

Löschanträge nach der DSGVO

Gelöscht ist noch nicht erledigt

Praxisleitfaden für Geschäftsführung, Datenschutz, Legal, IT, HR, Kundenservice und Vendor Management

8 Kernfragen	5 Prozessrisiken	1 30-Minuten-Test
------------------------	----------------------------	-----------------------------

Vom Antrag bis zur abschließenden Antwort

1 Anfrage erkennen Eingang erfassen	2 Rechtlich prüfen Löschgrund / Ausnahme	3 Daten finden Systeme & Dienstleister	4 Maßnahme umsetzen Löschen / sperren	5 Antwort & Nachweis Kommunizieren / dokumentieren
---	--	--	---	--

Worum es geht

Ein Löschantrag ist mehr als ein technischer Löschvorgang. Unternehmen müssen prüfen, ob und in welchem Umfang ein Anspruch besteht, die erforderliche Maßnahme in allen relevanten Systemen umsetzen, die betroffene Person fristgerecht informieren und den Vorgang nachvollziehbar dokumentieren. Der Fall EXTIA zeigt besonders deutlich: Selbst eine automatische Löschung kann die Pflicht zur Antwort nicht ersetzen.

Die wichtigste Erkenntnis

Technische Umsetzung und Bearbeitung eines Betroffenenantrags sind zwei getrennte Aufgaben. Ein Datensatz kann bereits gelöscht sein und der Antrag trotzdem noch nicht ordnungsgemäß abgeschlossen sein.

Stand: September 2026



Warum Löschanträge Prozesssache sind

Der Ausgangsfall zeigt eine organisatorische Schwachstelle, die praktisch jedes Unternehmen betreffen kann.

Löschanträge scheitern selten an nur einer Norm. Häufig greifen mehrere Probleme ineinander: Anfragen werden nicht erkannt, Daten liegen in mehreren Systemen, Aufbewahrungspflichten werden pauschal behandelt oder die technische Löschung erfolgt, ohne dass die betroffene Person eine fristgerechte Rückmeldung erhält.

300.000 €

Bußgeld im EXTIA-Fall

204 von 265 Löschanträgen
2024 nicht ordnungsgemäß behandelt

Der Ausgangspunkt

CNIL, Entscheidung vom 21.07.2026, Nr. SAN-2026-010.

EXTIA erhielt 2024 insgesamt 265 Löschanträge. Die CNIL stellte 12 nicht bearbeitete Anträge, 166 fehlende Rückmeldungen und 26 verspätete Rückmeldungen fest.

Eine zusätzliche Auskunftsanfrage wurde erst nach mehr als einem Jahr beantwortet. Der Fall zeigt: Automatische Löschung kann die materielle Löschpflicht beeinflussen, ersetzt aber nicht die Antwort auf den konkreten Antrag.

Die konkrete Bußgeldhöhe ist einzelfallbezogen und lässt sich nicht als feste Bußgeldformel auf andere Unternehmen übertragen.

Die vier Rechtsanker

Art. 12 Abs. 3 und 4 DSGVO

Über die ergriffenen Maßnahmen ist unverzüglich und grundsätzlich innerhalb eines Monats zu informieren. Wird einem Antrag ganz oder teilweise nicht entsprochen, sind Gründe und Rechtsbehelfsmöglichkeiten mitzuteilen.

Art. 17 Abs. 1 und 3 DSGVO

Das Recht auf Löschung setzt einen Löschgrund voraus. Ausnahmen, etwa gesetzliche Pflichten oder die Verteidigung von Rechtsansprüchen, müssen konkret für den jeweiligen Datenbestand geprüft werden.

Art. 5 Abs. 2 DSGVO

Die Rechenschaftspflicht verlangt, dass ein Unternehmen die Einhaltung der Datenschutzgrundsätze nachweisen kann. Bei Betroffenenanträgen bedeutet das eine nachvollziehbare Fallakte.

Art. 24 Abs. 1 und Art. 28 DSGVO

Geeignete technische und organisatorische Maßnahmen sowie die praktische Einbindung von Auftragsverarbeitern müssen sicherstellen, dass Anfragen nicht nur auf dem Papier, sondern im Prozess funktionieren.

