Löschkonzept (DSGVO)

Was Unternehmen beim Löschen beachten müssen

Die in diesem Konzept enthaltenen Informationen dienen der allgemeinen Orientierung und stellen eine Vorlage dar.

Rechtshinweis:

Die Inhalte wurden mit großer Sorgfalt recherchiert. Dennoch kann Sage keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen übernehmen. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen, insbesondere im Rahmen der DSGVO, konsultieren Sie bitte unbedingt einen Rechtsanwalt.

Stand: August 2018

Inhaltsverzeichnis

1.0 Löschkonzept zur Datenminimierung

Im Datenschutzrecht besteht eine gesetzliche Verpflichtung für Unternehmen personenbezogene Daten zu löschen, wenn diese für die Zwecke für die sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind und zudem auch keine gesetzliche Aufbewahrungspflicht der Löschung entgegensteht.

Durch die neue Datenschutzgrundverordnung (DSGVO) wurden diese Löschpflichten nochmals erheblich erweitert. Bei Nichtbeachtung drohen jetzt hohe Bußgelder.

Daher ist die Implementierung eines DSGVO konformen Löschkonzepts eng mit der Umsetzung handels- und steuerrechtlicher sowie weiterer Aufbewahrungspflichten verbunden (GoBD), die ebenfalls eine genaue Kenntnis der Datenflüsse im Unternehmen und ggfs. eine Bestandsaufnahme erfordern. So lässt sich z.B. ein Widerspruch gegen den Erhalt von E-Mail-Werbung nur durch Löschung bestimmter Daten umsetzen.

1.1 Artikel 5 der DSGVO

In diesem Artikel geht es um die einzuhaltenden Prinzipien bei der Verarbeitung personenbezogener Daten.

- Daten sollen rechtmäßig, die Verarbeitung nach Treu und Glauben, sowie transparent verarbeitet werden
- Die Verarbeitung sollte nur für festgelegte, eindeutig sowie legitime Zwecke erhoben werden und unterliegt einer Zweckbindung, was auch die Weiterverarbeitung betrifft
- Nach dem Prinzip der Datenminimierung ist die Datenverarbeitung auf das notwendige Maß zu beschränken
- Der Grundsatz der Richtigkeit erfordert, dass personenbezogene Daten sachlich richtig und aktuell sein müssen
- In zeitlicher Hinsicht gibt es eine Speicherbegrenzung für den Zeitraum, für den die entsprechenden personenbezogenen Daten im Hinblick auf den Zweck der Datenverarbeitung benötigt werden
- Es gelten die Grundsätze der Integrität und Vertraulichkeit im Hinblick auf die Datenverarbeitung, was geeignete technische und organisatorische Maßnahmen (TOMs) umfasst, die die verarbeiteten Daten vor Verlust, unrechtmäßiger Verarbeitung, vor Zerstörung oder Schädigung schützen sollen

1.2 Artikel 17 der DSGVO

In diesem Artikel wird das Recht auf Löschung der eigenen Daten festgeschrieben. Voraussetzung ist, das eine der folgenden Bedingungen vorliegt:

- Die Speicherung aus fachlichen Gründen ist nicht mehr notwendig
- Der Betroffene zieht seine Einwilligung zurück, dass die Daten verarbeitet werden dürfen
- Das Unternehmen oder die öffentliche Einrichtung hat die Verarbeitung unrechtmäßig vorgenommen
- Es besteht eine Rechtspflicht zum Löschen

Zudem gibt es Sondersituationen in denen gelöscht werden muss. Diese können aufgrund ihrer Unvorhersehbarkeit nicht von Löschregeln im Sinne eines Löschkonzepts umfasst werden. Dazu gehört:

- Das Löschen von unberechtigt erhobenen personenbezogenen Daten
- Das Löschen von personenbezogenen Daten beim Rückbau von Systemen

Für diese und ähnliche Sonderfälle müssen ebenfalls Löschmaßnahmen bestimmt werden, damit das Unternehmen im Eintrittsfall nicht ohne Handlungsoption dar steht.

