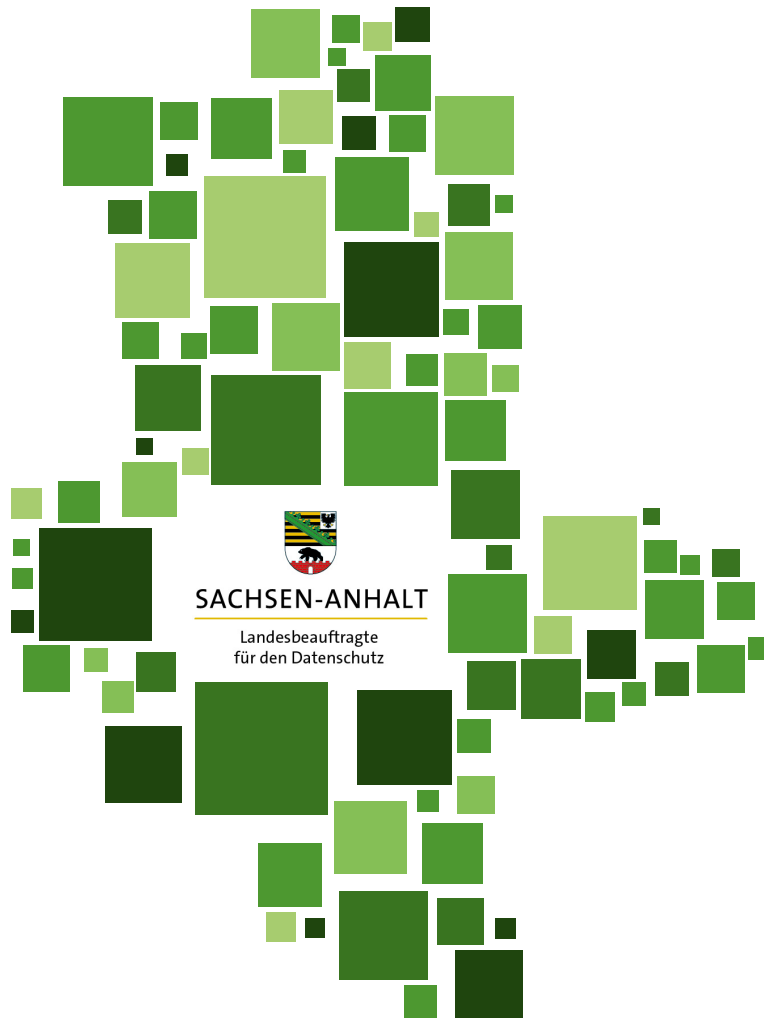




Löschkonzept für personenbezogene Daten nach DS-GVO

Leitfaden für kleine Unternehmen

Inhalt

1. Warum brauchen Sie ein Löschkonzept?	2
2. Prüfen Sie Ihre Rolle als Verantwortlicher	2
3. Rechtmäßigkeit der Datenverarbeitung sicherstellen	2
4. Vorgaben zur Datenlöschung kennen	3
5. Löschung von personenbezogenen Daten organisieren	4
6. Verzeichnis von Verarbeitungstätigkeiten anlegen	4
7. Übersicht von Systemen und Speicherorten erstellen	6
8. Löschregelkatalog aufstellen	8
9. Durchführung und Dokumentation der Löschung	10
10. Zuständigkeit und Aktualisierung des Löschkonzepts	13
11. Löschanfragen von Betroffenen bearbeiten	14
12. Wichtige Schritte im Umgang mit Löschanfragen	14
13. Hilfsmittel und Unterstützung nutzen	16

1. Warum brauchen Sie ein Löschkonzept?

Bevor Sie mit der Umsetzung beginnen, sollten Sie wissen: Ein Löschkonzept schützt Ihr Unternehmen vor Risiken und Sanktionen. Es sorgt für Übersicht, klare Abläufe und stärkt das Vertrauen von Kunden und Mitarbeitenden.

Damit das Konzept im Alltag funktioniert, sollten alle Mitarbeitenden im Unternehmen frühzeitig eingebunden werden.

2. Prüfen Sie Ihre Rolle als Verantwortlicher

Verarbeiten Sie personenbezogene Daten von Kunden, Mitarbeitenden, Lieferanten oder Website-Besuchern? Vielleicht nutzen Sie auch eine Videoüberwachung auf Ihrem Firmengelände.

