

Betroffenen Anfragen rechtssicher bearbeiten

Schritt-für-Schritt-Leitfaden zur DSGVO-konformen Bearbeitung von Auskunfts-, Löscho- und Widerspruchsanfragen mit Fristen, Identitätsprüfung und Dokumentationspflichten zur Vermeidung von Bußgeldern und Beschwerden bei Aufsichtsbehörden.

Betroffenen Anfragen müssen unverzüglich, spätestens innerhalb eines Monats beantwortet werden. Diese Checkliste führt Sie Schritt für Schritt durch den rechtssicheren Prozess – von Eingang bis Dokumentation.

1. Eingangsmanagement & Fristenkontrolle

- ☐ Eingangszeitpunkt dokumentiert (Frist beginnt sofort, nicht mit Bearbeitung)
- ☐ Anfrage an Datenschutzbeauftragten weitergeleitet (nicht Kundendienst)
- ☐ Eingangsbestätigung an Betroffenen versendet (gleicher Kommunikationsweg)
- ☐ Frist im Ticketsystem/Kalender eingetragen (1 Monat, max. 3 Monate)
- ☐ Bei Auftragsverarbeitung: Anfrage umgehend an Verantwortlichen weitergeleitet

2. Identitätsprüfung des Betroffenen

- ☐ Identität mit zusätzlichen Merkmalen geprüft (Geburtsdatum, Anschrift, Kundennummer)
- ☐ Bei sensiblen Daten: Personalausweis angefordert (geschwärzt bis auf Name, Anschrift, Geburtsdatum, Gültigkeit)
- ☐ Bei Bevollmächtigung: Vollmacht und Identität beider Personen geprüft
- ☐ Bei fehlender Identifikation: Anfrage gemäß Art. 12 Abs. 2 DSGVO eingestellt

3. Art der Betroffenenanfrage bestimmen

- ☐ Auskunft (Art. 15): Welche Daten, Zweck, Empfänger, Speicherdauer, Herkunft?
- ☐ Berichtigung (Art. 16): Falsche/unvollständige Daten korrigieren
- ☐ Löschung (Art. 17): Zweck erfüllt, unrechtmäßige Verarbeitung, Widerruf?
- ☐ Einschränkung (Art. 18): Richtigkeit bestritten, unrechtmäßig, Widerspruch?
- ☐ Datenübertragbarkeit (Art. 20): Kopie in maschinenlesbarem Format (.csv, .json)
- ☐ Widerspruch (Art. 21): Verarbeitung beenden (außer zwingende berechtigte Gründe)

4. Informationen zusammenstellen (max. 3 Wochen)

- ☐ Alle personenbezogenen Daten aus allen Systemen extrahiert (CRM, ERP, HR, Backup)
- ☐ Verarbeitungszwecke dokumentiert (Rechtsgrundlage nach Art. 6 DSGVO)
- ☐ Empfänger/Kategorien von Empfängern aufgelistet (Dienstleister, Behörden)
- ☐ Speicherdauer angegeben (gesetzliche Fristen, Vertragszweck)
- ☐ Herkunft der Daten dokumentiert (direkt vom Betroffenen oder Drittquelle)
- ☐ Automatisierte Entscheidungen geprüft (Profiling, KI, Scoring)
- ☐ Drittlandtransfers dokumentiert (USA, UK, andere Nicht-EU-Länder)

5. Ausnahmen prüfen

- ☐ Gesetzliche Aufbewahrungsfristen (HGB, AO) → Löschung verweigern, Einschränkung anbieten

- ☐ Rechtsansprüche (Verträge, Gewährleistung) → Löschung ablehnen, Begründung dokumentieren
- ☐ Öffentliches Interesse (Forschung, Statistik, Archiv) → Einschränkung statt Löschung
- ☐ Geschäftsgeheimnisse/Rechte Dritter → Daten schwärzen vor Auskunft

6. Antwort vorbereiten & versenden

- ☐ Sprache: präzise, verständlich, einfach (keine Fachbegriffe ohne Erklärung)
- ☐ Form: Schriftlich oder elektronisch (bei E-Mail-Anfrage elektronisch bevorzugt)
- ☐ Bei elektronischer Übermittlung: E-Mail & Anhänge verschlüsseln (z.B. PGP, S/MIME)
- ☐ Bei großen Datenmengen: Verschlüsselter USB-Stick oder sicherer Download-Link
- ☐ Kostenfreiheit gewährleistet (nur zusätzliche Kopien dürfen berechnet werden)
- ☐ Bei Fristverlängerung: Betroffenen innerhalb 1. Monats über Verlängerung + Gründe informiert

7. Dokumentation & Nachverfolgung

- ☐ Alle Schritte mit Zeitstempel im Ticketsystem dokumentiert
- ☐ Kopie der Antwort archiviert (Nachweispflicht nach Art. 5 Abs. 2 DSGVO)
- ☐ Bei Löschung: Empfänger (Dienstleister, Partner) über Löschung informiert
- ☐ Bei Berichtigung: Empfänger über Korrektur informiert
- ☐ Bei Einschränkung: Betroffenen informiert + vor Aufhebung erneut informieren

Häufige Fehler vermeiden

- ☐ Fristüberschreitung (häufigster Fehler) → Bußgeld bis 20 Mio. € oder 4% Jahresumsatz
- ☐ Unvollständige Auskunft (vergessene Systeme, Backup, E-Mail-Archiv)
- ☐ Fehlende Identitätsprüfung → Daten an falsche Person → Datenpanne nach Art. 33 DSGVO
- ☐ Unverschlüsselte Übermittlung sensibler Daten (Art. 9 DSGVO)
- ☐ Keine Dokumentation → Rechenschaftspflicht nicht erfüllt (Art. 5 Abs. 2 DSGVO)
- ☐ Anfrage ignorieren → Beschwerde bei Aufsichtsbehörde garantiert

Kritische Fristen:

- ✓ Antwortfrist: 1 Monat ab Eingang (Verlängerung auf 3 Monate mit Begründung möglich)
- ✓ Informationszusammenstellung: max. 3 Wochen (1 Woche Reserve für Versand)
- ✓ Eingangsbestätigung: unverzüglich (innerhalb 48 Stunden empfohlen)

Eine professionelle Bearbeitung von Betroffenenanfragen minimiert Bußgeldrisiken und Beschwerden. Bei komplexen Anfragen empfiehlt sich die Unterstützung durch einen erfahrenen externen Datenschutzbeauftragten.