Fünf typische Prozessrisiken

1 Anfrage wird nicht erkannt

E-Mail, Kontaktformular oder Ticket bleibt liegen oder wird zu spät an die zuständige Stelle weitergeleitet.

2 Daten werden nicht vollständig gefunden

CRM, HR-System, Dateiablage, Alt-Systeme, Archive oder Dienstleister werden bei der Suche übersehen.

3 Prüfung bleibt zu pauschal

Aufbewahrungspflichten oder Rechtsansprüche werden als pauschaler Grund genutzt, anstatt einzelne Datenbestände konkret zu prüfen.

4 Löschung und Antwort fallen auseinander

Die technische Maßnahme ist umgesetzt, aber niemand informiert die betroffene Person fristgerecht.

5 Nachweis fehlt

Einzelne E-Mails und Screenshots existieren, aber kein zusammenhängender Nachweis von Eingang, Prüfung, Umsetzung und Antwort.



Der Selbsttest: Eingang und Identität

Markieren Sie jede Frage mit Ja, Nein oder Unklar. Entscheidend ist nicht nur die Regel, sondern ob sie im Alltag nachweisbar funktioniert.

1

Werden Löschanträge über alle vorgesehenen Eingangskanäle erkannt und sofort erfasst?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Mit Eingang der Anfrage beginnen Fristen und interne Pflichten. Ein Antrag darf nicht davon abhängen, ob er im „richtigen“ Postfach landet.

Gute Umsetzung: E-Mail, Formular, Portal, Kundenservice, Vertrieb und HR haben klare Weiterleitungsregeln; Eingang und Friststart werden zentral dokumentiert.

Prüfnachweis: Liste der Eingangskanäle, Ticket oder Registereintrag, Zeitstempel, Arbeitsanweisung.

Typisches Warnsignal: Eine Anfrage steht mehrere Tage in einem allgemeinen Postfach oder wird nur mündlich weitergegeben.

Praxismaßnahme: Zentralen Erfassungsweg mit Fristerinnerung und Stellvertretung einrichten.

2

Wird die Identität angemessen geprüft, ohne unnötige Hürden zu schaffen?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Unternehmen müssen verhindern, dass Daten unberechtigt gelöscht oder offengelegt werden. Zusätzliche Informationen sollten nur verlangt werden, wenn begründete Zweifel bestehen.

Gute Umsetzung: Die Prüftiefe orientiert sich am Risiko und am vorhandenen Kontaktkanal. Zusätzliche Nachweise werden nur bei Bedarf angefordert.

Prüfnachweis: Identitätsprüfkonzept, dokumentierte Zweifel, Verifikationsweg, Löschregeln für unnötige Ausweiskopien.

Typisches Warnsignal: Standardmäßig wird immer eine Ausweiskopie verlangt, obwohl die Identität bereits zuverlässig feststeht.

Praxismaßnahme: Risikobasierte Identitätsprüfung mit zulässigen Alternativen definieren.

Zwischenstand

Wenn Sie bei einer dieser Fragen „Nein“ oder „Unklar“ markieren, besteht ein erhöhtes Risiko, dass Anfragen zu spät oder an die falsche Person bearbeitet werden. Stabilisieren Sie zuerst Eingang und Identitätsprüfung.

Der Selbsttest: Datenübersicht und Rechtsprüfung

Jetzt geht es darum, ob Sie die relevanten Daten vollständig finden und den Löschanspruch konkret statt pauschal beurteilen können.

3

Können Sie alle betroffenen Daten, Systeme und Dienstleister vollständig identifizieren?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Eine Löschung nur im führenden System kann unvollständig sein. Daten können zusätzlich in E-Mails, HR- oder CRM-Systemen, Dateiablagen, Alt-Systemen und bei Dienstleistern liegen.

Gute Umsetzung: Es gibt eine aktuelle System- und Datenübersicht. Für typische Betroffenengruppen sind Suchpfade und zuständige Systemowner bekannt.