Personenbezogene Daten sind dabei alle Informationen, die eine Person direkt (z. B. Name, Adresse, Geburtsdatum) oder indirekt (z. B. über eine Kundennummer oder Kombination mehrerer Angaben) identifizieren können. E-Mail-Adressen mit Klarnamen, Kfz-Kennzeichen von natürlichen Personen, Meinungen oder Bonitätsauskünfte gehören auch dazu.

Wenn Sie in diesem Sinne personenbezogene Daten erfassen, speichern oder sonst verwenden, sind Sie „Verantwortlicher“ nach Art. 4 Nr. 7 DS-GVO und müssen die Vorgaben der DS-GVO umsetzen.

Die Verarbeitung personenbezogener Daten bedarf einer datenschutzrechtlichen Erlaubnis.

3. Rechtmäßigkeit der Datenverarbeitung sicherstellen

Für jede Datenkategorie müssen Sie festlegen, warum Sie sie speichern (Zweck) und auf welcher gesetzlichen Grundlage (z. B. Einwilligung, Vertrag oder berechtigtes Interesse nach Art. 6 Abs. 1 DS-GVO).

Entfällt der Zweck der Datenverarbeitung, müssen Sie über die Löschung oder eine weitere Aufbewahrung der Daten entscheiden. Beispiele:

- **Einwilligung:**
Sie speichern die E-Mail-Adresse des Kunden, um ihm mit seiner Einwilligung einen Newsletter zu schicken. Die E-Mail-Adresse wird nur für diesen Zweck genutzt. Der Kunde bestellt den Newsletter ab.
- **Vertragserfüllung:**
Sie speichern die Adresse des Kunden, um die vertraglich vereinbarten Arbeiten am Haus des Kunden zu erbringen und um ihm die Rechnung per Post zu schicken. Die Leistung ist erbracht, der Kunde hat die Rechnung bezahlt.
- **Überwiegendes berechtigtes Interesse:**
Sie filmen außerhalb der Arbeitszeiten mit einer Videokamera Ihr Werksgelände, weil in der Vergangenheit Material gestohlen wurde. Mit einem Hinweisschild informieren Sie den Wachdienst, Postzusteller etc. über die Videoüberwachung. Es hat sich letzte Nacht kein Vorfall ereignet.

4. Vorgaben zur Datenlöschung kennen

Nach der DS-GVO gilt:

- **Speicherbegrenzung:**
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie für den festgelegten Zweck benötigt werden (Art. 5 Abs. 1 lit. e DS-GVO).
- **Umsetzung des Rechts auf Löschung einer betroffenen Person:**
Betroffene Personen können die Löschung ihrer Daten verlangen, zum Beispiel, wenn der Vertrag beendet ist, die Einwilligung widerrufen wurde oder die Daten unrechtmäßig erhoben wurden (Art. 17 DS-GVO).

Einer sofortigen Löschung stehen meist gesetzliche bzw. vertragliche Aufbewahrungspflichten oder Gewährleistungsfristen entgegen.

Die Datenlöschung setzt eine gute Organisation voraus. Sie müssen im Blick haben, wo und wie Sie personenbezogene Daten zu welchem Zweck und mit welcher Aufbewahrungsfrist speichern.

5. Löschung von personenbezogenen Daten organisieren

- Erfassen Sie, welche personenbezogenen Daten Ihr Unternehmen zu welchem Zweck verarbeitet. Legen Sie dazu ein **Verzeichnis von Verarbeitungstätigkeiten** (VVT) (s.u. Nummer 6) an.
- Dokumentieren Sie, in welchen Systemen und an welchen Orten personenbezogene Daten gespeichert werden. Schaffen Sie dazu eine detaillierte **Übersicht** (s.u. Nummer 7).
- Legen Sie fest, wer, welche Daten, wie und wann löscht. Halten Sie Aufbewahrungsfristen, Löschfristen und Zuständigkeiten in einem **Löschregelkatalog** fest (s.u. Nummer 8).
- Regeln Sie mit einer **internen Arbeitsanweisung**, wer für die Bearbeitung von Löschanfragen zuständig ist und welche Schritte dabei zu beachten sind (s.u. Nummer 9). Halten Sie fest, wie die Löschung umgesetzt wird und wie Sie die Einhaltung der Datenschutzgrundsätze nachweisen können, **Dokumentation der Löschpraxis** (s.u. Nummer 10).

