



Cortina Consult

WHITEPAPER

Löschkonzept in der Praxis

Ein Umsetzungsleitfaden für KMU

Cortina Consult · Fachlicher Entwurf · Stand: 14. Oktober 2026

Cortina Consult GmbH

Hafenweg 24 · 48155 Münster

Tel. +49 251 95 20 37 - 40 · post@cortina-consult.de

www.cortina-consult.com

Inhalt

1. Was ein Löschkonzept leisten muss
 2. Zuständigkeiten festlegen
 3. Datenbestände und Speicherorte erfassen
 4. Löschregeln entwickeln
 5. Typische Datenbestände richtig einordnen
 6. Musterfall: Ein Kundenauftrag ist abgeschlossen
 7. Löschung zuverlässig umsetzen
 8. Dienstleister und Backups einbeziehen
 9. Löschanfragen bearbeiten
 10. Durchführung nachweisen und kontrollieren
 11. Einführung und laufende Pflege
- Ihr Einstieg
-

Personenbezogene Daten entstehen in nahezu jedem Unternehmensbereich: bei Kundenanfragen, Aufträgen, Bewerbungen, der Personalverwaltung und im täglichen Austausch. Sie liegen in Anwendungen, E-Mails, Papierakten und gemeinsamen Ablagen. Hinzu kommen lokale Kopien, externe Dienstleister und Datensicherungen.

Mit der Zeit wird es schwieriger, den Überblick zu behalten. Welche Daten werden noch gebraucht? Welche Unterlagen müssen aufbewahrt werden? Wer veranlasst die Löschung – und wie lässt sich feststellen, ob sie funktioniert hat?

Ein Löschkonzept beantwortet diese Fragen. Es verbindet fachliche Entscheidungen mit Zuständigkeiten und technischen Verfahren. Dieser Leitfaden zeigt, wie KMU schrittweise ein solches Konzept aufbauen und im Alltag anwenden können.

Er richtet sich an Geschäftsführung, Datenschutzverantwortliche, Fachbereiche und IT deutscher Unternehmen. Besondere Branchenanforderungen, etwa im Gesundheitswesen oder bei regulierten Finanzunternehmen, benötigen zusätzliche Regeln. Die Beispiele dienen der Orientierung und müssen an die tatsächlichen Verarbeitungsvorgänge angepasst werden.

1. Was ein Löschkonzept leisten muss

Personenbezogene Daten dürfen grundsätzlich nur so lange gespeichert werden, wie dies für ihre zulässigen Zwecke erforderlich ist. Entfällt die Erforderlichkeit und besteht kein anderer tragfähiger Grund für die weitere Verarbeitung, müssen sie gelöscht werden. Unternehmen müssen diese Prüfung auch ohne Anfrage einer betroffenen Person organisieren.

Ein Löschkonzept legt dafür fest:

- welche personenbezogenen Daten verarbeitet werden;
- welchem Zweck die Verarbeitung dient;
- wo die Daten gespeichert sind;
- wann die weitere Speicherung überprüft wird oder endet;
- welche Aufbewahrungsgründe berücksichtigt werden müssen;
- wer entscheidet, löscht und kontrolliert;
- wie die Durchführung nachgewiesen wird.

Die DSGVO schreibt diese Pflichten insbesondere über Speicherbegrenzung, Rechenschaftspflicht und das Recht auf Löschung vor. Ein Dokument allein erfüllt sie noch nicht. Entscheidend ist, dass die beschriebenen Abläufe tatsächlich umgesetzt werden.

Quelle: DSGVO, insbesondere Art. 5, 17 und 24.

Praxisgedanke: Eine Rechnung kann aufbewahrungspflichtig sein, während überholte Gesprächsnotizen zum selben Kunden bereits gelöscht werden müssen. Deshalb braucht das Konzept Regeln für konkrete Datenbestände.

2. Zuständigkeiten festlegen

In einem kleinen Betrieb kann eine Person mehrere Aufgaben übernehmen. Mit zunehmender Unternehmensgröße werden Entscheidungen und Umsetzung häufig auf verschiedene Stellen verteilt. Die Verantwortung muss in beiden Fällen erkennbar bleiben.

Aufgabe	Typische Zuständigkeit
Konzept beauftragen, Ressourcen bereitstellen und freigeben	Geschäftsführung
Zwecke, benötigte Daten und fachliche Anforderungen bestimmen	Jeweiliger Fachbereich
Gesetzliche Aufbewahrung von Rechnungs- und Buchführungsunterlagen beurteilen	Buchhaltung, gegebenenfalls mit steuerlicher Beratung
Löschfunktionen, Berechtigungen und Backup-Verfahren umsetzen	IT und beauftragte Dienstleister
Datenschutzrechtlich beraten und die Einhaltung überwachen	Datenschutzbeauftragter, sofern bestellt
Löschanfragen koordinieren und Fristen überwachen	Benannte zuständige Stelle

Der Datenschutzbeauftragte unterstützt und überwacht. Seine Benennung überträgt ihm nicht automatisch die operative Verantwortung für sämtliche Löschentscheidungen.

Für jede Aufgabe sollten eine Vertretung und ein Eskalationsweg feststehen. Das ist besonders wichtig, wenn Anfragen während Urlaub oder Krankheit eingehen oder Löschläufe fehlschlagen.

3. Datenbestände und Speicherorte erfassen

Beginnen Sie mit den Verarbeitungstätigkeiten und den beteiligten Fachbereichen. Ein vorhandenes Verzeichnis von Verarbeitungstätigkeiten bietet dafür eine Grundlage. Ergänzen Sie es um die tatsächlichen Speicherorte.

Erfassen Sie neben den zentralen Anwendungen auch:

- E-Mail-Postfächer und gemeinsame Funktionspostfächer;
- Fileserver, Cloudspeicher und Dokumentenarchive;
- Tabellen, Exporte und lokale Downloads;

- mobile Geräte und Papierakten;
- Ticketsysteme, Messenger und Testumgebungen;
- Dienstleister, Unterauftragnehmer und Datensicherungen.

Die Prüfung sollte gemeinsam mit den Mitarbeitenden erfolgen. Sie kennen häufig Ablagen und Arbeitskopien, die in einer technischen Systemübersicht fehlen.

Arbeitshilfe: Speicherortinventar

Datenbestand	Zweck	System oder Ablage	Fachlich zuständig	Dienstleister und weitere Kopien
Kundenkontaktdaten	Auftragsbearbeitung	CRM	Vertrieb	CRM-Anbieter, Exporte
Rechnungen	Abrechnung und gesetzliche Aufbewahrung	Buchhaltungssoftware, Archiv	Buchhaltung	Abrechnungsdienstleister
Bewerbungsunterlagen	Personalauswahl	Bewerbungsportal, Postfach	Personal	Portalbetreiber, Downloads
Projektdokumente	Durchführung des Auftrags	Projektablage	Projektleitung	Cloudanbieter, lokale Kopien

Ergänzen Sie, welche Anwendung den maßgeblichen Bestand führt und wie Kopien entstehen. So lässt sich später bestimmen, an welchen Stellen eine Löschung durchgeführt werden muss.

Praktischer Einstieg: Wählen Sie zunächst einen überschaubaren Prozess, etwa abgeschlossene Kundenaufträge. Erproben Sie daran die Bestandsaufnahme und erweitern Sie das Vorgehen anschließend.

4. Löschregeln entwickeln

Für jeden Datenbestand sind vier Fragen zu beantworten:

1. Wird er noch für den bisherigen Zweck benötigt?
2. Besteht eine gesetzliche Aufbewahrungspflicht?
3. Ist eine weitere Speicherung für einen anderen zulässigen Zweck erforderlich?
4. Welche Daten und welcher Zeitraum sind dafür tatsächlich notwendig?

Eine Ausnahme rechtfertigt nur die erforderliche weitere Verarbeitung. Sie sollte deshalb mit dem betroffenen Umfang, ihrer Begründung und einem erneuten Prüftermin dokumentiert werden.

Löschklassen bilden

Eine **Löschklasse** ist eine Gruppe von Daten mit demselben Verarbeitungszweck, demselben Startzeitpunkt und derselben Löschrfrist. Eine **Löschregel** legt für eine Löschklasse fest, wann die Frist beginnt und wie gelöscht wird.

