Leitfaden Löschkonzept

Ein Löschkonzept – warum?

Durch die Digitalisierung sind Daten heutzutage viel leichter übertragbar, kopierbar und speicherbar. Unglaubliche Mengen an Daten werden auf Servern gespeichert oder schlummern in E-Mailpostfächern. Aus datenschutzrechtlicher Sicht dürfen Daten jedoch nur so lange aufbewahrt werden, wie sie tatsächlich **benötigt** werden (sog. Zweckgebundenheit). Nach **Wegfall des Zwecks** besteht eine Pflicht, diese Daten zu löschen. Daher müssen technische und organisatorische Maßnahmen getroffen werden, um der Löschpflicht nachzukommen. Diese sollen durch das Löschkonzept umgesetzt werden.

1. Was ist Löschen?

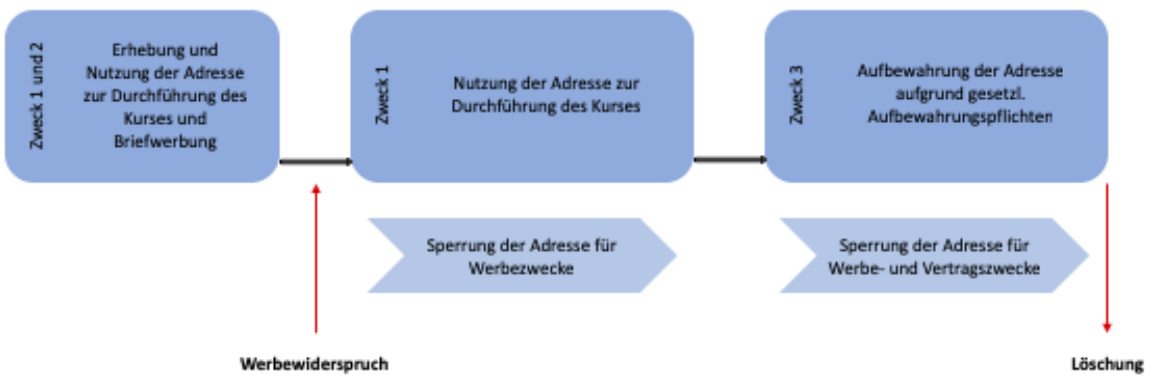
Löschen bedeutet **Beseitigen** oder **Unkenntlichmachen** von Daten mit der Folge, dass sie nicht mehr verwendet oder rekonstruiert werden können.
Die Rekonstruierbarkeit fehlt, wenn die Rekonstruktion nur mit unverhältnismäßig hohem Aufwand möglich oder aus technischen bzw. physikalischen Gründen unmöglich ist. Dabei ist die Annahme eines „unverhältnismäßig hohen Aufwands“ abhängig von der Schutzbedürftigkeit der jeweiligen Daten. Je höher die Schutzbedürftigkeit ist, desto mehr Aufwand ist zumutbar.

Beispiel für ein Löschen: Schreddern von Dokumenten; Zerstörung von Datenträgern

2. Was ist Sperren?

Von der Löschung zu unterscheiden ist die Sperrung. Sperren heißt, die Verarbeitung von Daten zu bestimmten Zwecken einzuschränken. Eine Sperrung ist in der Regel dann vorzunehmen, wenn die Daten nur noch für einen oder zwei Zwecke, z.B. die Aufbewahrung für die Steuer, benötigt werden und für eine sonstige Verwendung nicht mehr in Betracht kommen.

Das folgende Beispiel veranschaulicht den Unterschied zwischen Löschen und Sperren:



3. Was ist anonymisieren?

Anonymisieren ist das Unkenntlichmachen von Daten, so dass sie nicht mehr auf eine natürliche Person rückführbar sind. Beispiel ist das Erstellen von Statistiken: Wenn Sie der Datenbank Ihrer Teilnehmer jeweils nur das Alter entnehmen, können Sie das Durchschnittsalter Ihrer Teilnehmer bestimmen. Die in der Statistik erfassten Daten sind nicht mehr auf den einzelnen Teilnehmer rückführbar. Demnach besteht für die Statistik keine Löschpflicht.