Prüfnachweis: Verzeichnis von Verarbeitungstätigkeiten, Systemlandkarte, Datenfluss, Suchprotokoll, Dienstleisterliste.

Typisches Warnsignal: Das Team prüft nur das System, in dem die Anfrage eingegangen ist.

Praxismaßnahme: Für Kunden, Bewerber und Mitarbeiter verbindliche Suchpfade und Systemlisten hinterlegen.

4

Wird für jeden Antrag konkret geprüft, ob ein Löschgrund und gegebenenfalls eine Ausnahme vorliegt?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Art. 17 DSGVO kennt Löschgründe und Ausnahmen. Gesetzliche Aufbewahrungspflichten oder Rechtsansprüche können einer vollständigen Löschung entgegenstehen, aber nicht automatisch für alle Daten.

Gute Umsetzung: Die Entscheidung wird datenbezogen getroffen: löschen, teilweise löschen, einschränken oder begründet weiter speichern.

Prüfnachweis: Prüfvermerk, Rechtsgrundlage, Aufbewahrungskonzept, dokumentierte Begründung, zuständige Stelle.

Typisches Warnsignal: „Löschantrag“ löst pauschal entweder Total-Löschung oder pauschale Ablehnung aus.

Praxismaßnahme: Standardisierten Prüfpfad für Löschgründe, Ausnahmen und Teilbestände verwenden.

Praxisregel

Eine Aufbewahrungspflicht ist kein Freibrief zum Behalten. Prüfen Sie konkret, welche Daten für welchen Zweck noch benötigt werden und welche Daten trotzdem gelöscht werden können.

Der Selbsttest: Frist und Kommunikation

Technische Umsetzung und Antwortpflicht laufen nebeneinander. Genau an dieser Schnittstelle entstehen besonders häufig Fehler.

5

Wird die Monatsfrist nach Art. 12 Abs. 3 DSGVO aktiv und unabhängig von der Technik gesteuert?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Die Information über die ergriffenen Maßnahmen muss grundsätzlich innerhalb eines Monats erfolgen. Die Frist läuft ab Eingang des Antrags, nicht erst nach Abschluss technischer Arbeiten.

Gute Umsetzung: Fristen werden automatisch überwacht. Erforderliche Verlängerungen werden früh erkannt, begründet und innerhalb des ersten Monats mitgeteilt.

Prüfnachweis: Fristenkalender, Ticketregeln, Eskalationen, Verlängerungsmitteilung, Abschlusszeitpunkt.

Typisches Warnsignal: Die Frist wird erst geprüft, wenn die Löschung technisch abgeschlossen ist.

Praxismaßnahme: Friststeuerung sofort bei Eingang starten und Eskalationsschwellen festlegen.

6

Erhält die betroffene Person auch dann eine Rückmeldung, wenn Daten automatisch oder turnusmäßig gelöscht wurden?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Eine tatsächliche Löschung beantwortet den individuellen Antrag nicht automatisch. Art. 12 DSGVO verlangt eine Information über die ergriffenen Maßnahmen.

Gute Umsetzung: Automatische Löschregeln sind mit einem Kommunikationsprozess verbunden. Der konkrete Antrag wird registriert, geprüft und ausdrücklich abgeschlossen.

Prüfnachweis: Antwortvorlage, Versandnachweis, Systemstatus, Protokoll der automatischen Löschung.

Typisches Warnsignal: Der Vorgang wird intern als „erledigt“ markiert, weil der Datensatz ohnehin automatisch verschwindet.

Praxismaßnahme: Technische Löschung und Antwort als zwei getrennte Abschlusskriterien definieren.

Praxisregel

Ein Löschkonzept steuert den Lebenszyklus von Daten. Ein Prozess für Betroffenenrechte steuert individuelle Anträge. Beide Prozesse können verbunden werden, dürfen aber nicht miteinander verwechselt werden.



Der Selbsttest: Umsetzung und Nachweis

Zum Abschluss geht es um Dienstleister, Archive, Backups und die Frage, ob der gesamte Vorgang später nachvollziehbar bleibt.