6. Verzeichnis von Verarbeitungstätigkeiten anlegen

Erstellen Sie eine Übersicht aller Prozesse, bei denen personenbezogene Daten verarbeitet werden (z. B. Kundendatenverwaltung, Personalverwaltung, Marketing, Videoüberwachung).

Praxistipp: Wenn mehrere Prozesse ähnliche Datenkategorien betreffen und auf derselben Rechtsgrundlage beruhen (z. B. alle Lieferverträge), können Sie diese zusammenfassen. Für unterschiedliche Zwecke oder Abläufe legen Sie am besten separate Blätter oder Abschnitte an.

Für jede Verarbeitungstätigkeit dokumentieren Sie:

- **Name und Kontaktdaten des Verantwortlichen**
sowie ggf. des Datenschutzbeauftragten (hierzu zählen auch weitere gemeinsam Verantwortliche oder Datenschutzbeauftragte, zum Beispiel bei vertraglichen Kooperationen)
- **Zwecke der Verarbeitung**
Zum Beispiel:
 - Personalverwaltung: „Personalaktenführung/Stammdaten“, „Lohnabrechnung“, „Arbeitszeiterfassung“
 - Beschaffung/Einkauf: „Lieferantendatenverwaltung“
 - Videoüberwachung: „Feststellung von Diebstählen“
- **Beschreibung der Kategorien betroffener Personen und Daten**
Zum Beispiel:
 - Beschäftigte: Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Qualifikationen
 - Kunden: Kontaktdaten, Zahlungsdaten, Bonitätsdaten
- **Kategorien der Empfänger von Daten**
Zum Beispiel:
 - Lohnabrechnung: Banken, Sozialversicherungsträger, Finanzämter, Träger der Betriebsrente
- **Löschfristen für die verschiedenen Datenkategorien**
Zum Beispiel:
 - Handels- und steuerrechtliche Aufbewahrungspflichten für Personal- und Kundendaten
 - von Ihrem Unternehmen festgelegte Löschfristen

Eine praktische Übersicht zu Löschfristen finden Sie hier:
<https://ds-kleinunternehmen.de/arbeitshilfen>
- **Übermittlungen an ein Drittland**
- **Technische und organisatorische Maßnahmen**

Praxistipp: Unter <https://sauri.de/VerzVerarb> finden Sie eine Vorlage zur Erstellung eines ausführlichen VVT. Im Fall einer Prüfung durch die Aufsichtsbehörde sind Sie damit vorbereitet.

7. Übersicht von Systemen und Speicherorten erstellen

Dokumentieren Sie möglichst genau alle Systeme und Speicherorte, in denen personenbezogene Daten liegen. Dazu zählen zum Beispiel:

- **(Zentrale) Datenbanken:**
Hier werden oft Kundendaten, Auftragsdaten oder Mitarbeiterdaten gespeichert.
- **Backup-Systeme:**
Datensicherungen, die regelmäßig erstellt werden, enthalten meist Kopien aller wichtigen Daten.
- **E-Mail-Postfächer:**
In E-Mails finden sich häufig personenbezogene Informationen von Kunden, Mitarbeitern oder Lieferanten.
- **Excel- oder Access-Dateien:**
Viele kleine Unternehmen verwalten Daten in Tabellen, z. B. für Angebote, Rechnungen oder Personal.
- **Dokumentenablagen auf Fileserver und Cloudspeicher:**
Hier werden Verträge, Rechnungen, Angebote oder andere Dokumente abgelegt.
- **Ticketsysteme:**
Falls Sie ein System für die Bearbeitung von Kundenanfragen oder Support nutzen, werden dort ebenfalls personenbezogene Daten gespeichert.
- **Datenbanken von Auftragsverarbeitern oder Partnern:**
Wenn Sie z. B. Cloud-Dienste oder externe Dienstleister nutzen, werden dort oft auch Daten gespeichert.
- **Test-Datenbanken:**
Auch in Testumgebungen können personenbezogene Daten liegen, z. B. wenn Sie neue Software ausprobieren.