4. Bestandteile eines Löschkonzepts

Ein Löschkonzept besteht aus zwei Teilen:

- Definition und Dokumentation von Löschregeln sowie
- Umsetzung, Überprüfung und ggf. Anpassung der Löschregeln

4.1 Definition und Dokumentation von Löschregeln

Löschregeln legen fest, wann bestimmte Datenarten zu vernichten sind. Hier gibt es Löschgebote, welche sich nach einer bestimmten Frist berechnen und solche, welche sich nach anderen Ereignissen bestimmen, z.B. dem Wegfall einer Einwilligung oder Einzug der Teilnahmegebühr bei einmaligem Lastschrifteneinzug.

Um Löschregeln festlegen zu können, müssen Sie:

- die erhobenen Daten nach Datenart kategorisieren, z.B.:

• Kundenstammdaten
• E-Mailadressen (extra Kategorie notwendig wegen Werbung)
• Bankdaten
• Bewerberdaten
• Mitarbeiterstammdaten
• Daten Geburtstagsliste
• Personalakten etc.
• Cookiedaten sowie
• IP-Nummern

- das Datum festhalten, zu dem die Daten erhoben wurden. Dies ist wichtig, um ggf. bestehende Löschfristen einhalten zu können, die i.d.R. mit Erhebung der Daten zu laufen beginnen

- die Zwecke festhalten, zu denen die Daten erhoben wurden;

- die daraus resultierenden Löschzeitpunkte notieren (z.B. nach Ablauf von 10 Jahren, nach Widerruf der Einwilligung etc.)

Gerne können Sie hier auch Ihr Verarbeitungsverzeichnis für die Erstellung heranziehen, um sich doppelte Arbeit zu sparen.

- Nicht erheblich abweichende Löschfristen für Vertragsstammdaten (z.B. 8 Jahre und 10 Jahre), die auf gesetzliche Aufbewahrungspflichten zurückzuführen sind, können zu einer **Standardlöschfrist** zusammengefasst werden. Da die Aufbewahrungsfristen oftmals erst mit Schluss des Jahres beginnen, in denen die Rechnung ausgestellt wurde, bietet es sich an, anstelle von 10 Jahren die Dauer von 11 Jahren als Standardlöschfrist festzulegen.

- Für die Löschung von Kontodaten, die im Zusammenhang mit der Erteilung eines **SEPA-Dauerlastschriftmandats** mitgeteilt wurden, kann eine Standardlöschfrist von 3 Jahren vorgesehen werden.

- Im Falle von **flexiblen und unbestimmten Löschfristen**, wie sie z.B. für Kontaktdaten gelten, die zur Beantwortung von Fragen ohne anschließende Kursbuchung bereitgestellt wurden, kann auf eine Höchstfrist zurückgegriffen werden, welche üblicherweise für die Bearbeitung einer Anfrage anfällt. Hierzu kann beispielsweise eine Löschfrist von 6 Monaten bestimmt werden. Entsprechendes gilt für die Löschfrist von E-Mailadressen, die im Rahmen Newsletter-Anmeldungen von Personen bereitgestellt wurden, die nicht zugleich Kunde sind. Die Rechtsprechung zur erlaubten Nutzungsdauer von **E-Mailadressen** ist unterschiedlich. Die als zulässig angesehene Nutzungsdauer reicht derzeit bis zu 17 Monaten nach letztmaliger Nutzung der E-Mailadresse für Werbezwecke. Zur Standardisierung dieser Löschfrist ist es vertretbar, auf diese Höchstfrist zurückzugreifen.

- Zur Bildung von Standardlöschfristen für Daten kann auf **Fristkataloge** zurückgegriffen werden.

- Auch ist es vertretbar, Startzeitpunkte für Löschfristen für Vertragsstammdaten, die jemand zunächst als Interessent und sodann als Kunde wiederholt zur Verfügung stellt, z.B. zum Standardstartzeitpunkt „Vertragsschluss“ **zusammenzulegen**, selbst wenn die Startzeitpunkte streng genommen unterschiedlich sind.

Es ist zudem Fälle denkbar, in denen Daten(arten) umgehend und ohne eine Möglichkeit, hierfür einer Löschfrist vorzusehen, zu löschen sind. Hierzu zählen vor allem:

- Unberechtigt erhobene und zu berichtigende Daten (z.B. unzulässig angefertigte Videoaufzeichnungen, nicht mehr aktuelle Anschrift z.B. wegen Umzugs)

- Duplikate von Daten, die nach Migration, Umstellung, Neueinführung oder Tests von IT-Systemen entstehen

- Daten, die allein auf Grundlage einer Einwilligung erhoben wurden (z.B. Handynummer für SMS-Werbung, Portraitfoto

4.2 Umsetzung, Überprüfung und Anpassung von Löschregeln

Es genügt **nicht**, Löschregeln nur in einem Dokument festzuhalten. Sie müssen sicher im Unternehmen umgesetzt werden und damit in die maßgeblichen Prozesse einfließen.