7

Sind Dienstleister, Archive, Alt-Systeme und Sicherungskonzepte in der Umsetzung berücksichtigt?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Daten können außerhalb des führenden Systems fortbestehen. Nicht jede Kopie muss sofort physisch entfernt werden, aber Aufbewahrung, Zugriff und spätere Überschreibung müssen konzeptionell beherrscht werden.

Gute Umsetzung: Auftragsverarbeiter erhalten klare Weisungen. Archive und Backups folgen dokumentierten Löschrück- oder Sperrkonzepten; Wiederherstellungen berücksichtigen den Löschrückstatus.

Prüfnachweis: AV-Verträge, Löschrückkonzept, Weisung oder Ticket an Dienstleister, Backup- und Wiederherstellungskonzept.

Typisches Warnsignal: Im CRM ist der Datensatz weg, aber Exporte, SaaS-Tools oder Altsysteme bleiben unbeachtet.

Praxismaßnahme: System- und Dienstleisterkette vollständig erfassen und technische Restbestände mit Schutzmaßnahmen dokumentieren.

8

Können Sie Entscheidung, Umsetzung und Antwort als zusammenhängenden Vorgang nachweisen?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Im Beschwerde- oder Prüfungsfall zählt nicht nur das Ergebnis, sondern auch, ob das Unternehmen den Ablauf nachvollziehbar belegen kann.

Gute Umsetzung: Ein Fallprotokoll verbindet Eingang, Identitätsprüfung, Rechtsentscheidung, technische Maßnahmen, Dienstleisteraktionen und Antwort.

Prüfnachweis: Fallakte oder Ticket, Zeitstempel, Logs, Rechtsvermerk, Versandnachweis, Abschlusskontrolle.

Typisches Warnsignal: Es gibt einzelne E-Mails und Screenshots, aber keinen vollständigen Ablaufnachweis.

Praxismaßnahme: Einheitliches Fallprotokoll mit Pflichtfeldern und Abschlusscheck einführen.

Schnelle Selbstausswertung

7-8 x Ja	4-6 x Ja	0-3 x Ja
Gute Ausgangslage. Prüfen Sie trotzdem regelmäßig Fristen, Systemabdeckung und Nachweise mit realistischen Tests.	Mehrere Lücken sind möglich. Priorisieren Sie Friststeuerung, Rechtsprüfung, Systemkette und Dokumentation.	Der Prozess sollte zeitnah grundlegend geprüft und verbindlich geordnet werden.

Wichtig

Die Selbstausswertung ist nur eine praktische Orientierung und keine rechtliche Bewertung. Ein einzelner kritischer Fehler kann bereits erheblich sein.



Wer sollte sich darum kümmern?

Löschanträge sind ein bereichsübergreifender Prozess. Eine eindeutige Prozessverantwortung verhindert Zuständigkeitslücken.

Der Datenschutzbeauftragte berät und überwacht, sollte aber nicht automatisch zum operativen Prozessverantwortlichen gemacht werden. Entscheidend ist, dass Eingang, Rechtsprüfung, technische Umsetzung, Kommunikation und Nachweis einer klaren Verantwortungslogik folgen.

Bereich	Kernaufgabe	Typischer Nachweis
Prozessowner / Privacy	Gesamtprozess, Fristen, Standards, Eskalation und Qualitätskontrolle koordinieren.	Prozessbeschreibung, KPI, Fallstichprobe, Eskalationsmatrix
Legal / Datenschutz	Löschgründe, Ausnahmen, Aufbewahrung und Antwortinhalte rechtlich einordnen.	Prüfschema, Rechtsvermerk, Vorlagen
IT / Systemowner	Daten auffinden, löschen oder sperren, Schnittstellen und Logs beherrschen.	Systemliste, Löschjobs, Logs, Wiederherstellungskonzept
HR / Kundenservice / Fachbereich	Anfragen erkennen, Kontext liefern und die operative Bearbeitung unterstützen.	Arbeitsanweisung, Ticketkategorie, Schulungsnachweis
Vendor Management	Auftragsverarbeiter und SaaS-Dienste in Löschung und Nachweis einbinden.	AV-Vertrag, Weisung, Löschbestätigung, Kontrollnachweis
Datenschutzbeauftragter	Beraten, überwachen, sensibilisieren und bei Beschwerden oder Kontrollen unterstützen.	Beratungsvermerk, Audit- oder Kontrollbericht, Schulung

