Löschen nach Konzept

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) verpflichtet ab Ende Mai 2018 mit neuem Nachdruck zum Löschen personenbezogener Daten. Diese Herausforderung rückt für viele Organisationen derzeit in den Fokus ihrer Datenschutz-Projekte. Was aber muss gelöscht werden und wie gestaltet man ein durchgängiges Löschkonzept sinnvoll? Die DIN 66398 macht Vorschläge für ein effizientes Vorgehen.

Text: **Volker Hammer** (Secorvo Security Consulting GmbH)

Was und warum Löschen

Das Löschen personenbezogener Daten wird bereits seit den 1990er Jahren vom Bundesdatenschutzgesetz (BDSG) und auch von der DSGVO gefordert. Die DSGVO ist ab Ende Mai 2018 anzuwenden und löst dann viele nationale Datenschutzvorschriften ab. Sie enthält unter anderem wesentlich höhere Bußgelder, die bis zum Maximum von 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes einer Organisation betragen können. In vielen Organisationen hat die Umsetzung der DSGVO daher die Aufmerksamkeit der Geschäftsführung.

Foto © sebra/fotolia

Personenbezogene Daten sind nach der DSGVO alle Informationen, die sich auf eine identifizierbare natürliche Person (betroffene Person) beziehen. Identifizierbar ist eine Person auch, wenn Daten über beliebige Indirektheitsstufen und beliebige Merkmale zugeordnet werden können. Dabei sind alle Merkmale und Merkmalskombinationen für die Identifizierung zu berücksichtigen, die der verantwortlichen Stelle zugänglich sind, beispielsweise Personalnummern, Kontonummern, E-Mail-Adressen oder auch IP-Adressen oder eindeutige Bewegungsmuster. Für das Kriterium der Identifizierbarkeit sind auch Informationen außerhalb der verantwortlichen Stelle zu berücksichtigen, beispielsweise im Internet, zumindest wenn sie legal zugänglich sind. Nach dieser Definition sind sehr viele Datenbestände in Organisationen personenbezogen und deshalb der Löschung zu unterwerfen. Dazu gehören Daten von Probanden in Projekten, Daten in der Personalverwaltung in Forschungsinstituten, Daten der Berechtigungsverwaltung oder in Log-Protokollen im IT-Betrieb, oder auch Daten der Ansprechpartner von Lieferanten. Zum Löschen gleichwertig ist Anonymisieren, weil die Daten danach nicht mehr unter das Regime des Datenschutzes fallen. Allerdings ist eine echte Anonymisierung gefordert – und diese gelingt oft nur mit erheblichem Aufwand. Es darf nämlich **keine Möglichkeit** mehr bestehen, auf die Person zurückzuschließen. Löschen ist meist die viel einfachere Alternative.

Das Datenschutzrecht fordert, dass personenbezogene Daten nur verarbeitet werden, solange die Organisation, die sie verarbeitet (Verantwortlicher), einen rechtmäßigen Zweck nachweisen kann. Die Zulässigkeitsgrundlagen legt Art. 6 DSGVO fest. Dazu gehören insbesondere gesetz-

liche Vorschriften für die Verarbeitung von Daten, Pflichten für die Abwicklung eines Vertrages oder Einwilligungen. Sind die Zwecke erledigt, müssen die Daten gelöscht werden (Art. 5: Datenminimierung und Speicherbegrenzung). Dies begründet die Pflicht zur Regellöschung.

Daneben besteht nach Art. 17 DSGVO die Möglichkeit, dass die betroffene Person eine frühere Löschung im Einzelfall beantragt. Dem Antrag muss stattgegeben werden, wenn bestimmte Bedingungen erfüllt sind. Außerdem kann die betroffene Person per Antrag auch verlangen, dass die Löschung im Einzelfall ausgesetzt wird. Auch dafür müssen bestimmte Bedingungen erfüllt sein.

Neben diesen Vorschriften, die für das technische Löschen relevant sind, definieren weitere Artikel der DSGVO verschiedene Dokumentations-, Informations- oder Meldepflichten.