1.3 Löschkonzept DSGVO konform umsetzen nach DIN 66398

Hilfreich bei der Erstellung eines Löschkonzepts ist die Leitlinie DIN 66398. Sie definiert ein Modell zur Entwicklung und Etablierung eines Löschkonzepts. Die Norm beschreibt Vorgehensweisen, durch die Löschregeln festgelegt werden und gibt eine Struktur zur Dokumentation des Löschkonzepts vor.

Diese Leitlinie basiert auf den Erfahrungen der Toll Collect GmbH, die im Rahmen eines Normungsprojekts mit Unterstützung von fünf Unternehmen zur DIN 66398 weiterentwickelt wurde.

Hinweis: Beziehen Sie in jedem Fall den internen bzw. externen Datenschutzbeauftragten (DSB) bei der Erstellung des Löschkonzeptes mit ein.

Teilen Sie den Datenbestand in verschiedene Datenarten auf. Für jede dieser Datenarten ist eine Löschregel zu definieren. Diese Löschregel besteht aus zwei Angaben:

- Regellöschfrist
- Startzeitpunkt, ab dem die Regellöschfrist läuft

Vorgaben Löschkonzept

Anforderung	Beschreibung	Beispiel
Festlegung von Löschregeln	Wie lange werden welche Daten gespeichert bzw. wie wird die Frist festgelegt?	Kunden-/Lieferantendaten werden nach Beendigung des Geschäftsverhältnisses noch 10 Jahre aufbewahrt
Vorgaben für die Umsetzung der Löschregeln	Wie wird konkret gelöscht?	Einmal jährlich wird geprüft, welche Kunden/Lieferanten schon länger als 10 Jahre die Geschäftsbeziehung beendet haben
Vorgaben für die Dokumentation	Wie wird die Löschung dokumentiert?	Der Verantwortliche dokumentiert die Durchführung des Löschkonzepts und legt es z.B. in einem DMS (digitales Archiv) ab
Festlegung von Verantwortlichkeiten	Wer ist dafür verantwortlich, dass gelöscht wird? Wer führt die Löschung durch?	Das Unternehmen (GF) ist verantwortlich. In Absprache mit dem Datenschutzbeauftragten, den Fachabteilungen und der Administration wird eine Prüfung vorgenommen und es erfolgt die Löschung.

2.0 Löschkonzept erstellen

2.1 Personenbezogene Daten im Unternehmen lokalisieren

Für jede Abteilung des Unternehmens sollte erfasst werden, welche personenbezogenen Daten dort verarbeitet werden. Welche Daten werden auf welchen Systemen gespeichert? Gibt es ein zentrales System für Stammdaten?

Dabei sollten erfasst werden:

- die Datenkategorien, d.h. die Art der Daten
- handelt es sich um besondere Kategorien personenbezogener Daten
- die Dauer, für die diese Daten unmittelbar für den jeweiligen Geschäftsvorgang benötigt werden. Beim Massengeschäft, z.B. der Verarbeitung von Zahlungstransaktionen, könnte eine durchschnittliche Verweildauer ermittelt werden
- ob die betreffenden Daten aufbewahrungspflichtig sind. Dazu sind die Rechtsvorschriften zu ermitteln, die für diese Daten gelten
- wie lange die Aufbewahrungspflicht gilt, d.h. wann die entsprechende Frist beginnt und wann sie endet
- auf welchem System oder Datenträger diese Daten gespeichert werden
- welche Datenzu- und Abflüsse in bzw. von anderen Systemen es gibt, d.h. für welche Systeme das betrachtete System die Datenquelle ist und welche Systeme für das betrachtete System maßgeblich sind (z.B. zentrale Stammdatenbank)

Eine solche Bestandsaufnahme umfasst alle Applikationen, mit denen im Unternehmen personenbezogene Daten bearbeitet werden.

2.2 Daten in Kategorien einordnen

Die erhobenen Datenarten sollten verschiedenen Kategorien zugeordnet werden, für die jeweils die gleiche Aufbewahrungsdauer gilt. Dabei sollte danach unterschieden werden, ob es sich um besondere personenbezogene Daten handelt, da hier weitere Einschränkungen gelten können.

