DIN 66398: Löschen – aber mit Konzept!

Paradigmenwechsel: In der klassischen Welt der automatischen Informationsverarbeitung ist das „Löschen von Daten“ eigentlich kein Thema. Im Gegenteil: Alle Bestrebungen sind darauf gerichtet, einen Datenverlust zu vermeiden. Es werden große Anstrengungen unternommen, um Backup- und Restore-Prozeduren zu implementieren und zu testen. Daten werden in immer größeren Umfängen („Big Data“) und für immer längere Zeiträume online vorgehalten, weil der Speicher immer billiger wird. Die Systeme eine immer performantere Recherche ermöglichen und die zukünftigen Auswertungswünsche von Controllern, Revisoren und externen Prüfern ja kaum vorhersehbar sind. Die Mindest-aufbewahrungsfristen nach gesetzlicher Grundlage (z.B. Abgabenordnung und Handelsrecht) werden um ein Vielfaches übererfüllt. Ein geregeltes Löschen ist in den Prozessen nicht oder nur kaum vorgesehen. Auch der Umgang mit Backup- und Archivdateien ist durch den Grundsatz „Je mehr, desto besser“ geprägt. Klassische Software-Systeme, z.B. SAP ERP, sehen das Löschen bestimmter Stammdaten (z.B. Organisationseinheiten wie Einkäufergruppen, Buchhaltergruppen) gar nicht vor. Andere Daten stehen oft in komplizierter Abhängigkeit zu Bewegungsdaten, so dass eine sehr genaue Analyse dieser Abhängigkeiten erfolgen muss, bevor Daten gelöscht werden können, ohne die Konsistenz des Systems zu zerstören.

Betrachtet man die Datenvorratsfrage jedoch aus Datenschutz-Sicht, besonders unter Berücksichtigung der Europäischen Datenschutzgrundverordnung, der sich ab Mai 2018 alle nationalen Datenschutzrechte und auch das kirchliche Datenschutzrecht anpassen müssen, sind die Prämissen neu zu setzen. Besonders das Prinzip der Datenminimierung und das Recht auf Löschung („Recht auf Vergessenwerden“) zwingt die Verantwortlichen, bei der Konzeption neuer und der Weiterentwicklung bestehender IT-Systeme, mit denen personenbezogene Daten verarbeitet werden, effektive Löschprozesse regelmäßiger Art (nach Ablauf der Regellöschfrist) sowie für Sonderfälle (berechtigte Löschbegehren vor Ablauf der Regellöschfrist) vorzusehen.

Die Zweckbindung der Verarbeitung personenbezogener Daten zwingt dazu, die Frage zu beantworten, wie die Verarbeitung unwiderruflich beendet wird („löschen“), wenn der Zweck entfällt und wie mit Daten umzugehen ist, die „unabsichtlich“ als „Beifang“ aufgrund technisch unvermeidbarer Zusammenhänge anfallen.

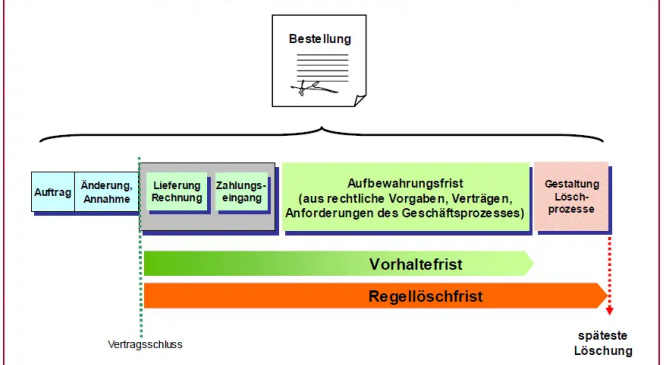
„Big Data“ auf deutschen Autobahnen
Im Projekt „Toll-Collect“ wurde die Erhebung und Verarbeitung von Daten realisiert, die zur Berechnung der benutzungsabhängigen Maut auf Autobahnen und Fernstraßen herangezogen werden. Neben Stammdaten (KFZ-Nummer, KFZ-Kategorie etc.) fallen in den Prozessen Unmengen von Bewegungsdaten von mautpflichtigen Fahrzeugen, aber – weil zunächst alle an einer Erfassungsstation vorbeifahrenden Fahrzeuge über ihr Nummernschild erfasst werden – auch von nicht mautpflichtigen Fahrzeugen an. Ein Unterprojekt erarbeitete deshalb unter Beteiligung des Bundesministeriums für Wirtschaft und Technologie und des Deutschen Instituts für Normung eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“. Diese „Leitlinie Löschkonzept“ wurde im Rahmen eines Normungsprojekts zur DIN 66398 weiterentwickelt und vom zuständigen Arbeitskreis im DIN im September 2015 verabschiedet.

DIN 66398 stellt demnach ein Verfahren zur Verfügung, mit dem in wiederholbarer Weise in jedem IT-Projekt – ob mit oder ohne Verarbeitung personenbezogener Daten – effektive Löschprozesse aufgesetzt werden können. So wird eine Best-Practice ausgerollt und der relativ neuen Forderung nach Erstellung und Umsetzung von Löschkonzepten mit einer durchaus konkreten Handlungsempfehlung begegnet.