Nicht vergessen:

- **Unstrukturierte Dateien:**
Denken Sie auch an Dateien, die auf den lokalen Rechnern oder Mobilgeräten Ihrer Mitarbeitenden gespeichert sind, wie z. B. Word-Dokumente, PDFs oder Fotos.
- **Messenger-Dienste:** Wenn Ihre Mitarbeiter zur internen Kommunikation Messenger-Apps (z. B. WhatsApp, Signal) nutzen, können auch dort personenbezogene Daten ausgetauscht werden.
- **Mobile Geräte:** Smartphones, Tablets oder Laptops, die im Unternehmen genutzt werden, enthalten oft Dokumente, E-Mails, Kontakte oder andere personenbezogene Daten.
- **Cloudspeicher:** Dokumentenablagen werden für mobiles Arbeiten oder den Austausch oft in der Cloud bei entsprechenden Speicherdienstleistern organisiert (Nextcloud, OneDrive, Dropbox usw.).

Stichwort: Schatten-IT: *Die Ermittlung, ob und wo Mitarbeiter im Alltagsgeschäft personenbezogene Daten außerhalb der zentralen Systeme verarbeiten oder vielleicht sogar auf privaten Medien, ist mühsam. Bieten Sie Alternativen an und legen Sie per Arbeitsanweisung fest, wie und wo personenbezogene Daten gespeichert werden dürfen.*

Soweit Sie darüber hinaus auch noch in **Papierform** personenbezogene Daten verarbeiten („nicht-automatisiert“), müssen Sie auch diese Daten noch entsprechend berücksichtigen.

8. Löschregelkatalog aufstellen

Was gehört in den Löschregelkatalog? Erfassen Sie in einer Tabelle oder in einem Datenmanagement-Tool für jede Datenkategorie (z. B. Kundendaten, Mitarbeiterdaten, Bewerbungen) folgende Informationen:

- **Datenkategorie**
Welche Daten sind gemeint? (z. B. Bewerberdaten, Kundendaten)
- **Zweck der Verarbeitung und Rechtsgrundlage**
Warum werden die Daten gespeichert? (z. B. Vertragsabwicklung, Bewerbungsverfahren) und auf welcher gesetzlichen Grundlage? (z. B. Art. 6 Abs. 1 Satz 1 lit. b DSGVO)
- **Aufbewahrungsfrist**
Wie lange müssen die Daten mindestens aufbewahrt werden? (z. B. 10 Jahre für Rechnungen)
- **Löschfrist**
Wie schnell ggf. nach Ablauf einer Aufbewahrungsfrist werden die Daten gelöscht? (Kurze angemessene Bearbeitungszeit)
- **Ort**
Wo werden die Daten gespeichert? (z. B. im System, im Aktenschrank)
- **Zuständigkeit**
Wer ist für die Löschung zuständig? (z. B. Personal, Vertrieb)
- **Nachweis**
Wie wird die Löschung dokumentiert? (z. B. Löschprotokoll, System-Log)
- **Bemerkungen:**
Besondere Hinweise (z. B. Einwilligung für längere Speicherung möglich, steuerrechtliche Pflichten beachten).

Weitere Informationen finden Sie hier: <https://ds-kleinunternehmen.de/arbeitshilfen>

Beispiel für einen Löschregelkatalog:

Datenkategorie	Zweck der Verarbeitung + Rechtsgrundlage	Aufbewahrungsfrist	Löschfrist nach Fristende	Ort	Zuständigkeit	Nachweis	Bemerkung
Bewerberdaten	Bewerbungsverfahren Art. 6 Abs. 1 Satz 1 lit. b DS-GVO	6 Mo nach Abschluss des Verfahrens	7 Tage	Fileserver	Personalabt.	Manuelle Protokolle	Einwilligung für längere Speicherung möglich
Mitarbeiterdaten	Arbeitsvertrag	10 J nach Austritt	1 Monat	Elektronische Personalakte	Personalabt.	Logfiles	steuerrechtliche Aufbewahrungspflichten beachten
Lohnbelege	Lohn- und Gehaltsabrechnungen, Lohnkonten, Buchungsbelege § 147 AO, § 257 HGB, § 41 EStG, § 28f SGB IV	10/8/6 Jahre		Abrechnungssystem	Personalabt, Abrechnungsdienstleister		
Kundendaten	Vertragsabwicklung Art. 6 Abs. 1 Satz 1, lit. b DS-GVO	10 J nach Vertragsende	1 Monat		Vertrieb		Handels- und steuerrechtliche Pflichten
Newsletter-Abonnenten	Versand von Newslettern Art. 6 Abs. 1 Satz 1 lit. a DS-GVO	bis Widerruf der Einwilligung	7 Tage		Marketing	Logfiles	Sofortige Löschung bei Widerruf
Videoüberwachung	Gebäudesicherheit Art. 6 Abs. 1 Satz 1 lit. a DS-GVO	72 Stunden	Sofort		IT/Facility		Längere Speicherung nur bei Vorfall

