

Löschkonzept

Frist, Fristbeginn, Löschweg und Protokoll je Datenkategorie

Produktversion 2026.10.03 · Handbuch-Revision 2.1

Stand 03.10.2026 · Plattform .NET 10 / Windows Server

ID-56 Löschkonzept

Löschkonzept

Dieses Kapitel nennt für jede Kategorie personenbezogener Daten, die Ordvis IT speichert, die **Frist**, den **Fristbeginn**, den **Löschweg** und ob die Löschung **protokolliert** wird. Es richtet sich an **Datenschutzbeauftragte** und den **IT-Betrieb**. Es erfüllt die Grundsätze der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) und des Rechts auf Löschung (Art. 17 DSGVO) auf der Seite des Produkts.

Beschrieben ist der Stand der Fassung, mit der dieses Kapitel ausgeliefert wird. Die technischen und organisatorischen Maßnahmen insgesamt stehen in ID-55, die Löschung bei der Außerbetriebnahme in ID-53, Abschnitt 7.

INHALT

1 Wer die Fristen festlegt

1.1 Eine Frist ändern

2 Begriffe

3 Datenkategorien, Fristen und Löschrwege

3.1 Konten und Anmeldung

3.2 Service Desk

3.3 Benachrichtigungen

3.4 Alarmierung und Notfallmanagement

3.5 CMDB, Inventar und Netz

3.6 Weitere Module

3.7 Außerhalb der Datenbank

4 Automatische Löschläufe im Überblick

5 Löschen von Hand

5.1 Betroffenenanfrage: Auskunft, Anonymisierung, Einschränkung

5.2 Weitere Löschrwege

5.3 Daten in Sicherungen

6 Ihre Fristen dokumentieren

7 Bekannte Grenzen

8 Beispiele aus der Praxis

8.1 Beispiel: Sitzungsdaten nach 14 Tagen löschen

8.2 Beispiel: Löschantrag eines ausgeschiedenen Mitarbeiters

9 Häufige Fragen

Verwandte Themen

1 Wer die Fristen festlegt

Die Fristen legen Sie fest. Als Verantwortlicher entscheiden Sie, wie lange Sie Daten für Ihre Zwecke brauchen; Ihre Aufbewahrungsvorschriften und Ihr Archivrecht gehen vor. Ordvis IT liefert dafür je Kategorie eine **Vorgabefrist** und den Löschweg. Sie übernehmen die Vorgabe oder ändern sie.

Heute löscht das Produkt nur einen Teil selbst. Die Tabellen in Abschnitt 3 sagen je Kategorie, ob ein automatischer Löschlauf besteht. Wo keiner besteht, ist die Vorgabefrist eine **Empfehlung**, die Sie bis zum automatischen Löschlauf von Hand umsetzen (Abschnitt 5). Abschnitt 7 fasst diese Lücken zusammen.

Fristen der Fristenlöschung ändern. Die Kategorien der Fristenlöschung (in Abschnitt 3 als „einstellbar“ bezeichnet) stellen Sie je Mandant über die Schnittstelle ein, mit dem Recht `privacy.manage`. Eine Seite in Client und Portal gibt es dafür noch nicht.

Kategorie (Schlüssel)	Bezeichnung	Vorgabe	Fristbeginn
<code>Sitzungen</code>	Sitzungen und Erneuerungstoken	30 Tage	Ablauf oder Beenden
<code>Anmeldeanfragen</code>	Anmeldeanfragen (Anmeldung per App)	30 Tage	Ablauf
<code>KennwortZuruecksetzen</code>	Kennwort-Zurücksetzen	30 Tage	Ablauf oder Einlösung
<code>MailWarteschlange</code>	Mail-Warteschlange	30 Tage	Versand; bei endgültig gescheiterten Mails die Anlage
<code>PushWarteschlange</code>	Push-Warteschlange	7 Tage	Zustellung oder endgültiges Scheitern
<code>MessengerWarteschlange</code>	Messenger-Warteschlange	30 Tage	Versand; bei endgültig gescheiterten Nachrichten die Anlage
<code>BcmOfflineKits</code>	BCM-Offline-Notfall-Kits	7 Tage	Erzeugung; das jüngste Kit bleibt immer

1.1 Eine Frist ändern

Über die Schnittstelle: GET und PUT /api/v1/datenschutz/loeschfristen mit PowerShell 7 · privacy.manage — Client und Portal bieten dafür noch keine Seite.



Klickweg – Eine Frist ändern

- Öffnen Sie PowerShell 7 und melden Sie sich mit einem Konto an, das `privacy.manage` trägt (ID-60, Beispiel 7.1).
- Lesen Sie die geltenden Fristen: `powershell Invoke-RestMethod -Uri "$base/api/v1/datenschutz/loeschfristen" -Headers $kopf`
- Setzen Sie die neue Frist für eine Kategorie (1 bis 3650 Tage): `powershell Invoke-RestMethod -Method Put -Uri "$base/api/v1/datenschutz/loeschfristen/Sitzungen" -Headers $kopf -ContentType "application/json; charset=utf-8" -Body '{ "tage": 14 }'`

✓ **Ergebnis:** Die Antwort nennt `vorgabeTage`, die geltenden `tage` und `abweichend = true`. Die Änderung steht mit altem und neuem Wert im Prüfprotokoll; der nächste Löschlauf (03:25 UTC) wendet sie an. Tragen Sie wieder die Vorgabe ein, folgt die Kategorie danach auch jeder künftigen Vorgabe.

2 Begriffe

Begriff	Bedeutung
Frist	Wie lange ein Datensatz nach dem Fristbeginn höchstens bleibt
Fristbeginn	Das Ereignis, ab dem die Frist läuft, etwa das Schließen eines Vorgangs
Löschen	Der Datensatz wird aus der Datenbank entfernt
Anonymisieren	Die personenbezogenen Felder werden überschrieben; der Datensatz bleibt für Zählungen und Verweise stehen
automatisch	Ein geplanter Lauf des Servers löscht ohne Zutun
von Hand	Jemand mit dem genannten Recht löscht in der Oberfläche
keine Vorgabe	Nachweis- oder Archivdaten, deren Frist allein Ihr Recht bestimmt

3 Datenkategorien, Fristen und Löschwege

3.1 Konten und Anmeldung

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Benutzerkonten	Anmeldename, Name, Mailadresse, Telefon, Abteilung, Funktion, Verzeichnisattribute, letzte Anmeldung	6 Monate, dann anonymisieren	Deaktivierung	von Hand: Anonymisierung (Abschnitt 5.1). Ein Konto lässt sich deaktivieren, aber nicht löschen
Sitzungen und Erneuerungstoken	IP-Adresse, Browserkennung, Gerät	30 Tage	Ablauf oder Beenden	automatisch (Fristenlöschung), einstellbar (Abschnitt 1)
Anmeldeanfragen (Anmeldung per App)	IP-Adresse, Browserkennung, antwortendes Gerät	30 Tage	Ablauf	automatisch (Fristenlöschung), einstellbar (Abschnitt 1)
Kennwort-Zurücksetzen	Kontobezug (Token nur als Hashwert)	30 Tage	Ablauf oder Einlösung	automatisch (Fristenlöschung), einstellbar (Abschnitt 1)

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Zweiter Faktor	Gerätename, verschlüsseltes Geheimnis	mit dem Konto	Neueinrichtung oder Anonymisierung	von Hand: MFA zurücksetzen löscht sofort
Mobilgeräte der App	Gerätename, Push-Kennung, öffentlicher Schlüssel, zuletzt gesehen	90 Tage	Abmelden des Geräts	Abmelden entfernt die Push-Kennung; der Eintrag bleibt
Integrations-Token	Name, ausstellende Person, zuletzt benutzt (Token nur als Hashwert)	90 Tage	Widerruf oder Ablauf	Widerruf entfernt den Eintrag sofort; abgelaufene werden beim Ausstellen eines neuen entfernt
Anzeigegeräte (Wallboard), Kalender-Abonnements	Name, gebundenes Konto, zuletzt benutzt (Token nur als Hashwert)	90 Tage	Widerruf oder Ablauf	keiner
Zugriffsüberprüfungen	Person, Rolle, Entscheidung, Begründung, Prüfer	3 Jahre	Abschluss des Durchlaufs	keiner
Vertretungen	Vertretene und vertretende Person, Notiz	1 Jahr	Ende der Vertretung	keiner

3.2 Service Desk

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Vorgänge mit Verlauf, Kommentaren, Mails und Anhängen	Melder, Bearbeiter, Entscheider, Mailadressen, Freitext, Originalmail mit Kopfzeilen	3 Jahre	Schließen des Vorgangs	keiner. Einzelne Anhänge von Hand löschar; Vorgänge selbst nicht
Termine zu Vorgängen	Teilnehmer, Mailadresse, Ort	mit dem Vorgang	Schließen des Vorgangs	keiner
Arbeitszeitbuchungen	bearbeitende Person, Dauer, Notiz	mit dem Vorgang	Schließen des Vorgangs	keiner
Zufriedenheitsbewertungen	Sterne, Kommentar	mit dem Vorgang	Schließen des Vorgangs	keiner
Telefonnotizen	Rufnummer, Notiz	mit dem Vorgang	Schließen des Vorgangs	keiner
Probleme und Änderungen	Melder, Bearbeiter, Genehmiger, Freitext	3 Jahre	Abschluss	Probleme von Hand (<code>tickets.delete</code>); Änderungen keiner
Kontakte	Mailadresse, Name, Telefon, Organisation, Notiz	3 Jahre	letzter Vorgang des Kontakts	von Hand: Löschen (<code>contacts.manage</code>) oder Anonymisierung
Aufrufe und Suchen in der Wissensdatenbank	Person, Artikel bzw. Suchbegriff	90 Tage	Aufruf bzw. Suche	keiner; beim Löschen eines Artikels fallen seine Aufrufe mit
Rohereignisse des Monitorings	Hostname, Meldungstext	30 Tage	Eingang	automatisch , täglich 03:15 UTC; Ereignisse offener Störungen bleiben. Nicht einstellbar

3.3 Benachrichtigungen

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Benachrichtigungen (Glocke)	Empfänger, Betreff, Text	90 Tage	Lesen	von Hand durch den Empfänger selbst
Mail-Warteschlange	Empfänger, