DSB5seenland

Löschkonzept nach DSGVO und DIN 66398

guido.feuerriegel@vt-coaching.eu; www.vt-coaching.eu

Löschkonzept

DSB5seenland

Warum eigentlich ein Löschkonzept?

Im normalen Geschäftsbetrieb entstehen zahlreiche personenbezogene Daten

- Kundendaten
- Mitarbeiterdaten
- Bewerberdaten
- Finanz- und Rechnungsdaten
- Werbung und Marketing

Viele davon haben unterschiedliche Aufbewahrungsfristen und sind auf unterschiedliche Art und Weise gespeichert

Löschkonzept

DSB5seenland

Wann müssen personenbezogene Daten gelöscht werden:

- Wenn sie für den Zweck der Erhebung nicht mehr benötigt werden
- Wenn die betroffene Person es verlangt (Recht auf Vergessenwerden)
- Wenn die Aufbewahrungsfristen auf Basis einer Rechtsvorschrift abgelaufen sind

…und alle Löschungen müssen dokumentiert werden (Art.5, 2 DSGVO Rechenschaftspflicht)

Wie soll das ohne schriftliches Löschkonzept auseinander gehalten werden?

Löschkonzept

DSB5seenland

Zuständige Norm: DIN 66398

Der Leitfaden zur DIN 66398 strukturiert das Löschkonzept in 6 einzelne Schritte

Was ist Löschen (Leitlinie zur DIN 66398)

DSB5seenland

Löschen

- behandeln von personenbezogenen Daten derart, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können.

- ANMERKUNG 1: In der Regel ist "sicheres Löschen" gefordert. Sicheres Löschen meint, dass der Aufwand für die Rekonstruktion der Daten unverhältnismäßig hoch ist oder aus physikalischen Gründen unmöglich ist.

- ANMERKUNG 2**:** Wenn die einschlägigen Rechtsvorschriften dies zulassen, können personenbezogene Daten auch anonymisiert werden, statt sie zu löschen.

Was ist Löschen (Leitlinie zur DIN 66398)

DSB5seenland

Anonymisieren
Prozess, durch den pbD so verändert werden, dass der Betroffene nicht mehr direkt oder indirekt identifiziert werden kann.
ANMERKUNG 1: Um pbD zu anonymisieren, werden beispielsweise einzelne Attribute eines Datenobjekts gelöscht oder überschrieben, die die Zuordnung zum Betroffenen ermöglichen. Die verbleibenden Daten (für die der Personenbezug aufgehoben wurde), fallen nicht mehr unter die Regeln des Datenschutzes und müssen demnach nicht mehr nach deren Vorgaben gelöscht werden. Identifizierende Attribute können z. B. sein Name und Geburtsdatum, Identifikationsnummern, biometrische Merkmale, zugeordnete Kontonummern, Telefonnummern, Steuernummern und dergleichen, Datenbankschlüssel, die auf Personen verweisen, oder auch eine Kombination mehrerer oder vieler einzelner Merkmale, die auf eine einzelne Person (oder eine kleine Gruppe) rückschließen lässt.
ANMERKUNG 2: Je nach den Vorgaben der einschlägigen Rechtvorschriften muss der Aufwand zur Wiederherstellung eines Personenbezugs unverhältnismäßig hoch sein oder er darf gar nicht möglich sein. [ISO 29100] fordert, dass die Anonymisierung irreversibel ist.

Was ist Löschen (Leitlinie zur DIN 66398)

DSB5seenland

Anonymisieren (2)

ANMERKUNG 3:

Je nachdem, welcher Datenbestand nach der Aufhebung des Personenbezugs noch vorhanden ist und welche Daten für die Wiederherstellung benutzt werden können, können sehr vielfältige Strategien zur Wiederherstellung des Personenbezugs greifen. So können z. B. Zeitpunkte bestimmter Ereignisse, Bewegungsprofile oder Rechnungsbeträge verwendet werden, um Korrelationen zwischen Datenbeständen zu bestimmen und damit den Personenbezug wieder herzustellen.