Wie werden die Fristen festgelegt?

Die Aufbewahrungsfristen richten sich grundsätzlich nach den gesetzlichen Vorgaben (Handelsgesetzbuch, Abgabenordnung u.a.).

In vielen Bereichen existieren auch sogenannte Standardlöschfristen, welche sich in der Praxis herausgebildet haben. Diese können als Orientierung genutzt werden, sollten jedoch auf den jeweiligen Fall bezogen geprüft und adaptiert, nicht nur übernommen werden.

Wenn die Aufbewahrungsfrist abgelaufen ist, sind die Daten unverzüglich zu löschen (Art. 17 Abs. 1 DS-GVO). Eine kurze organisatorische Frist mit technisch bzw. organisatorisch passender Begründung (z. B. Löschläufe, Prüfungen, Sicherstellung der vollständigen Löschung) ist möglich.

Typische Aufbewahrungsfristen:

- Rechnungen: 10 Jahre (§ 257 HGB, § 147 AO)
- Handelsbriefe & Buchungsbelege: 6 bzw. 10 Jahre
- Mitarbeiterunterlagen (z. B. Arbeitsverträge): meist 3 bis 10 Jahre

Eine praktische Übersicht zu Löschfristen finden Sie z. B. hier: <https://ds-kleinunternehmen.de/arbeitshilfen>

Wann beginnt die Frist?

Der Startzeitpunkt für die Aufbewahrungs- oder Löschfrist kann unterschiedlich sein, z. B.:

- das Ende eines Vertrags
- der Abschluss eines Bewerbungsverfahrens
- der Wegfall des Zwecks (z. B. nach Projektende)
- der Zeitpunkt der Datenerhebung

Wenn mehrere Aufbewahrungsregeln gleichzeitig gelten, gilt immer die längste Frist. In manchen Fällen kann es sinnvoll sein, Daten aus Gründen der Rechtsverteidigung länger aufzubewahren. Diese Entscheidung sollten Sie im Löschkonzept dokumentieren und begründen.

9. Durchführung und Dokumentation der Löschung

Halten Sie als Nachweis fest, welche Datenkategorien wann, von wem und auf welche Weise gelöscht (automatisch/manuell) wurden. Die personenbezogenen Daten selbst sollten dabei nicht Teil der Dokumentation sein.

Diese Dokumentation kann in Form eines **Löschprotokolls** (z. B. als Tabelle in Excel oder Word) oder durch automatische Protokolle (Logfiles) in Ihren IT-Systemen erfolgen. Wichtig ist, dass die Aufzeichnungen aussagekräftig und im Bedarfsfall vorzeigbar sind – etwa bei einer Prüfung durch die Datenschutz-Aufsichtsbehörde.

Löschen oder Vernichten?

Mit dem **Löschen** werden personenbezogene Daten so aus den IT-Systemen entfernt, dass sie mit vertretbarem Aufwand nicht wiederhergestellt werden können. Die Datenträger selbst (z. B. Computer, Speichermedien) bleiben dabei erhalten und können weiter genutzt werden.

Beim **Vernichten** wird der Datenträger selbst zerstört, sodass ein späteres Auslesen der Überreste unmöglich ist. Ein typisches Beispiel ist das Schreddern von Papierakten, CDs oder Festplatten. Die Vernichtung elektronischer Datenträger ist **immer dann erforderlich**, wenn eine sichere Löschung der Datenträger per Software etwa aufgrund von Defekten oder Beschädigungen nicht mehr durchführbar ist. Für eine Datenträgervernichtung bieten sich sowohl Geräte, die selbst betrieben werden können, als auch zertifizierte Dienstleister an.