Entscheidend ist die Gruppierung nach Zweck statt nach System. Eine Löschklasse gilt dann über alle Anwendungen, Ablagen und Archive hinweg. Wer je System eine Liste führt, pflegt dieselbe Entscheidung mehrfach und übersieht Kopien.

Diese Systematik ist nicht vorgeschrieben. Sie stammt aus der DIN EN ISO/IEC 27555:2025-09 (vormals DIN 66398) und ihre Anwendung ist freiwillig. Verpflichtend ist allein das Ergebnis. Die Methode ist der kürzeste Weg dorthin, weil Sie dann keine eigene Systematik entwickeln müssen.

Die folgenden Löschklassen kommen in fast jedem Unternehmen vor. Die Werte sind Beispiele und müssen an Ihre tatsächlichen Verarbeitungen angepasst werden.

Löschklasse	Startzeitpunkt	Löschfrist
Recruiting, abgelehnt	Versand der Absage	6 Monate
Kunden, inaktiv	Letzte Bestellung	Betrieblich festzulegen; Belege gesondert
Marketing, Newsletter	Abmeldung	Versand unverzüglich stoppen
Buchhaltung, Rechnungen	Schluss des Kalenderjahres	8 Jahre (§ 147 AO)
Personal, ausgeschieden	Ende des Arbeitsverhältnisses	Je Unterlage; Lohnkonten 6 Jahre
Verträge, Geschäftspartner	Vertragsende	6 Jahre (§ 257 HGB)
Web-Analytics	Erhebung	Nach Zweck; Produktvorgaben sind keine Rechtsgrundlage
Support-Tickets	Ticket-Schließung	Betrieblich festzulegen

Achtung bei Mischklassen: Eine Löschklasse „Kunden“ darf nicht an der Rechnungsfrist hängen. Der Beleg ist aufbewahrungspflichtig, das Kundenprofil nicht. Beides gehört in getrennte Löschklassen, sonst wird das gesamte Profil acht Jahre mitgeschleppt.

Eine Verjährungsfrist ist dabei keine automatische Pflicht, sämtliche Unterlagen aufzubewahren. Die regelmäßige Verjährung beträgt zwar drei Jahre; ihr Beginn hängt grundsätzlich von Anspruchsentstehung und Kenntnis ab. Besondere Fristen und Hemmungen können hinzukommen.

Quellen: § 195 BGB, § 199 BGB.

Was in eine vollständige Löschregel gehört

Feld	Inhalt
Regelnummer	Eindeutige Bezeichnung, beispielsweise K-01
Datenbestand	Präzise Beschreibung der betroffenen Daten
Zweck und Rechtsgrundlage	Begründung der Verarbeitung und weiteren Speicherung
Auslöser und Fristbeginn	Beispielsweise Zweckwegfall, Ablehnung oder Jahresende
Dauer	Gesetzliche Frist oder begründete betriebliche Festlegung
Speicherorte	Anwendungen, Ablagen, Kopien und Dienstleister
Verantwortliche Stelle	Entscheidung, Durchführung und Kontrolle
Verfahren	Automatische Funktion oder konkrete Arbeitsanweisung
Ausnahmen	Voraussetzungen, Freigabe und erneuter Prüftermin
Nachweis	Zeitpunkt, Ergebnis und gegebenenfalls Fehlerbehandlung

5. Typische Datenbestände richtig einordnen

Die folgenden Regeln zeigen die notwendige Differenzierung. Sie ersetzen keine vollständige Bestandsprüfung.

Datenbestand	Ausgangspunkt für die Regel
Rechnungen und Buchungsbelege	Grundsätzlich acht Jahre ab Schluss des maßgeblichen Kalenderjahres; Sonderregeln und Verlängerungen berücksichtigen.
Handels- und Geschäftsbriefe	Grundsätzlich sechs Jahre ab Schluss des Jahres des Empfangs oder Versands.
Bücher, Inventare und bestimmte Abschlussunterlagen	Grundsätzlich zehn Jahre; die jeweils einschlägige Vorschrift und ihren Fristbeginn prüfen.
CRM-Profil und Gesprächsnotizen	Nach Ende der Betreuung beziehungsweise Zweckwegfall prüfen. Keine pauschale Aufbewahrungsfrist für das gesamte Profil.
Bewerbungsunterlagen abgelehnter Personen	Nach Auswahlende gegebenenfalls befristete Speicherung zur Rechtsverteidigung. Bis zu sechs Monate nach Ablehnung sind eine aufsichtsbehördliche Orientierung, keine gesetzliche Mindestfrist.
Bewerberpool	Gesonderter Zweck, wirksame Einwilligung und festgelegte Dauer; Widerruf berücksichtigen.

Datenbestand	Ausgangspunkt für die Regel
Lohnkonten	Bis zum Ablauf des sechsten Kalenderjahres nach der zuletzt eingetragenen Lohnzahlung.
Newsletter-Versandbestand	Bei Widerruf den Versand unverzüglich stoppen. Versanddaten, erforderliche Nachweise und gegebenenfalls Ausschlussmerkmale getrennt bewerten.
Arbeitskopien und Exporte	Nach Wegfall des Arbeitszwecks löschen, soweit keine eigenständige Aufbewahrung erforderlich ist.

Für gewöhnliche KMU ergeben sich die handels- und steuerrechtlichen Fristen insbesondere aus § 257 HGB, § 147 AO und § 14b UStG. Steuerliche Gründe können eine Aufbewahrung über die reguläre Dauer hinaus erforderlich machen.

Die Bewerberorientierung beschreibt das Bayerische Landesamt für Datenschutzaufsicht. Die Lohnkontenfrist regelt § 41 EStG.

Personalakten aufteilen: Arbeitsverträge, Lohnkonten, Arbeitszeitznachweise, Krankheitsinformationen und Bewerbungsunterlagen benötigen jeweils eigene Regeln. Eine gemeinsame Frist für alle Mitarbeiterdaten ist dafür zu grob.

6. Musterfall: Ein Kundenauftrag ist abgeschlossen

Ein Dienstleistungsbetrieb mit 85 Mitarbeitenden hat einen Auftrag für eine Privatkundin abgeschlossen. Die Rechnung wurde am 15. September 2026 ausgestellt und bezahlt. Eine laufende Betreuung besteht nicht. Am 14. Oktober 2026 verlangt die Kundin die Löschung ihrer Daten.

Die Daten liegen im CRM, im Rechnungsarchiv, in Projektordnern, E-Mails, lokalen Arbeitskopien und Backups.

Entscheidung über die einzelnen Bestände

Bestand	Entscheidung
Rechnung und Buchungsbelege	Die erforderlichen Unterlagen bleiben im Archiv. Bei einer 2026 ausgestellten Rechnung endet die reguläre achtjährige Aufbewahrungsfrist am 31. Dezember 2034. Vor der Löschung sind mögliche weitere Aufbewahrungsgründe zu prüfen.
Auftragsbestätigung und geschäftliche Korrespondenz	Soweit sie als Handels- oder Geschäftsbriefe einzuordnen sind, gilt grundsätzlich eine sechsjährige Frist. Für 2026 empfangene oder versandte Briefe endet sie regulär am 31. Dezember 2032.

Bestand	Entscheidung
CRM-Profil	Telefonnummer, Präferenzen und Gesprächsnotizen werden einzeln bewertet. Ohne weiteren erforderlichen Zweck werden sie gelöscht. Angaben, die für den Zugriff auf aufbewahrungspflichtige Unterlagen erforderlich sind, werden auf das notwendige Maß begrenzt.
Projektdokumente	Der Fachbereich bestimmt, welche Unterlagen noch gesetzlich oder für begründete Rechtsverteidigung benötigt werden. Übrige personenbezogene Inhalte werden gelöscht.
E-Mails und lokale Kopien	Aufbewahrungspflichtige Nachrichten werden geordnet archiviert. Überholte Terminabstimmungen, Downloads und Arbeitskopien werden gelöscht, sofern kein weiterer erforderlicher Zweck besteht.
Dienstleister und Backups	Die Umsetzung umfasst auch externe Systeme. Verbleibende Sicherungskopien werden nach dem festgelegten Backup-Verfahren behandelt.