Solche Möglichkeiten müssen bereits in den Umsetzungsvorgaben für die Aufhebung des Personenbezugs berücksichtigt werden.

Datenbestände zu anonymisieren ist deshalb häufig wesentlich schwieriger, als sie fristgerecht zu löschen.

Je nach Umsetzung kann die Anonymisierung möglicherweise auch mit neuen Erkenntnissen oder neu verfügbaren Datenbeständen wieder rückgängig gemacht werden

Anonymisierung - Verfahren

DSB5seenland

Von der Art. 29 -Gruppe werden die möglichen Methoden der Anonymisierung in die Randomisierung und die Generalisierung sowie deren Kombination eingeteilt.

Randomisierung:
Zufälliges Herausgreifen und Isolation der Datensätze aus dem Datenbestand, wobei dies je nach Datenbestand zu einer dauerhaften De-Identifikation führen kann, was im konkreten Fall zu prüfen und sicherzustellen ist.

Generalisierung:
Aggregation von Einzelangaben, Werten, d.h. eine künstliche Unschärfe.

Verhinderung der Verknüpfung:
Verhinderung der Verknüpfung der Datensätze in verschiedenen Datenbanken, so dass diese nicht mehr in Beziehung gesetzt werden können.

Löschkonzept

DSB5seenland

Schritt 1 – Datenbestand analysieren

- Welche Daten werden wo verarbeitet
- Basis kann das Verzeichnis der Verarbeitungstätigkeiten sein, das vorgeschrieben und nützlich ist
- Daraus die Datenarten extrahieren
- Datenflüsse in den Abteilungen analysieren und Synergien feststellen

Löschkonzept

DSB5seenland

Schritt 1 – Datenbestand analysieren (Beispiel)

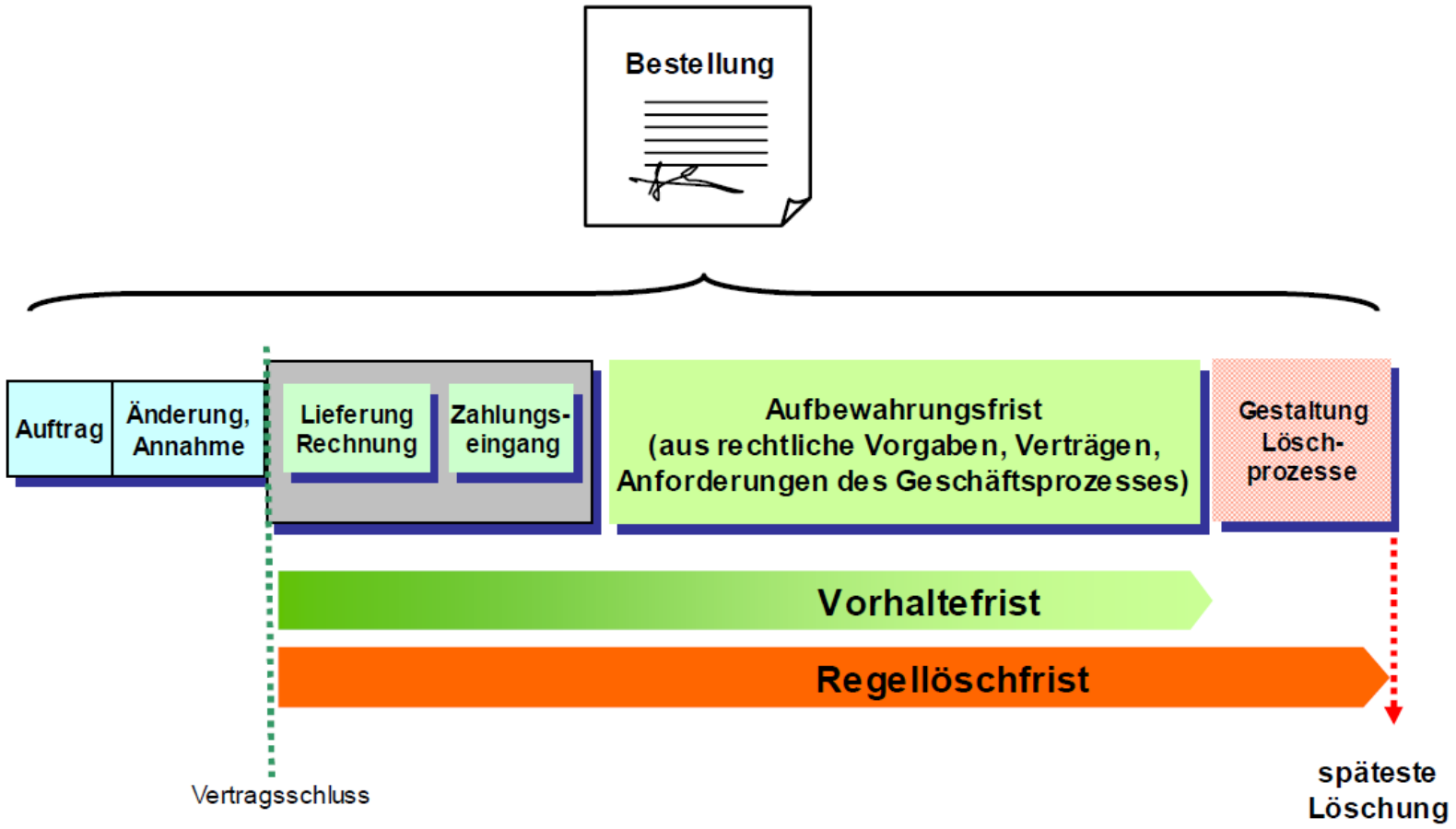
Verarbeitungstätigkeit	Datenart
Personalverwaltung	Personalstammdaten von Beschäftigten Abmahnungen Erweiterte Stammdaten
Lohn-/Gehaltsabrechnung	Buchungsbelege Auszahlungsbelege Adressdaten
Finanzbuchhaltung	Rechnungen Kundendaten Buchungsbelege
CRM	Kundendaten Angebots- Vertragsdaten Korrespondenz