Wie wird gelöscht?

Beim Löschvorgang sind folgende Umstände zu unterscheiden:

- Handelt es sich um analoge oder elektronische Datenhaltung?
- Werden die Daten beim Unternehmen selbst oder bei Dienstleistern aufbewahrt?
- Muss die Datenlöschung manuell erfolgen oder gibt es Möglichkeiten zu Automatisieren?

Analoge Datenhaltung auf Papier:

Die DIN 66399 unterscheidet je nach Sensibilität der personenbezogenen Daten 3 Schutzklassen und 7 Sicherheitsstufen. Nutzen Sie einen Aktenvernichter, der mindestens der Sicherheitsstufe P-3 entspricht. Für besonders schützenswerte Daten (z. B. Gesundheitsdaten, Personalakten) wird mindestens Stufe P-4 empfohlen. Werden die Papierunterlagen durch einen Dienstleister vernichtet, ist ein Auftragsverarbeitungsvertrag gem. Art 28 DS-GVO abzuschließen, der auch Festlegungen bezüglich der Schutzklasse und Sicherheitsstufe enthält.

Elektronische Datenhaltung:

Daten in IT-Systemen sollten immer mit den vom System bzw. den Anwendungen zur Verfügung gestellten Mitteln und Funktionen gelöscht werden. Wenn möglich zeitgesteuert und unter Aktivierung einer Protokollierung. Elektronische Datenträger (z. B. Festplatten, USB-Sticks) sollten vor der Entsorgung oder Verwendung zu anderen Zwecken sicher überschrieben oder mit speziellen Lösch-Werkzeugen behandelt werden, damit eine Wiederherstellung ausgeschlossen ist. Auch dieser Vorgang ist ähnlich dem manuellen Löschen mit Angaben zur Bezeichnung des Datenträgers zu protokollieren.

Datenträger, die nicht mehr sicher überschrieben werden können, sind entsprechend der Schutzklasse und Sicherheitsstufe nach DIN 66399 zu vernichten. Die Auswahl der Schutzklasse und Sicherheitsstufe richtet sich nach der Sensibilität der gespeicherten Daten.

Aufbewahrung im Unternehmen:

Die Löschung muss innerbetrieblich geregelt sein und beim eigenen Personal angewiesen werden. Das Personal muss die entsprechenden Funktionen in den Systemen und Anwendungen kennen ggf. dafür geschult werden. Automatismen sind im Vier-Augen-Prinzip und ggf. unter Hinzuziehung der IT-Abteilung einzurichten und sollten genauestens dokumentiert sein.

Aufbewahrung beim Dienstleister:

Lassen Sie Daten beim Dienstleister (z. B. Cloudanbieter) löschen, indem selbst entsprechende Funktion aufgerufen werden oder Weisungen an den Dienstleister erteilt werden. Dienstleister müssen als Auftragsverarbeiter gem. Art. 28 DS-GVO vertraglich gebunden sein.

Manuelles Löschen:

Auch eine manuell durchgeführte Löschung muss protokolliert werden. Eine sinnvolle Protokollierung enthält Angaben zum Datenbestand (ohne Nennung personenbezogener Daten), das Datum der Löschung und den Namen der Person oder Abteilung, die die Löschung vorgenommen hat.

Automatisches Löschen:

Viele moderne Programme (z. B. DMS, CRM, ERP) bieten automatische Löschfunktionen. Prüfen Sie, ob diese aktiviert und richtig eingestellt sind, damit Daten nach Ablauf der Fristen automatisch gelöscht oder archiviert werden. Das System sollte die Löschung dann selbst in seinen Logfiles protokollieren.

Achtung: *Das Verschieben von Dokumenten und Dateien in den Papierkorb des Betriebssystems oder E-Mail-Programms entspricht nicht den Anforderungen an eine Löschung. Oft sind einzelne Dateien mit wenig Aufwand wiederherstellbar, selbst wenn der Papierkorb geleert wurde.*

Besonderheiten bei Backups beachten!