Organisation und Antwort

Eine benannte Stelle koordiniert die Prüfung. Buchhaltung und Projektleitung treffen die fachlichen Entscheidungen; IT und Dienstleister setzen sie um.

Die Kundin erhält eine verständliche Antwort: Welche Daten wurden gelöscht? Welche Unterlagen bleiben aus welchem Grund gespeichert? Wie wird mit Sicherungskopien verfahren?

Eine pauschale Bestätigung, alle Daten seien gelöscht, wäre in diesem Fall falsch. Ebenso unzutreffend wäre die Aussage, wegen der Rechnung müsse die vollständige Kundenakte acht Jahre unverändert gespeichert bleiben.

7. Löschung zuverlässig umsetzen

Anwendungen und Ablagen

Nutzen Sie geeignete Löschfunktionen der jeweiligen Systeme. Prüfen Sie, ob sie auch Anhänge, verknüpfte Datensätze und relevante Kopien erfassen. Das Entfernen eines Eintrags aus einer Bildschirmansicht belegt noch keine vollständige Löschung.

Archivierung ist weiterhin Speicherung. Auch ein Archiv benötigt einen zulässigen Zweck, passende Zugriffsrechte und eine Regel für die spätere Löschung.

Bei E-Mails und Dateien müssen Papierkörbe, Versionen, synchronisierte Ablagen und Exporte berücksichtigt werden. Welche Maßnahmen erforderlich sind, hängt vom System und der Speicherarchitektur ab.

Papier und Datenträger

Papierunterlagen werden entsprechend ihrem Schutzbedarf vernichtet. Das Verfahren muss auch Sammlung, Zwischenlagerung und Transport berücksichtigen.

Bei elektronischen Datenträgern richtet sich das Verfahren nach dem Schutzbedarf. Die DIN 66399 beschreibt die Schutzklassen und Sicherheitsstufen für die Vernichtung. Für die Vernichtung gilt sie auch dann, wenn Sie die Löschrufen nach einer anderen Systematik bilden.

Ein verbreiteter Irrtum betrifft das Überschreiben: Mehrfachdurchgänge sind technisch nicht erforderlich, ein Durchgang genügt. Bei SSDs und Flashspeichern ist Überschreiben dagegen grundsätzlich unzuverlässig, weil Wear-Leveling und Overprovisioning Bereiche unerreichbar lassen. Dort führen Secure-Erase-Befehle oder kryptografische Löschung zum Ziel.

Schutzbedarf	Angemessenes Verfahren	Beispiele
Gering	Standardlöschung im System	Allgemeine Korrespondenz
Normal	Überschreiben; bei SSD Secure Erase oder kryptografische Löschung	Kunden- und Vertragsdaten
Hoch	Zertifizierte Löschung, bei magnetischen Medien Degaußen	Gehalts- und Finanzdaten
Sehr hoch	Physische Vernichtung nach DIN 66399	Gesundheits- und biometrische Daten (Art. 9 DSGVO)

Automatische Löschläufe

Automatisierung erleichtert wiederkehrende Aufgaben. Vor der Aktivierung sollten Auswahlregeln, Ausnahmen, Berechtigungen und Fehlermeldungen getestet werden.

Ein regelmäßiger Löschlauf muss zur jeweiligen Pflicht passen. Ein monatlicher Lauf rechtfertigt nicht automatisch, Daten einen zusätzlichen Monat zu speichern. Besonders bei Löschanfragen kann ein gesonderter zeitnaher Ablauf erforderlich sein.

8. Dienstleister und Backups einbeziehen

Externe Dienstleister

Klären Sie zunächst die Rolle des Dienstleisters. Er kann Auftragsverarbeiter oder eigenständig Verantwortlicher sein. Daraus ergeben sich unterschiedliche Zuständigkeiten und vertragliche Anforderungen.