Ausgangssituation in der Praxis

In der Praxis gibt es große Umsetzungsdefizite beim Löschen. Das hat zwei Ursachen: Die Löschregeln sind nicht definiert und es fehlen Löschmechanismen in Anwendungen. Insgesamt zeigt sich schnell, dass das Löschen personenbezogener Daten keine einmalige Aktion sein kann, sondern ein systematisches Vorgehen erfordert. Sinnvoll ist ein Löschkonzept, das die Aufgabe gut strukturiert und dauerhaft gepflegt werden kann. Wie aber kann ein solches Löschkonzept aufgebaut sein und erstellt werden? Eine bewährte Vorgehensweise wäre für die Projektplanung sehr hilfreich.

Seit April 2016 liegt mit der DIN 66398 eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ vor. Auch eine englische Sprachfassung steht zur Verfügung. Die Norm geht auf ein Industrieprojekt zum Löschen personenbezogener Daten zurück und stellt einen praxistauglichen, effizienten und systematischen Weg vor, wie Löschkonzepte in Organisationen etabliert werden können. Derzeit greifen Organisationen diese Vorgehensweise auf, um mit Blick auf die DSGVO ihre Löschkonzepte aufzusetzen.

Inhalte der Norm

Die Norm bietet umfangreiche Hilfestellungen, um ein Löschkonzept zu erstellen und in Organisationen zu etablieren, insbesondere:

- bietet sie bewährte Begriffe für Löschprojekte,
- beschreibt sie Vorgehensweisen, durch die Löschregeln festgelegt werden,
- gibt sie Vorschläge für die Umsetzung der Löschregeln,
- empfiehlt sie eine Struktur für die Dokumente des Löschkonzepts,
- gibt sie Empfehlungen, wie das Löschkonzept etabliert und fortgeschrieben werden kann.

Die Norm schlägt eine **Struktur für die Dokumente** des Löschkonzepts in drei Ebenen vor (Abb. 1). Im Dokument zur Vorgehensweise beschreibt die jeweilige Organisation unter anderem, welche Datenbestände sie mit ihrem Löschkonzept abdeckt und welche Vorgehensweise sie anwendet. Außerdem werden die Verantwortlichen für die einzelnen Dokumente und Prozesse festgelegt. Den Kern des Löschkonzepts bildet der Katalog der Löschregeln. Schließlich muss beschrieben werden, wie die Löschregeln in der Praxis anzuwenden sind. Dazu dienen die sogenannten Umsetzungsvorgaben, die diese Festlegungen jeweils für einen Bereich treffen. Die Norm empfiehlt, mit Ausnahme des Regelkatalogs, die Dokumentation zum Löschkonzept in vorhandene Dokumente zu integrieren, soweit dies sinnvoll erscheint.

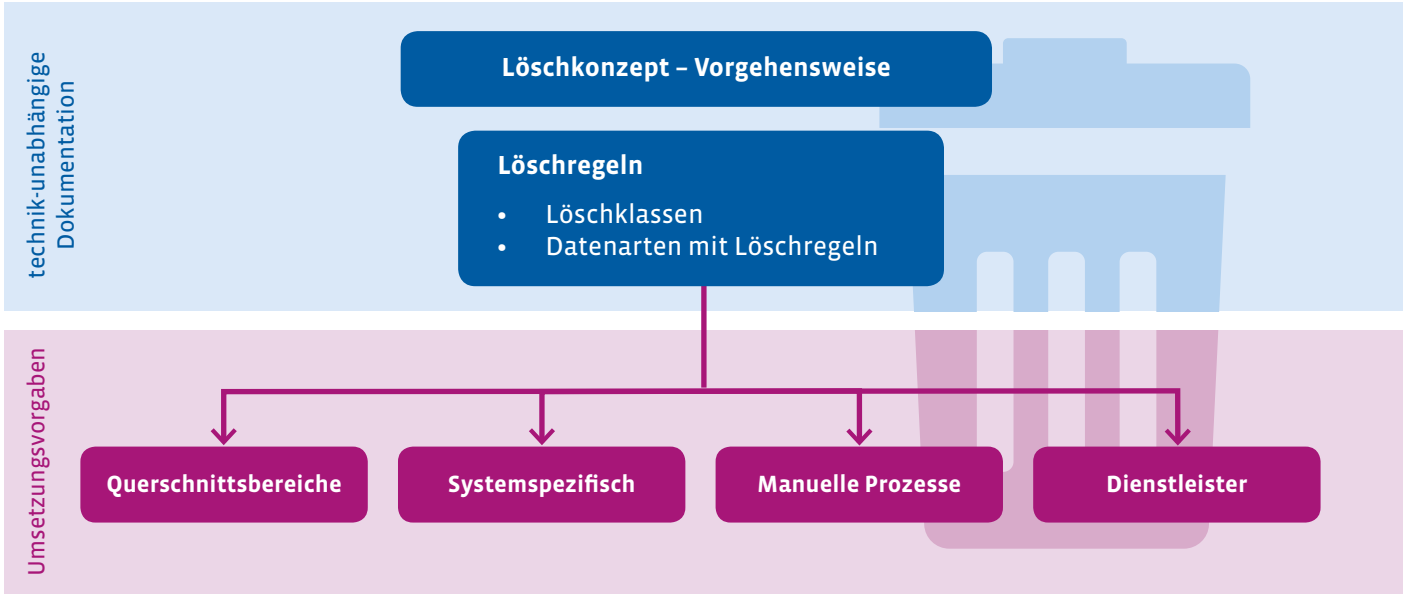

Abbildung 1: Dokumentationsstruktur eines Löschkonzepts in Anlehnung an DIN 66398

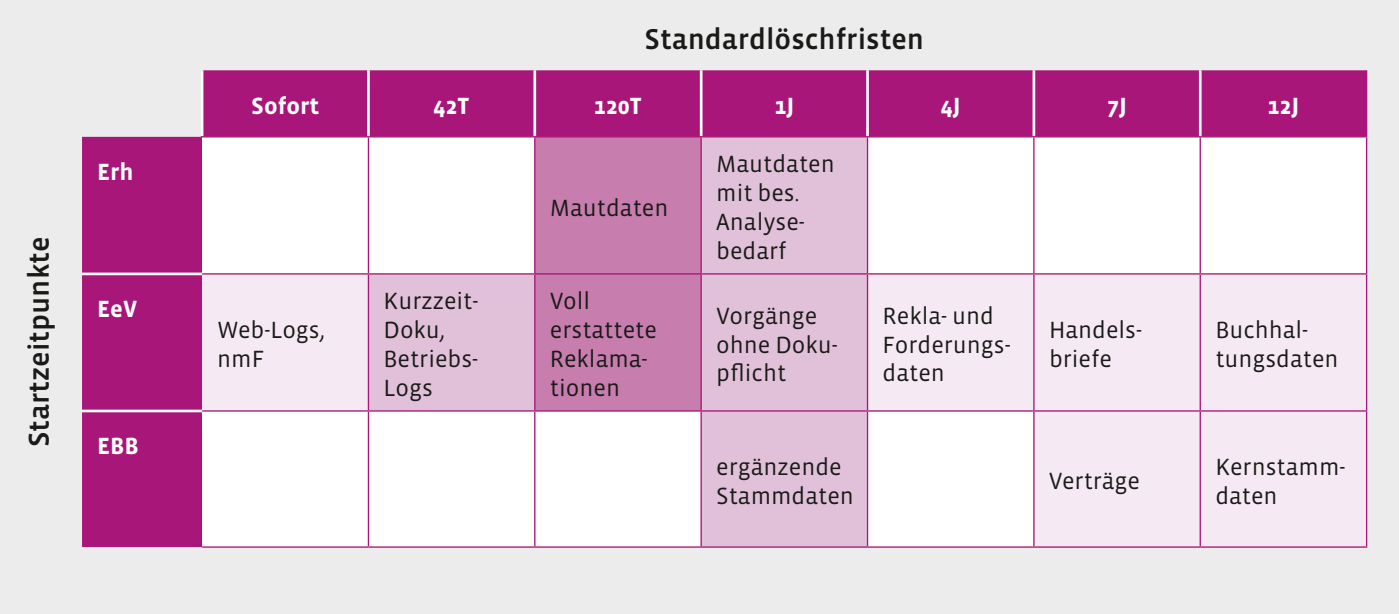

Abbildung 2: Matrix der Löschklasse der Toll Collect GmbH in Anlehnung an DIN 66398 (Legende im Text)