5. Umsetzung

Bei Umsetzung der Löschregeln empfiehlt es sich, die einzelnen Prozesse zu kategorisieren. Die konkrete Art und Weise der Umsetzung der Löschregeln differiert dabei abhängig von der jeweiligen Prozessart.

- **Interne Prozesse:** Innerhalb Ihres Unternehmens
- **Externe Prozesse**: Außerhalb Ihres Unternehmens, z.B. bei einem Dienstleister
- **Softwaregestützter interner Prozess:** Das Löschen erfolgt automatisiert über die IT. Hierzu müssen Sie sich an Ihren IT-Administrator wenden.
- **Manueller interner Prozess:** Die Löschung muss händisch erfolgen, z.B. das Schreddern oder Zurücksenden von Bewerbungsunterlagen. Hierzu sollten Sie Unternehmensrichtlinien bzw. konkrete Instruktionen vorsehen.
- **Echter externer Prozess:** Verarbeitung der Daten durch einen unabhängigen Dritten.
  Beispiel: Sie leiten die Daten aufgrund einer gesetzlichen Verpflichtung an das Jobcenter weiter. Hier müssen Sie nichts weiter veranlassen – Sie sind für die Datenverarbeitung des Dritten **nicht** verantwortlich.
- **Unechter externer Prozess:** Dies umfasst ausgelagerte Verarbeitungen, für die Sie in der Regel einen Auftragsverarbeitungsvertrag schließen, z.B. das Speichern Ihrer Webseite auf einem externen Server. Für diese Prozesse sind Sie verantwortlich und haben den Dritten entsprechend zu instruieren und auf die Umsetzung der Löschregeln zu achten.

6. Überprüfung

Die Löschregeln müssen regelmäßig **überprüft** werden. Die Hauptverantwortlichkeit hierfür sollte beim Datenschutzbeauftragten liegen. Intervall der Prüfungen, Datum der Prüfungen, jeweiliges Prüfungsergebnis und Verantwortlichkeiten sollten durch den Datenschutzbeauftragten festgelegt und dokumentiert werden.

7. Anpassung

Sollte ein Überprüfung der Löschregeln ergeben, dass eine Anpassung notwendig ist, ist diese umzusetzen und als Anpassung zu dokumentieren. Wichtig ist wiederum, diese Anpassung nicht nur „auf dem Papier“ vorzunehmen, sondern die hierfür Verantwortlichen zu informieren und die Prozesse anzupassen.

Anlage (Beispiel für einen Fristkatalog)

	Aufbewahrungsfrist in Jahren
Abtretungsunterlagen	6
Buchungsbelege	10
Lohnabrechnung zur Sozialversicherung	6
Lohn- und Gehaltskonto	10
Dokumentation zur EDV-Buchführung	10
Buchungsanfragen	6
Buchungsbestätigungen	6
Vertrag über Schulung	6
Vertrag mit Dozenten	6
Steuerlich relevante Vorstandsprotokolle	6
Vermögensaufstellungen	10
Jahresabschlüsse	10
An- und Abmeldung für Krankenkasse	6
Angestelltenversicherung	10
Verträge über Arbeitnehmersparzulage	6
Bankbelege	10
Bankbürgschaften	6
Darlehenskonten	10
EDV Programme und System Dokumentation	10
Gewährleistungsverpflichtungen	6
Grundbuchauszüge	10
Hypothekenpfandbriefe	6
Jubiliarfeierunterlagen	10
Kantinenunterlagen	10
Kaufverträge	6
Kommissionslisten	6
Lessingunterlagen	6
Leergutabrechnungen	6
Mahnungen/Mahnbescheide	6
Mietunterlagen	6
Pensionsrückstellungsunterlagen	10
Pensionszahlungen	10
Postaufträge	6

Rückstellungsunterlagen	10
Schadensmeldungen	6
Sicherungsübereignungen	6
Sozialpläne	6
Steuerbescheinigungen und –Erklärungen	10
Überstundenlisten	6
Urlaubslisten für Rückstellungen	10
Verbindlichkeiten	10
Vermögensverzeichnis	10
Vollmachtsurkunden	6
Weihnachtsgratifikation	10
Werbekostenbelege	10
Überweisungsbelege	10