Gerade bei Backups (Datensicherungen) ist Vorsicht geboten: Oft ist es technisch nicht möglich, einzelne Datensätze gezielt aus einem Backup zu löschen. Deshalb sollten Sie Ihr Backup-Konzept so gestalten, dass Backups regelmäßig überschrieben werden und keine gelöschten Daten wiederhergestellt werden können.

Backups sollten zweckgebunden verwendet werden, also nur für die Wiederherstellung versehentlich oder böswillig verloren gegangener Daten und nicht für die Wiederherstellung bereits ordnungsgemäß gelöschter Daten. Dies sollte organisatorisch geregelt sein. Der administrative Zugriff auf Backups sollte auf ein Minimum an Personen beschränkt sein.

Stellen Sie sicher, dass nach einer Wiederherstellung eines IT-Systems aus einem Backup zwischenzeitlich gelöschte personenbezogene Daten nicht wieder in das System eingespielt werden („Sperrliste“). Dazu müssen diese vorab in geeigneter Form erfasst werden.

10. Zuständigkeit und Aktualisierung des Löschkonzepts

Anweisungen zu Zuständigkeiten und klaren Abläufen regeln!

- Legen Sie fest, wer im Unternehmen für das Löschen und die Kontrolle zuständig ist (z. B. Chef, Buchhaltung, IT).
- Schulen Sie Ihre Mitarbeiter, damit sie keine Daten unkontrolliert weiter speichern (Stichwort: Schatten-IT) und die Löschvorgaben konsequent einhalten.
- Legen Sie Regeln für lokale Dateien, E-Mails und mobile Geräte fest.
- Definieren Sie klare Abläufe, wie bei einer Löschanfrage vorzugehen ist und wie mit gesperrten Daten in der Zwischenzeit umzugehen ist.
- Achten Sie darauf, dass auch Verträge mit Dienstleistern (z. B. Cloud-Anbietern, Auftragsverarbeitern) Regelungen zur Löschung nach Zweckwegfall enthalten, damit auch außerhalb Ihres Unternehmens gelöscht wird.

Regelmäßige Überprüfung und Aktualisierung des Löschkonzepts!

Ihr Löschkonzept sollte mindestens einmal im Jahr überprüft und bei Bedarf angepasst werden. Gründe dafür können sein:

- neue IT-Systeme oder Programme
- geänderte Geschäftsabläufe
- neue oder geänderte gesetzliche Vorgaben (z. B. verkürzte Aufbewahrungsfristen)

Stellen Sie sich regelmäßig (möglichst jährlich) folgende Fragen:

- Werden alle definierten Löschfristen eingehalten?
- Funktionieren die technischen Löschmechanismen wie vorgesehen?
- Gibt es neue Datenarten, die ins Konzept aufgenommen werden müssen?
- Entspricht alles dem aktuellen Stand der Technik und Gesetzeslage?

11. Löschanfragen von Betroffenen bearbeiten

Wer kann eine Löschung verlangen?

Jede Person, deren Daten Sie gespeichert haben, zum Beispiel Kunden, Geschäftspartner, Mitarbeiter, Besucher Ihrer Website oder Personen, die auf Ihrer Videoüberwachung zu sehen sind, kann von Ihnen verlangen, dass ihre personenbezogenen Daten gelöscht werden.

Wie lange haben Sie Zeit?

Sie müssen grundsätzlich unverzüglich, aber spätestens innerhalb eines Monats auf eine Löschanfrage reagieren. In Ausnahmefällen (z. B. wenn die Anfrage sehr kompliziert ist oder viele Anfragen gleichzeitig kommen) dürfen Sie sich bis zu zwei weitere Monate Zeit nehmen. In diesem Fall müssen Sie die Person aber innerhalb des ersten Monats über die Verzögerung und die Gründe informieren (Art. 17, Art. 12 Abs. 3 DS-GVO). Bevor Sie Daten löschen, beachten Sie die Schritte unter Nummer 12.

Wie muss die Antwort aussehen?

Die Antwort muss verständlich und klar sein. Auf Wunsch kann die Auskunft auch mündlich erfolgen, zum Beispiel am Telefon (Art. 12 Abs. 1 DS-GVO).

Damit Sie diese Vorgaben einhalten, sollten Sie klare Prozesse und Arbeitsanweisungen im Unternehmen festlegen.