Eigene Kategorien sollten für Daten gebildet werden, die vom Unternehmen im Wege der Auftragsverarbeitung (AV) von einem Dienstleister verarbeitet werden, oder die das Unternehmen selbst im Auftrag eines Dritten verarbeitet. Auch Konzerngesellschaften können Auftragsverarbeiter oder Auftraggeber einer Auftragsverarbeitung sein.

2.3 Löschregeln je Kategorie definieren

Die DSGVO sieht vor, dass personenbezogene Daten nur solange gespeichert werden dürfen, wie dies unbedingt notwendig ist. Daher sollte für jede Kategorie anhand von Erhebungsdatum, voraussichtlicher (durchschnittlicher) Bearbeitungszeit und dem Beginn

der jeweiligen Aufbewahrungsfrist eine Löschregel bestimmt werden. Es ist sinnvoll, die Anzahl der Löschregeln möglichst gering zu halten.

2.4 Archvieren

Ist die Bearbeitung von Daten für einen bestimmten Geschäftsvorfall abgeschlossen, steht vor der Löschung der Daten in den allermeisten Fällen die Archivierung. Dabei werden die Daten i.d.R. in einem digitalen System (oder in Papierakten) archiviert, welche den gesetzlichen Vorschriften zur Aufbewahrung, insbesondere handels- und steuerrechtlichen Vorschriften oder Vorgaben (GoBD), genügen.

2.5 Sonderfälle

In bestimmten Fällen kann es vorkommen, dass Datensätze außerhalb der definierten Regeln gelöscht/anonymisiert werden müssen:

- Ein Betroffener macht Gebrauch von seinem „Recht auf Vergessenwerden“
- Ein Datensatz wurde rechtswidrig erhoben
- Eine Aufsichtsbehörde verlangt dies vom Unternehmen
- Das Unternehmen kann verpflichtet werden, alle Löschungen und Änderungen der Daten zu stoppen,
    - wenn z.B. die steuerrechtlichen Dokumente noch in einem ausstehenden Gerichtsverfahren benötigt werden
    - Auftragsverarbeiter
      Sind Sie selbst als Auftragsverarbeiter für ein anderes Unternehmen tätig, legen Sie Vorgaben für die Löschung von Datensätzen fest und dokumentieren Sie dies in einem Löschprotokoll.

Idealerweise legen Sie in einer eigenen Beschreibung der Verarbeitungstätigkeit fest, wie ein Löschvorgang in einem der vorgenannten Sonderfälle abläuft, so dass Sie dem Betroffenen, oder einer Aufsichtsbehörde belegen können, dass die Daten gelöscht bzw. vor Veränderungen geschützt wurden. Dazu gehört die Definition der Vorgehensweise und das Festlegen eventueller manueller Eingriffe (z.B. Auswahl der Daten, Vier-Augen-Prinzip, Dokumentation/Protokoll)

2.5.1 Verwendung von Datensicherungen

Bitte beachten Sie, dass sich auf Datensicherungen ebenfalls personenbezogene Daten befinden können. Bei der Erstellung des Löschkonzeptes, müssen Sie daher Datensicherungen und deren Löschung mit einbeziehen.

2.5.2 Löschung von Mitarbeiterdaten

Verlässt ein Mitarbeiter das Unternehmen, darf die Personalakte keinesfalls „einfach so“ entsorgt werden. Zunächst gelten die gesetzlichen Aufbewahrungsfristen. In dieser Zeit ist das Unternehmen verpflichtet, alle entsprechenden Unterlagen zu archivieren und jederzeit vorzuhalten. Nach Ablauf der Aufbewahrungsfrist muss auf eine "sichere" Vernichtung der Daten geachtet werden. Neben dem datenschutzkonformen Schreddern

der Papierakten gibt es spezielle Verfahren zur spurenlosen Löschung elektronischer Unterlagen.

Setzen Sie die personenbezogenen Daten in Ihrer Personalwirtschaft z.B. auf inaktiv und beachten Sie, dass eine Löschung des Benutzerprofils unter Microsoft Windows berücksichtigt werden muss.