Löschkonzept

DSB5seenland

Schritt 2 – Löschregeln

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.

DSB5seenland

Schritt 2 – Löschregeln festlegen

Benötigt werden Fristbeginn und Regellöschfrist

Beispiel: Für Handels- und Geschäftsbriefe, wie E-Mails oder Briefe, beginnt die Frist mit dem Schluss des Jahres, in dem diese empfangen oder abgesandt wurden (§ 147 Abs. 4 AO). Die Löschfrist für Korrespondenz des Jahres 2020 beginnt also am 31.12.2020.

Sie sind 6 Jahre aufzubewahren (§ 147 Abs. 1 Nr. 2, Abs. 3 AO). Die Vorhaltefrist beträgt also 6 Jahre. Die Gestaltung des Löschprozesses sollte nicht länger als ein Jahr dauern. Dadurch ergibt sich eine Regellöschfrist von 7 Jahren.

DSB5seenland

Schritt 3 - Ausnahmen prüfen

- Welche Datenarten werden über die Zweckerfüllung hinaus benötigt (z.B. Verteidigung/Abwehr von Rechtsansprüchen, Rechnungen, Buchungsbelege
- Welche Datenarten können vorzeitig anonymisiert und archiviert werden
- Entscheidung durch den Eigentümer der Daten und IT

DSB5seenland

Schritt 4 – Datenbestand kategorisieren und Löschklassen bilden

- Welche Datenarten haben ähnliche Aufbewahrungsfristen
- Ähnliche Fristen zu Löschklassen zusammenfassen
- Standard-Löschfristen für die Löschklassen definieren

DSB5seenland

Schritt 5 – Löschvorgang planen

- Den Datenarten mit ihrer Löschklasse die entsprechende Verarbeitung bzw. Speicherort zuordnen
- Jeweilige Löschmechanismen für die Verfahren bestimmen
- Sicherheitsanforderungen, bzw. Schutzstufen berücksichtigen

DSB5seenland

Schritt 6 – Verantwortung delegieren

- Entwicklung und Fortschreibung des Löschkonzeptes
- Einhaltung und tatsächliche Durchführung des Löschens
- Kontrolle des ordnungsgemäßen Löschens
- Beantwortung von Löschbegehren.