12. Wichtige Schritte im Umgang mit Löschanfragen

1. Löschanfragen erfassen:

Löschanfragen können auf verschiedenen Wegen eingehen – schriftlich, per E-Mail, telefonisch oder auch persönlich. Jede Anfrage sollte dokumentiert werden, damit Sie im Streitfall Ihren Nachweispflichten nachkommen können.

2. Zuständigkeit festlegen:

Bestimmen Sie, wer im Unternehmen für die Bearbeitung von Löschanfragen verantwortlich ist (z. B. Chef, Datenschutzbeauftragter, Buchhaltung).

3. Identitätsprüfung:

Prüfen Sie, ob die anfragende Person tatsächlich die betroffene Person ist. Das ist wichtig, um Verwechslungen zu vermeiden und keine Daten an Unbefugte herausgegeben werden. Bei begründeten Zweifeln können Sie zusätzliche Informationen zur Verifikation anfordern, z. B. einen Adressabgleich.

4. Inhaltliche Prüfung der Löschanfrage:

Ein Recht auf Löschung besteht zum Beispiel, wenn:

- die Daten nicht mehr für die Erfüllung der Geschäftszwecke benötigt werden,
- die Verarbeitung auf einer Einwilligung beruht und diese widerrufen wurde,
- die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und keine vorrangigen berechtigten Gründe für eine weitere Verarbeitung vorliegen,
- die Daten unrechtmäßig verarbeitet wurden.

5. Ablehnung von Löschgesuchen:

Eine Löschung darf abgelehnt werden, wenn:

- die Identität der antragstellenden Person nicht geklärt werden kann,
- die Daten aus rechtlichen Gründen (z. B. handels- oder steuerrechtliche Aufbewahrungspflichten für Geschäftsbriefe oder Buchungsbelege) noch benötigt werden,
- die Daten zur Verteidigung von Rechtsansprüchen weiterhin erforderlich sind.

In diesen Fällen müssen die Daten gesperrt werden (d. h. sie dürfen nicht mehr für andere Zwecke genutzt werden) und sind zu löschen, sobald der Hinderungsgrund wegfällt. Die betroffene Person ist über die Entscheidung und die Begründung transparent zu informieren (Art. 12 DS-GVO).

6. Durchführung und Bestätigung der Löschung:

Wenn die Löschanfrage berechtigt ist, führen Sie die Löschung unverzüglich durch und bestätigen Sie der betroffenen Person, dass die Daten gelöscht wurden.

7. Dokumentation:

Jeder Löschvorgang sollte dokumentiert werden, inklusive der Anfrage, des Prüfergebnisses, der ergriffenen Maßnahmen und des Erledigungsdatums.

8. Andere Empfänger informieren:

Wenn Sie die Daten an Dritte oder Auftragnehmer weitergegeben haben (z. B. Steuerberater, Cloud-Anbieter), müssen Sie diese ebenfalls über die Löschung informieren (Art. 19 DS-GVO).

Praxistipp: Prüfen Sie, ob die zu löschenden Daten auch tatsächlich gelöscht wurden!

„Ziemlich gelöschte“ Daten bereiten in der Praxis immer wieder Probleme. Sie tauchen zur Unzeit auf und können Schadensersatzansprüche der betroffenen Person auslösen und/oder Maßnahmen der Datenschutz-Aufsichtsbehörde nach sich ziehen.

13. Hilfsmittel und Unterstützung nutzen

Vorlagen und weiterführende Informationen:

- <https://ds-kleinunternehmen.de/arbeitshilfen>
- <https://lsaur.l.de/VerzVerarb>
- <https://lsaur.l.de/Kurzpapiere>

Sie können gerne bei der Landesbeauftragten und Ihren Mitarbeitern nachfragen.



Disclaimer: Dieser Leitfaden erhebt keinen Anspruch auf Vollständigkeit, sondern soll eine erste Hilfestellung zur Umsetzung der DS-GVO-Anforderungen sein

Impressum:

Landesbeauftragte für den Datenschutz
Otto-von-Guericke-Str. 34a, 39104 Magdeburg
Telefon: 0391 81803-0
E-Mail: poststelle@lfd.sachsen-anhalt.de
Internet: <https://datenschutz.sachsen-anhalt.de>
Stand: September 2026