Die Löschregeln

Die größte Hürde für die Löschung personenbezogener Daten ist das Fehlen von Löschregeln. Ohne Löschregeln können keine Mechanismen implementiert werden. Der Kern der Norm ist deshalb eine Vorgehensweise, um Löschregeln zu definieren. Der Datenbestand der verantwortlichen Stelle wird dazu nach datenschutzrechtlichen Zwecken in sogenannte Datenarten unterteilt. Für jede Datenart wird genau eine Löschregel definiert. Sie besteht aus einem Startzeitpunkt und einer Regellöschfrist.

Um die Komplexität der Regelbildung und der Implementierung zu reduzieren, schlägt die DIN 66398 vor, Standardlöschfristen zu verwenden, um Löschfristen, die vergleichsweise nahe beieinanderliegen, in einer Frist zusammenzufassen. In Abbildung 2 werden sieben Fristen nach Tagen (T) und Jahren (J) unterschieden. Solche Standardfristen ergeben sich insbesondere aus Gesetzen, die übergreifend für alle Verantwortlichen gelten (in Abb. 2 hell), spezifische Rechtsvorschriften für den Anwendungsbereich (dunkel) und die frei gewählten Fristen (mittel). Es zeigt sich außerdem, dass sich die Startzeitpunkte nach drei wesentlichen Typen einteilen lassen: der Erhebung (Erh), einem Ereignis in einem Vorgang (EeV) oder dem Ende der Beziehung zum Betroffenen (EBB). Diese Typen von Startzeitpunkten abstrahieren von konkreten Ereignissen und werden in der Norm verwendet, um mit den Standardlöschfristen die sogenannten Löschklassen zu bilden (Abbildung 2). Diese Matrix ist ein ausgezeichnetes Hilfsmittel, um Löschregeln für Datenarten zu identifizieren und einen Überblick über die Datenarten und ihre Einordnung zu behalten. Die Datenarten müssen allerdings so eingeordnet werden, dass die Löschung der Datenobjekte datenschutzrechtlich nicht unangemessen lange verzögert wird.

Im Katalog werden Datenarten und Löschregeln technikunabhängig formuliert, also unabhängig von der Art ihrer Repräsentation oder von Speicherorten und Verarbeitungsprozessen. Für die Löschregel zur Datenart „Rechnung“ ist es deshalb unerheblich, ob sie in einer Datenbank, als PDF oder in einem Aktenordner vorliegt. Als Begründung für die Regeln sind im Katalog die datenschutzrechtlichen Zwecke aufzuführen.

Umsetzung

Die Übertragung und technische Umsetzung für konkrete Systeme und andere Bereiche wird für den Regelbetrieb über sogenannte **Umsetzungsvorgaben** gesteuert. Eine Umsetzungsvorgabe legt dann für die Datenarten des jeweiligen Bereichs fest, wie die Löschregeln angewandt werden. Dadurch wird beispielsweise in Systemlöschkonzepten für das System geregelt, welche Mechanismen mit welchen Konfigurationsparametern die Löschung ausführen, von wem sie gesteuert werden und welche Nachweise für Löschläufe erzeugt werden müssen.

Neben dem Löschen im Regelbetrieb muss ein Löschkonzept in der Praxis aber auch Sondersituationen abdecken. Die Norm gibt auch dafür Hinweise.