Wichtige Begriffe
Die Leitlinie „Löschen“ bzw. die DIN 66398 führt die folgenden Begriffe ein:

- Datenart:
  vereint alle Datenobjekte (Entitäten), die zu einem gemeinsamen Zweck verarbeitet werden. Das können z.B. Personen, deren Eigenschaften (Attribute), Objekte oder Beziehungen (Relationen) sein. Backup- und Archivdaten bilden i.d.R. eigene Datenarten.
- (Regel-)Löschfrist:
  Zeitraum, nach dem die Daten i.d.R. gelöscht werden sollen. Die Löschfrist ergibt sich u.a. aus den gesetzlichen oder vertraglichen Aufbewahrungsfristen sowie bestimmten Prozesszeiten:

Abbildung 1: Beispiel für Fristabschnitte für einen Auftrag im Löschkonzept



Im Beispiel beginnt der Lauf der Vorhalte- und der Regellöschfrist mit dem Vertragsschluss. Der Vertragsschluss ist ein Beispiel für einen Startzeitpunkt vom Typ „Ende eines Vorgangs". Die aktive Verwendung des Vertrages endet mit dem Zahlungseingang. Danach wird der Vertrag noch für eventuelle Garantiefälle und als Handelsbrief nach AO und HGB aufbewahrt.

- Startzeitpunkt:
  Ereignis, ab dem die Löschfrist läuft. Beispielsweise Erhebung der Daten, Ende des Vorgangs oder Ende der Beziehung zum Betroffenen
- Löschklassen:
  werden durch die Einstufung der Datenarten nach Löschfrist und Startzeitpunkt gebildet.

Abbildung 4: Beispiel für eine Matrix mit Löschklassen (Toll Collect)

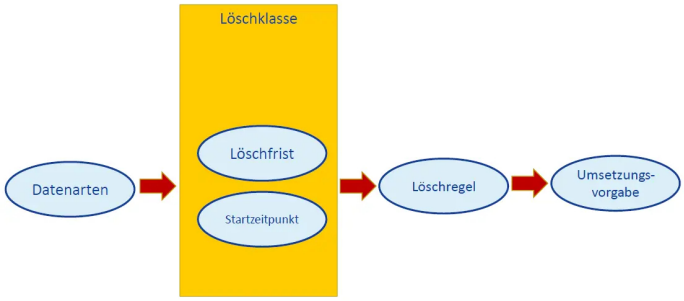
Startzeitpunkte	Standardfristen: Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Ab Erhebung			Mautdaten	Mautdaten mit bes. Analyse-bedarf			
Ab Ende Vorgang	nmF, Web-Logs	Kurzzeit-Doku., Betriebs-Logs	EFN, voll erstattete Reklama-tionen	Vorgänge ohne Doku-pflicht	Rekla- und Forde-rungs-daten	Handels-briefe	Buch-haltungs-daten
Ab Ende Beziehung				ergän-zende Stamm-daten		Verträge	Kern-stamm-daten.

LEGENDE:
gelb unterlegt: Frist abgeleitet aus allgemeinen Gesetzen
blau unterlegt: Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
grün unterlegt: Frist frei gewählt
ABKÜRZUNGEN: nmF = Mautdaten nicht-mautpflichtiger Fahrzeuge; EFN = Einzelfahrtennachweis

- Löschregel:
  Wird für jede Datenart über die Löschklasse definiert.
- Umsetzungsvorgabe:
  Konkretisiert die Löschregel in Bezug auf die verwendete Technik und wird getrennt von der Löschregel dokumentiert.
- Verantwortlichkeiten:
  Werden festgelegt für die Durchführung der Umsetzungsvorgaben, aber auch für die Weiterentwicklung des Löschkonzeptes und die Pflege der Dokumentation.

Der Weg zum Löschkonzept

Das Löschkonzept wird laut DIN 66398 in der Weise erstellt, dass zuerst die Datenarten bestimmt und diese dann in Löschklassen zusammengefasst werden. Anschließend werden für die Datenarten die Löschregeln formuliert und für jede verwendete Technologie eine Umsetzungsregel aufgestellt. Die einzelnen Schritte werden modular dokumentiert und mit Verantwortlichkeiten versehen.



Auf Sondersituationen geht die DIN 66398 nicht explizit ein. Es ist jedoch offensichtlich, dass ein effektives Löschkonzept nicht nur die regelmäßigen regulären Löschvorgänge nach Ablauf der Regellöschfrist beschreibt, sondern auch für Situationen wie das notwendige Löschen von unberechtigt erhobenen Daten und das Löschen von personenbezogenen Daten nach einem berechtigten Löschbegehren des Betroffenen (§ 35 BDSG) praktikable Anweisungen enthalten muss.

Auch die Frage, wie mit (personenbezogenen) Daten beim Rückbau von IT-Systemen umzugehen ist, wenn es für jene keine „Anschlussverwendung“ gibt, muss von einem umfassenden Löschkonzept beantwortet werden.