkonzept die Chance, die im Folgenden

näher beschriebenen Synergieeffekte für Informationssicherheit und Datenschutz zu erschließen.

Übersicht über Datenbestände

Um ein Löschkonzept systematisch zu erstellen und zu pflegen, müssen im Projekt alle Datenbestände der Organisation betrachtet und dokumentiert werden. Daraus entsteht eine Übersicht, die sowohl für die Arbeit des Datenschutzbeauftragten als auch für den Informationssicherheitsbeauftragten sehr hilfreich ist. In der Regel werden dabei einige weiße Flecken auf der Daten-Landkarte identifiziert und befüllt – diese Bestände kann man dann in die Regelprozesse einbeziehen. Das Projekt „Löschkonzept" bietet deshalb für die Informationssicherheit die Chance, sich in eine Bestandsaufnahme einzuklinken und daraus bestehenden Handlungsbedarf zu erkennen. Unter anderem können sich so auch Erkenntnisse für die Business-Impact-Analyse (BIA) ergeben.

Durchgängige Sicherheitsklassifikation von Datenarten

Der Regelkatalog bietet mit den Datenarten ein sehr umfassendes Bild über die Datenbestände der Organisation. Da die Datenarten nach Zwecken „sortiert" sind, haben sie oft auch den gleichen Schutzbedarf. Deshalb bietet es sich an, im Regelkatalog eine Klassifikation der Datenarten unter Gesichtspunkten der Informationssicherheit zu ergänzen – das ist vergleichsweise wenig Aufwand und erhöht den Nutzen des Regelkatalogs. Wenn nicht-personenbezogene Daten als Datenarten geführt werden, kann auch für diese die Informationssicherheitsklassifikation angegeben werden. Im Ergebnis entsteht ein umfassendes Nachschlagewerk – auch für die Informationssicherheit. Voraussetzung ist allerdings, dass eine Sicherheitsklassifikation für Informationen überhaupt definiert und eingeübt ist.

Wissen um Probleme und Sicherheit von Löschmechanismen

In vielen Organisationen ist die Informationssicherheit stärker in technische Themen involviert als der Datenschutz. Das kann als eine sinnvolle Arbeitsteilung gesehen werden, denn in diesem Bereich überschneiden sich viele Ziele.

Wenn die Löschregeln umgesetzt werden sollen, stellt sich häufiger die Frage, wie sich sicheres Löschen erreichen lässt. Hier könnte die Informationssicherheit entsprechend unterstützen: In den Umsetzungsprojekten sollten die Löschmechanismen hinsichtlich ihrer Sicherheitseigenschaften und Löschwirkung geprüft werden – das könnte die Informationssicherheit beitragen. Wenn für das Löschen im IT-System Defizite erkannt werden, lassen sich vielleicht pragmatische Workarounds identifizieren und – soweit es sich um personenbezogene Daten handelt – mit dem Datenschutz abstimmen.

Für die physische Vernichtung von Datenträgern liefert die DIN 66399 [4] Vorgaben. Festplatten können zudem durch entsprechende Programme oder Hardware-Befehle vor der Wiederverwendung in anderem Kontext vollständig gelöscht werden. Auf weiterführende Quellen für sicheres Löschen verweisen beispielsweise auch [2] und [7].

Für die Regellöschung in IT-Prozessen wird man auf eine große Bandbreite verschiedener Löschaufgaben treffen: von einzelnen Merkmalen über komplexe Datenobjekte bis hin zu Containern oder virtuellen Maschinen in der Cloud. Dann erfordert sicheres Löschen häufig ein Überschreiben von Speicherbereichen, wenn man forensische Möglichkeiten zur Wiederherstellung berücksichtigt. In Anwendungssystemen kann dabei schon das Überschreiben einzelner Datensätze schwierig sein, wenn sie nicht darauf vorbereitet sind. In Zeiten von Flash-Speichern bildet die Hardware eine zusätzliche Hürde: Bei Solid-State-Disks (SSD) und anderen Flash-Medien verhindert ein Speichercontroller den direkten Zugriff auf die abgelegten Daten in den physischen Sektoren – Speicherblöcke werden nur logisch freigegeben und können mit hardwarenahen Werkzeugen dennoch weiter ausgelesen werden.

Neuere Ansätze versuchen daher, Datensätze oder Teile davon durchgängig nur verschlüsselt zu speichern und später – statt sie zu löschen – den Schlüssel zu vernichten (sog. Crypto-Shredding). Die Praxis wird allerdings noch zeigen müssen, wie gut solche Techniken die Aufgabe lösen können.