Verjährungsfrist für Versorgungsansprüche:
Bei Ansprüchen der Altersvorsorge in Bezug auf eine Pensionskasse, beträgt die Verjährungsfrist 30 Jahre. Solange sollten die dazu bestehenden Unterlagen aufbewahrt werden. Die Verjährungsfrist beginnt im genannten Fall erst am Jahresende des Jahres, in dem der betroffene Angestellte aus dem Unternehmen ausscheidet.

Verjährungsfrist für Steuerrelevante Dokumente
Eine Aufbewahrungsfrist von sechs Jahren ist bindend, wenn in der Personalakte Dokumente zum Steuerrecht zu finden sind. Dies ist die gesetzliche Aufzeichnungs- und Aufbewahrungspflicht im Rahmen des Steuerrechts. Damit wird gewährleistet, dass Steuerbehörden sowie Sozialversicherungsträger bei Betriebsprüfungen oder Lohnsteuer-Außenprüfungen auf die Dokumente zugreifen können.

Die Verjährungsfristen ehemaliger Arbeitnehmer können darüber hinauswirken, wenn arbeitsrechtliche Ansprüche, wie z.B. Schadenersatzansprüche oder die Aushändigung eines Arbeitszeugnisses verlangt werden.

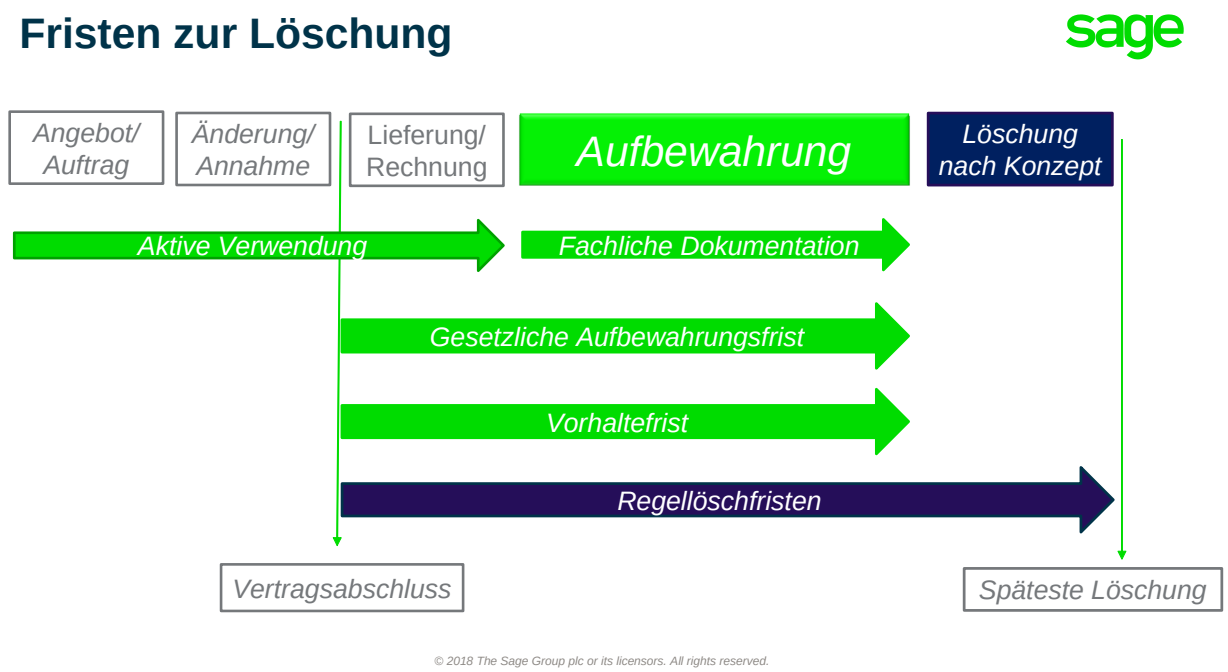
2.6 Eigentliche Löschung

Sind für archivierte Datensätzen die Aufbewahrungsfristen abgelaufen, müssen diese gelöscht werden. Dazu sollten sichere Verfahren vorgesehen werden, die – ggfs. nach manueller Bestätigung – die Löschung durchführen und den Löschvorgang automatisiert mitprotokollieren (Löschprotokoll). Treten dabei Fehler auf, z.B. wird ein Datensatz nicht gefunden oder ist gesperrt, sollte das Löschverfahren eine Meldung erzeugen. Das Löschprotokoll sollte von einem entsprechend unterrichteten Mitarbeiter geprüft werden.