Vier Sätze, die Mitarbeiter erkennen sollten

Typische Formulierung	Was daraus folgen kann
„Bitte löschen Sie meine Daten.“	Löschantrag nach Art. 17 DSGVO prüfen und weiterleiten.
„Ich möchte, dass Sie meine Bewerbungsunterlagen entfernen.“	Kann ein Löschantrag sein; HR-Prozess und gespeicherte Datenbestände prüfen.
„Warum haben Sie meine Daten noch?“	Kann auf eine Lösch-, Auskunfts- oder Rechtmäßigkeitsfrage hinweisen.
„Bitte bestätigen Sie mir die Löschung.“	Die Rückmeldung ist Teil der Bearbeitung und darf nicht vergessen werden.

Praxisregel

Benennen Sie eine Stelle, die den Gesamtprozess besitzt. Sie muss nicht jede technische oder rechtliche Aufgabe selbst erledigen, aber sicherstellen, dass alle Beteiligten zusammenarbeiten und offene Fälle sichtbar bleiben.



Der 30-Minuten-Praxistest

Prüfen Sie nicht nur den Löschknopf, sondern den vollständigen Weg vom Eingang bis zur abschließenden Antwort.

1	☐	Testprofil anlegen Einen fiktiven Kunden- oder Bewerberdatensatz in typischen Systemen anlegen. Keine echten personenbezogenen Daten verwenden.
2	☐	Antrag stellen Über einen realen Eingangskanal eine Löschanfrage absenden und Uhrzeit dokumentieren.
3	☐	Routing prüfen Kontrollieren, ob Ticket, Frist, Verantwortlicher und gegebenenfalls Identitätsprüfung korrekt ausgelöst werden.
4	☐	Datenkette prüfen CRM, HR, Dateiablage, E-Mail, SaaS-Dienste und gegebenenfalls Archive anhand Ihrer Systemliste abgleichen.
5	☐	Rechtsentscheidung simulieren Für den Testfall einen eindeutigen Löschgrund ohne Aufbewahrungspflicht wählen und die Entscheidung dokumentieren.
6	☐	Umsetzung prüfen Löschung oder Sperrung in allen Testsystemen nachvollziehen; Dienstleister- und Backup-Prozess zumindest anhand des Konzepts verifizieren.
7	☐	Antwort prüfen Kontrollieren, ob eine verständliche Rückmeldung erstellt, fristgerecht ausgelöst und versandseitig nachweisbar ist.
8	☐	Abweichungen festhalten Fehler, fehlende Systeme, manuelle Schritte und Verantwortliche dokumentieren und in Maßnahmen überführen.

Welche Nachweise sollten auffindbar sein?

Bereich	Beispiele
Eingang	Datum, Uhrzeit, Kontaktkanal, Friststart, zuständige Stelle.
Rechtsprüfung	Löschgrund, Ausnahme, Aufbewahrungspflicht, Begründung bei Teilsablehnung.
Technische Umsetzung	Betroffene Systeme, Statuswechsel, Logs, Dienstleisteraktionen, Restbestände.
Kommunikation	Antwort an die betroffene Person, Versandzeitpunkt, Verlängerungs- oder Ablehnungsmitteilung.
Kontrolle	Abschlusscheck, Abweichungen, Korrekturmaßnahmen und Verantwortliche.



Ihr Maßnahmenplan

Nutzen Sie diese Seite als interne Arbeitsvorlage. Nicht jede Maßnahme ist in jedem Unternehmen zwingend erforderlich.

Priorisieren Sie zuerst Punkte, bei denen Anfragen übersehen werden, Fristen nicht zuverlässig laufen, Datenbestände unvollständig erfasst sind oder die Antwortpflicht nach technischer Umsetzung vergessen werden kann.

Maßnahme	Verantwortlich	Priorität	Frist	Status	Nachweis
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	

Drei Prioritäten, wenn Sie heute anfangen

Zwingend prüfen

Zentrale Erfassung, Verantwortlichkeit und Friststeuerung für alle Betroffenenanfragen.

Empfohlen

System- und Dienstleisterkette für typische Löschfälle vollständig dokumentieren und regelmäßig testen.

Zusätzliche Absicherung

End-to-End-Tests mit internem Testdatensatz, Vertretungsregeln und Lastspitzen-Szenarien etablieren.

Merksatz

Ein Löschprozess ist nicht dann gut, wenn Daten möglichst schnell verschwinden. Er ist gut, wenn das Unternehmen nachvollziehbar entscheiden kann, was gelöscht werden muss, was weiter gespeichert werden darf, wann und wie umgesetzt wurde und wie die betroffene Person informiert wurde.



Rechtsgrundlagen, Quellen und Hinweise

Die drei wichtigsten Punkte

1

Löschung und Antwort sind getrennte Pflichten. Technische Löschung ersetzt nicht die Information nach Art. 12 DSGVO.

2

Nicht jeder Löschantrag führt zur vollständigen Löschung. Art. 17 DSGVO verlangt eine fallbezogene Prüfung von Löschgründen und Ausnahmen.

3

Der belastbare Prozess endet mit einem Nachweis. Eingang, Entscheidung, Umsetzung und Kommunikation müssen zusammenhängend dokumentiert werden.

Rechtsgrundlagen

Art. 12 Abs. 3 und 4 DSGVO: Fristen und Informationspflichten bei der Bearbeitung von Betroffenenrechten sowie Begründung, wenn einem Antrag nicht entsprochen wird.

Art. 17 Abs. 1 und 3 DSGVO: Voraussetzungen des Rechts auf Löschung und gesetzliche Ausnahmen.

Art. 5 Abs. 2 DSGVO: Rechenschaftspflicht: Der Verantwortliche muss die Einhaltung der Datenschutzgrundsätze nachweisen können.

Art. 24 Abs. 1 DSGVO: Geeignete technische und organisatorische Maßnahmen zur Sicherstellung und zum Nachweis DSGVO-konformer Verarbeitung.

Art. 28 DSGVO: Bei Auftragsverarbeitern muss Unterstützung bei Betroffenenrechten vertraglich und praktisch funktionieren.

Kurzes Glossar

Begriff	Einfach erklärt
Betroffenenanfrage	Antrag einer Person auf Ausübung eines Rechts nach der DSGVO, zum Beispiel Auskunft, Berichtigung oder Löschung.
Löschgrund	Voraussetzung aus Art. 17 Abs. 1 DSGVO, bei deren Vorliegen personenbezogene Daten grundsätzlich zu löschen sind.
Ausnahme	Fall nach Art. 17 Abs. 3 DSGVO, in dem Daten trotz eines Löschbegehrens weiter verarbeitet oder aufbewahrt werden dürfen oder müssen.
Einschränkung / Sperrung	Begrenzung der weiteren Verarbeitung. Sie kann je nach Rechtslage an die Stelle einer vollständigen Löschung treten.
Auftragsverarbeiter	Externer Dienstleister, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Fallprotokoll	Zusammenhängende Dokumentation von Eingang, Prüfung, Maßnahmen, Kommunikation und Abschluss eines Betroffenenfalls.

Quellen

Primärquelle: CNIL, [Délibération SAN-2026-010 vom 21.07.2026](#)

CNIL-Mitteilung: [Failure to respect the rights of individuals: EUR 300,000 fine against EXTIA](#)

EDPB-Meldung zur Entscheidung

Hinweis

Dieses Dokument dient der allgemeinen Information und als praktische Arbeitshilfe. Es ersetzt keine rechtliche Prüfung des konkreten Einzelfalls. Ob und in welchem Umfang Daten zu löschen, einzuschränken oder weiter aufzubewahren sind, hängt vom jeweiligen Zweck, der Rechtsgrundlage, gesetzlichen Pflichten und dem konkreten Antrag ab.