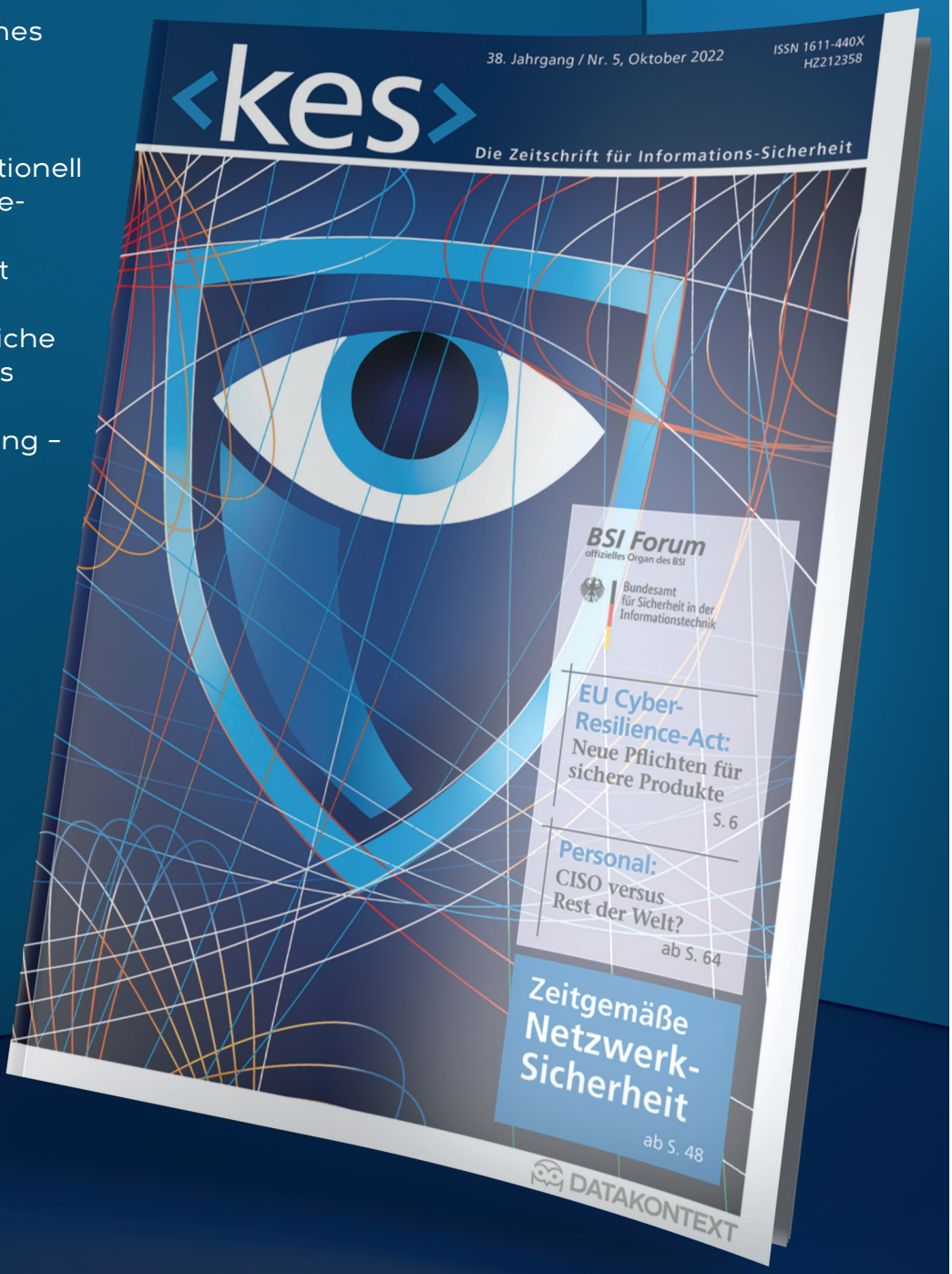
Bewusstsein für Datenschutz und Informationssicherheit

Für die Definition von Löschregeln und deren Umsetzung müssen die Fachabteilungen einbezogen werden. Die Erfahrung zeigt jedoch, dass die Beteiligten zunächst skeptisch auf die Aufgabe reagieren. Die Vorgehensweise nach den Standards – kombiniert mit einer guten Projektorganisation – macht die Aufgabe aber durchaus handhabbar.

Außerdem wird in der Auseinandersetzung mit dem Thema allen klar, dass das Löschen nicht nur eine Datenschutzvorgabe, sondern grundsätzlich sinnvoll ist: Am Anfang ist es mühsam, Löschaufgaben aufzusetzen. Als Lohn winken aber neben der Compliance zum Beispiel verbesserte Fachprozesse durch konsolidierte Datenbestände, Stabilität und Performance von Anwendungssystemen, weil Datenbestände deutlich reduziert werden

Need to know für CISO & Co.

- <kes> liefert strategisches Wissen für Security-Verantwortliche
- <kes> informiert redaktionell unabhängig zu Management und Technik der Informations-Sicherheit
- <kes> enthält das amtliche Organ des Bundesamts für Sicherheit in der Informationsverarbeitung – BSI-Forum
- <kes> kostet im Jahr weniger als zwei Beraterstunden



<kes>
Die Zeitschrift für Informations-Sicherheit

Für 159,00 € jährlich (inkl. MwSt. und Versandkosten) erhalten Sie alle zwei Monate eine gedruckte Ausgabe und für bis zu fünf Mitarbeiter am belieferten Standort Online-Zugriff auf alle aktuellen Beiträge sowie das <kes>-Archiv.