Beachten Sie hierbei die Wege, die diese Daten in Ihrem Unternehmen durchlaufen:

- Gibt es z.B. Stammdaten in verschiedenen Systemen, muss dies ebenso berücksichtigt werden, wie ein Datenaustausch zwischen verschiedenen Systemen, von denen eines das Maßgebliche ist. Eine zentrale Datenbank für Stammdaten kann dabei vieles vereinfachen
- Vernichten sie papiergebundene Dokumente z.B. mittels Aktenreißwolf
- Löschen Sie Daten von Festplatten, Druckern oder Telefax-/Multifunktionsgeräten
- Ein Überschreiben von Daten ist nicht in allen Konstellationen machbar, z.B. wenn die Daten in einem Shared System oder in einer Datenbank gespeichert sind, die weitere noch aufzubewahrende Datensätze enthält. Die Verschlüsselung einer Gruppe von Datensätzen mit gemeinsamem Löschdatum kann hierfür eine Lösung sein, oder die Anonymisierung der Datensätze.

- Bei Cloud-Anwendungen können z.B. Cloud Access Security Broker bzw. ein Cloud Data Protection Gateway eingesetzt werden, bei denen von vornherein verschlüsselte Daten an die Cloud übergeben werden. Hier genügt es den Schlüssel zu löschen, um die Daten dauerhaft unzugänglich zu machen.
- Nutzen Sie ein Löschprotokoll, das für eine gewisse Dauer aufbewahrt wird, da Löschungen u.U. nachzuweisen sind.



Muster zur Übersicht der Löschfristen:

Die Einhaltung der Löschfristen sollte einmal jährlich überprüft werden. Das Ergebnis dieser Überprüfung ist zu dokumentieren.

	sofort	***6 Monate***	***4 Jahre***	***7 Jahre***	***10 Jahre***	***20 Jahre***
Beschäftigten daten					*Nach Aus-scheiden*	
Bewerber-daten		*Prüfen*				
Finanzbuch haltung				*Prüfen*		*Buchführungsdaten*
EDV	*Weblogeinträge*	*Betriebs-logdatei, Kurzzeitdaten*				
Warenwirt-schaft			*Reklamationen*	*Handelsbriefe*		*Stammdaten*

.

3.0 Muster Checkliste

3.1 Checkliste für ein Löschkonzept

Auflistung pro Abteilung, welche personenbezogenen Daten verarbeitet werden:
Art der Daten, Aufbewahrungspflichten, Besonderheiten, Datenträgernutzung

Zusammenfassung der Datenarten
Gruppieren Sie Daten, die z.B. die gleiche Aufbewahrungszeit haben oder bei denen es sich um besondere personenbezogene Daten handelt.

Archivierung der Daten
Bereits vor Archivierung festlegen, wann und wie lange die Daten aufbewahrt werden müssen und ab wann diese aus dem Archiv gelöscht werden können.

Löschregeln und -klassen bilden sowie Löschprozesse einrichten
- Startdatum + Bearbeitungszeit + Aufbewahrungsfrist = Löschklasse
- Datum der Löschklasse = konkretes Datum, zu dem ein Datensatz gelöscht werden kann = Löschregel
- regelmäßig, automatisch startende Löschläufe die auftretende Fehler protokollieren und an Mitarbeiter weitergegeben werden = Löschprozesse

Sonderfälle vorsehen
Legen Sie eine Vorgehensweise fest, wie mit zu löschenden Daten umzugehen ist, wenn ein Betroffener wünscht, dass diese außerhalb der Regel gelöscht werden sollen bzw. wenn sich herausstellt, dass unrechtmäßig erhobene Daten nicht gelöscht wurden.

Auftragsdatenverarbeitung
Prüfung der Verträge, ob und welche Klauseln zur Löschung enthalten sind und diese ggf. anpassen. Sind Sie Nutzer, verlangen Sie vom Auftragnehmer bei Löschung ein entsprechendes Löschprotokoll.