Um Backups und Wiederherstellung abzudecken, muss klar unterschieden werden zwischen Produktion und Archiven einerseits, in denen die Regellöschfristen zur Anwendung kommen, und Backups andererseits, die löschfällige Daten datenschutzrechtlich angemessen kurz über die Regellöschfrist hinaus vorhalten dürfen und dann überschrieben werden müssen.

Die Umsetzungsvorgaben müssen festlegen, wie die löschfälligen Daten nach einer Wiederherstellung behandelt werden. Andere Sonderfälle behandeln beispielsweise Beweismittel für einen Rechtsstreit, Störungen in einem IT-Prozess oder Fehler in Datenbeständen. Dazu können beispielsweise Kennzeichen zum Aussetzen der Löschung für einzelne Datenobjekte verwendet werden oder Löschmechanismen insgesamt befristet gestoppt werden.

Etablieren eines Löschkonzepts

Die Norm fasst Erfahrungen aus sieben Jahren Projektarbeit zusammen. Sie bietet ein praxistaugliches und systematisches Vorgehen für Löschkonzepte. Die DIN 66398 macht auch einen Vorschlag zur Organisation eines Löschprojekts, mit dem ein solches Konzept in der Organisation etabliert werden kann. Die klare Struktur der Dokumentation legt ein entsprechendes Vorgehen im Projekt nahe: Zunächst wird ein Katalog der Löschregeln erstellt. Danach werden die Umsetzungsvorgaben definiert und implementiert. Bereits zu Beginn eines Projekts „Löschkonzept“ besteht damit eine klare Strategie und es stehen einheitliche Begriffe zur Verfügung. Fehlschläge und lange Lernkurven können vermieden werden.

Im Rahmen des Projekts muss aber auch erreicht werden, dass Löschen nicht nur als eine einmalige Projektaufgabe, sondern als kontinuierlicher Prozess verstanden wird. Das Löschen von nicht mehr aufbewahrungspflichtigen oder obsoleten Daten soll als eine „übliche Anforderung“ an IT-Systeme verstanden werden. Die Aufgabe muss daher Bestandteil von Beschaffungs- und Entwicklungsprojekten sein und in Projektprozesse integriert werden.

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 Changemanagements oder bei Systembeschaffungen.

Vielfältiger Nutzen

Motiviert werden Löschkonzepte derzeit über die Datenschutz-Anforderungen der DSGVO. Es ist naheliegend, dass daher auch der Nutzen für den Datenschutz zunächst in den Fokus rückt. Bereits die Gewinne für den Datenschutz sind überraschend breit: Zunächst können die Vorgaben zum generellen Löschen und zum Löschen im Einzelfall erfüllt werden. Die Maßnahmen können auch gegenüber der Aufsichtsbehörde nachgewiesen werden. Für die Datenschützer der Organisation wird aber auch die Informationsbasis für andere Aufgaben wesentlich verbessert. Durch den Katalog der Löschregeln und die Umsetzungsvorgaben werden Datenbestände, Verantwortliche und Fachprozesse umfassend dokumentiert. Eine solche Dokumentation ist gleichzeitig die Voraussetzung, um die Rechtsansprüche der betroffenen Personen auf Auskunft, Sperrung oder Löschung überhaupt erfüllen zu können. Für die Dokumentation der Löschregeln sind die Zulässigkeitsgrundlagen zu erheben. Damit werden gleichzeitig die datenschutzrechtlichen Grundlagen aller Fachprozesse geprüft. Und schließlich kann durch das Löschprojekt und die Integration der Löschanforderungen in Projektprozesse die Einbettung des Datenschutzes in die Organisation deutlich verbessert werden.

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. ◆

WEITERFÜHRENDE MATERIALIEN

- DIN 66398:2016-05: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth-Verlag, 2016.
- Hammer, V. (2016): DIN 66398 - Die Leitlinie Löschkonzept als Norm, DuD 8/2016, 528 ff.; Download unter www.secorvo.de › Publikationen › Fachaufsätze › 2016.
- 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.

Eine Übersicht zu den Inhalten der DIN 66398 und weiterführende Informationen gibt auch die Webseite DIN-66398.de.