Online bestellen: datakontext.com/kes
oder per Mail: abo@kes.de

DATAKONTEXT

können, und/oder Kosteneinsparungen in IT-Projekten, weil man (nunmehr gelöschte) Altbestände nicht mehr teuer migrieren muss.

Der Regelkatalog bietet mit den Datenarten dann auch klare Soll-Vorgaben für die Implementierung. Zudem ist offensichtlich: Das Thema wird dauerhaft nur dann systematisch behandelt, wenn für alle neuen IT-Projekte und Änderungen in Fachprozessen die Anforderungen zum Löschen von Beginn an mitgedacht werden. Das klingt altbekannt für die Informationssicherheit – denn auch hier gilt: Je früher sie in Projekte involviert wird, desto besser kann eine „sichere Gestaltung" gelingen.

Die Vorgaben der DSGVO sind eine starke Anforderung, Projektprozesse zu ergänzen und Löschvorgaben beispielsweise in Quality-Gates für Meilensteine zu prüfen. Wenn Datenschutz und Informationssicherheit eng zusammenarbeiten, kann sich die Informationssicherheit hier einklinken. Dann haben beide Bereiche das Potenzial, sehr früh in Projekten beteiligt zu werden. Das wiederum eröffnet die Chance, von Anfang an konstruktiven Einfluss auf Ziele und Anforderungen zu nehmen und so als Gestalter wahrgenommen zu werden – und nicht erst am Projektende als Störer oder Verhinderer.

Fazit

Die Löschvorgaben der DSGVO liefern starke Argumente, ein umfassendes Löschkonzept zu etablieren. Die Löschaufgaben der Informationssicherheit lassen sich dort integrieren. Ein übergreifendes Löschkonzept wiederum kann die Informationslage für Datenschutz und Informationssicherheit gleichermaßen verbessern.

Synergieeffekte bieten eine zusätzliche Motivation, damit Datenschutz und Informationssicherheit beim Thema Löschen gemeinsam auftreten. Um Löschroutinen nachhaltig zu etablieren, muss auch dieses Thema frühzeitig in Projekten berücksichtigt werden. Damit bietet ein Löschkonzept eine gute Gelegenheit für beide Bereiche, eine Rolle als Gestalter einzunehmen. Dabei können dann auch andere Themen aus Datenschutz und Informationssicherheit proaktiv mitgestaltet werden – wie Berechtigungskonzepte, der Umfang der Datenhaltung sowie Fragen von Archivierung, Monitoring oder Logging-Strategien.

Wenn Datenschutz und Informationssicherheit als Gestalter agieren, kann das den Blick aus den Fachabteilungen auf beide Aufgabenbereiche verändern und die Themen besser in der Organisation verankern. Die Erfahrung aus datenschutzrechtlichen Löschprojekten zeigt, dass solche Veränderungen wirklich stattfinden können – ein gutes Löschkonzept kann dazu ein Auslöser sein. ■

Dr. Volker Hammer ist Mitarbeiter bei der Secorvo Security Consulting GmbH (www.secorvo.de) mit Arbeitsschwerpunkten in Datenschutz und Informationssicherheit. Seit 2004 berät er zu Löschkonzepten, unter anderem auch bei Toll Collect – er war Editor der DIN 66398 und Co-Editor im Projekt für die ISO/IEC 27555. Ab Juni 2022 wird er freiberuflich Löschprojekte unterstützen (www.loeschprojekte.de).

Literatur

[1] Deutsches Institut für Normung e. V. (DIN), Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, DIN 66398:2016, Mai 2016, www.din.de/de/wdc-beuth:din21:249218525

[2] International Organization for Standardization (ISO), Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion, ISO/IEC 27555:2021, Oktober 2021, www.iso.org/standard/71673.html

[3] Deutsches Institut für Normung e. V. (DIN), Büro- und Datentechnik – Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe, DIN 66399-1:2012, Oktober 2012, www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:155420083

[4] Deutsches Institut für Normung e. V. (DIN), Büro- und Datentechnik – Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern, DIN 66399-2:2012, Oktober 2012, www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:155420668

[5] Volker Hammer, Die Webseite zur DIN 66398/Leitlinie Löschkonzept – Inhalte, Nutzen, Bezüge, Materialien, www.din-66398.de

[6] Volker Hammer, DIN 66398 – Die Leitlinie Löschkonzept als Norm, DuD 8/2016, S. 528, online verfügbar über https://secorvo.de/publikationen/din-66398-hammer-2016.pdf

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Baustein zur Konzeption und Vorgehensweise – CON.6: Löschen und Vernichten, Februar 2021, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2022.pdf?__blob=publicationFile&v=3#download=1