DSB5seenland

Projektablauf Löschkonzept

DSB5seenland

Hilfsmittel Löschfristen

Löschkonzept EcoDMS

DSB5seenland

Löschkonzept EcoDMS

Mit dem Dokumenten-Management-System ecoDMS wird eine revisionskonforme Archivierung aller Dokumente für jedermann möglich. Die sichere Archivierung ist das A und O einer solchen Softwarelösung. Trotzdem ist unter bestimmten Umständen das Löschen bestimmter Daten unausweichlich. In die aktuellen ecoDMS Version 18.09 (apu) haben die Aachener ein modernes Löschkonzept integriert, welches es erlaubt Dokumente und personenbezogene Daten gemäß GoBD und DSGVO gesetzeskonform aus dem Archiv zu entfernen. Dabei unterscheidet die Software zwischen dem einfachen Verschieben von Dokumenten in einen virtuellen Papierkorb, der unwiderruflichen Entfernung von Dokumenten aus dem Archiv und dokumentenunabhängig dem Löschen personenbezogener Daten, also angelegten Benutzern. Das Video ist auf der ecoDMS Webseite und im ecoDMS YouTube-Channel verfügbar.

Über die Funktion „In den Papierkorb verschieben" können nicht mehr benötigte Dokumente aus der Hauptansicht entfernt und in einen virtuellen Papierkorb verschoben werden. Diese Funktion steht allen Benutzern zur Verfügung, die die betroffenen Dokumente im Archiv klassifizieren dürfen. Neben der einfachen Papierkorb-Funktion verfügt ecoDMS über eine Löschfunktion, die es autorisierten Benutzern erlaubt Dokumente mittels integriertem Löschkonzept endgültig aus dem Archiv zu entfernen. Die Dokumente durchlaufen hierbei mehrere Stufen. Nach dem Verschieben einer Datei in den Papierkorb werden diese dem zuständigen Benutzer zur Prüfung vorgelegt. Ob ein Dokument aber tatsächlich entfernt werden darf, hängt von den genauen Dokumenteneinstellungen ab. Denn jeder Dokumentenart kann optional auch eine eigene Aufbewahrungsfrist zugewiesen werden. Diese legt fest, ab wann ein Dokument tatsächlich entfernt werden darf. So können z.B. für Rechnungen die gesetzlichen Aufbewahrungsfristen berücksichtigt werden. Außerdem kann eine zusätzliche Sichtungsprüfung vor dem Löschvorgang gefordert werden.

Umsetzungsbeispiel

DSB5seenland

Die Umsetzung dieser Sicherheitsmaßnahmen erfolgt über den Einstellungsdialog vom zuständigen Administrator im Bereich „Dokumentenarten“. Bei der Überprüfung des Dokuments kann der zuständige Benutzer optional die hinterlegte Frist verlängern oder die sofortigen Freigabe zum Löschen der Datei erteilen. Der anschließende Löschvorgang erfordert das Erstellen eines Löschprotokolls. An dieser Stelle müssen ein PIN-Code und eine Begründung für den Löschvorgang erfasst werden. Dieses Protokoll ersetzt anschließend die ursprüngliche Originaldatei. Innerhalb der Klassifizierung und Historie werden zudem jegliche Textinformationen anonymisiert. Das Bemerkungsfeld im Klassifizierungsdialog ist beispielsweise ein solches Textfeld. Zugriff auf das Löschprotokoll haben anschließend nur noch Super Administratoren mit bestimmten Zugriffsrechten auf das Archiv. Neben dem Löschen von Dokumenten erlaubt ecoDMS auch die Entfernung angelegter Benutzer. In diesem Fall werden Berechtigungen innerhalb von Klassifizierungen und Ordnerstrukturen auf einen anderen, bestehenden Benutzer übertragen. Dies ist nur ein kleiner Auszug der vielen Möglichkeiten mit dem ecoDMS Archiv. Diese und weitere Informationen finden Sie im Internet unter www.ecodms.de.