Bei Auftragsverarbeitung muss erkennbar sein:

- wie Löschungen ausgelöst werden;
- welche Systeme und Unterauftragnehmer betroffen sind;

- wie lange verbleibende Kopien gespeichert werden;
- wie die Durchführung nachgewiesen wird;
- was bei Vertragsende geschieht.

Die eigene Verantwortung endet nicht mit dem Versand einer Löschanweisung. Das Unternehmen muss die Umsetzung angemessen nachvollziehen können.

Backups

Backups dienen der Wiederherstellung und können bereits im Produktivsystem gelöschte Daten enthalten. Häufig lassen sich einzelne Datensätze darin nicht ohne Weiteres entfernen.

Das Backup-Konzept braucht deshalb eine begründete maximale Speicherdauer, begrenzte Zugriffe und einen dokumentierten Ablauf für Löschung und Wiederherstellung. Technische Schwierigkeiten schaffen keine pauschale Ausnahme von Datenschutzpflichten.

Wird ein älterer Stand wiederhergestellt, müssen zwischenzeitliche Löschungen berücksichtigt werden, bevor die Daten wieder regulär genutzt werden. Dafür kann ein geschützter Abgleich erforderlich sein. Auch dessen Inhalt und Aufbewahrung sind auf das notwendige Maß zu begrenzen.

Kontrollfrage: Kann das Unternehmen nach einer Wiederherstellung erkennen und umsetzen, welche personenbezogenen Daten inzwischen gelöscht wurden?

9. Löschanfragen bearbeiten

Eine Anfrage kann per E-Mail, Brief, Telefon oder persönlich eingehen. Mitarbeitende müssen wissen, an wen sie diese weiterleiten.

Ein praktikabler Ablauf umfasst:

1. **Erfassen:** Eingangstag, Anliegen, betroffene Person und Antwortfrist dokumentieren.
2. **Identität klären:** Nur bei erforderlicher Prüfung zusätzliche Informationen anfordern und deren Umfang begrenzen.
3. **Bestände finden:** Fachbereiche, Systeme und relevante Empfänger einbeziehen.
4. **Entscheiden:** Für jeden Bestand Löschung oder begründete weitere Speicherung festhalten.
5. **Umsetzen:** Löschungen durchführen und verbleibende Daten auf den erforderlichen Zweck begrenzen.
6. **Empfänger berücksichtigen:** Mitteilungspflichten prüfen und Auftragsverarbeiter entsprechend anweisen.
7. **Antworten:** Ergebnis verständlich erläutern und die Bearbeitung dokumentieren.

Grundsätzlich muss innerhalb eines Monats über die ergriffenen Maßnahmen informiert werden. Eine Verlängerung ist unter bestimmten Voraussetzungen möglich und innerhalb des ersten Monats zu begründen. Eine gebotene Löschung ist unverzüglich umzusetzen.

Wird ein Antrag ganz oder teilweise abgelehnt, sind Gründe, Beschwerdemöglichkeit und gerichtlicher Rechtsbehelf mitzuteilen.

Quelle: Datenschutzaufsicht Baden-Württemberg: Recht auf Löschung.

10. Durchführung nachweisen und kontrollieren

Ein Löschprotokoll soll den Vorgang nachvollziehbar machen. Es sollte gelöschte Inhalte nicht vollständig erneut speichern.

Arbeitshilfe: Löschprotokoll

Feld	Beispiel
Vorgang oder Regelnummer	K-03
Betroffener Bestand	Nicht mehr erforderliche CRM-Gesprächsnotizen
System	CRM
Datum und Verfahren	Ausführung über freigegebene Löschfunktion
Zuständige Stelle	Vertrieb / IT
Ergebnis	Erfolgreich; zwei Datensätze zur begründeten Ausnahmeprüfung zurückgestellt
Kontrolle	Ergebnisprüfung dokumentiert
Offene Maßnahmen	Ausnahmeprüfung mit festgelegtem Termin

Auch Protokolle und Unterlagen zu Löschanfragen benötigen eine eigene Aufbewahrungsregel und passende Zugriffsrechte.

Arbeitshilfe: Wirksamkeitsprüfung

- Sind alle relevanten Speicherorte erfasst?
- Sind Fristbeginn und Löschbedingungen eindeutig?
- Werden Ausnahmen begründet und erneut geprüft?
- Funktionieren Löschläufe tatsächlich?
- Werden Fehler erkannt und behoben?
- Sind lokale Kopien und Dienstleister berücksichtigt?
- Werden Löschungen nach einer Backup-Wiederherstellung umgesetzt?
- Stimmen Datenschutzhinweise und tatsächliche Speicherpraxis überein?

11. Einführung in acht Schritten

Führen Sie das Konzept schrittweise ein. Die begleitende Excel-Vorlage bildet diese acht Schritte als Checkliste ab.

1. **Verantwortung benennen.** Eine zuständige Person und eine Stellvertretung festlegen.
2. **Verarbeitungsverzeichnis heranziehen.** Das Verzeichnis nach Art. 30 DSGVO als Grundlage nutzen und alle Datenarten erfassen.
3. **Datenströme kartieren.** Anwendungen, Datenbanken, Backups, Cloud-Dienste, Postfächer, mobile Geräte und Papierakten.
4. **Aufbewahrungsfristen ermitteln.** Gesetzliche und vertragliche Fristen je Datenkategorie recherchieren und festhalten.
5. **Löschklassen bilden.** Nach Verarbeitungszweck, Startzeitpunkt und Löschfrist gruppieren – nicht nach System.
6. **Löschregeln dokumentieren.** Je Löschklasse die vollständige Regel mit präzisiertem Startzeitpunkt.
7. **Löschverfahren festlegen.** Automatisiert, manuell oder Datenträgervernichtung nach DIN 66399, passend zum Schutzbedarf.
8. **Protokollierung und Review.** Nachweis einrichten und mindestens jährliche Überprüfung terminieren.

Beginnen Sie nicht mit dem gesamten Unternehmen. Nehmen Sie einen überschaubaren Bereich, etwa abgeschlossene Kundenaufträge, und gehen Sie die acht Schritte einmal vollständig durch. Dieser erste Durchlauf zeigt, welche Angaben fehlen und ob die Systeme leisten, was die Regel annimmt.

Überprüfen Sie das Konzept regelmäßig und zusätzlich bei neuen Anwendungen, Dienstleistern, Geschäftsprozessen oder rechtlichen Änderungen. Eine jährliche Überprüfung kann als organisatorischer Ausgangspunkt dienen; wesentliche Änderungen müssen zeitnah berücksichtigt werden.

Für die Freigabe sollten Geschäftsführung, Fachbereiche und IT dieselben Fragen beantworten können: Was wird gelöscht? Wann geschieht das? Wer ist zuständig? Welche Ausnahmen gelten? Wie wird das Ergebnis geprüft?

Ihr Einstieg

Wählen Sie einen Datenbestand, dessen Lebenszyklus gut nachvollziehbar ist. Erfassen Sie seine Speicherorte, entwickeln Sie eine vollständige Löschregel und prüfen Sie die Umsetzung.

Dieser erste Durchlauf zeigt, welche Informationen fehlen, welche Systeme Unterstützung benötigen und wo Zuständigkeiten geklärt werden müssen. Daraus lässt sich das unternehmensweite Konzept gezielt weiterentwickeln.

**Sie möchten Ihr Löschkonzept aufbauen oder bestehende Regeln überprüfen?
Sprechen Sie mit Cortina Consult über Ihre Ausgangslage und die nächsten
Umsetzungsschritte.**

Quellen und Einordnung

Dieser Leitfaden wurde eigenständig für die betriebliche Umsetzung aufbereitet. Als Ausgangspunkt diente der Leitfaden „Löschkonzept für personenbezogene Daten nach DS-GVO“ der Landesbeauftragten für den Datenschutz Sachsen-Anhalt, Stand September 2026. Fristenbeispiele wurden anhand der oben genannten Rechtsquellen überprüft und differenziert.

Behördlicher Ausgangsleitfaden

Die Darstellung konzentriert sich auf typische Abläufe deutscher KMU. Maßgeblich bleiben die jeweils einschlägigen Vorschriften, der konkrete Verarbeitungszweck und die tatsächlichen technischen Möglichkeiten.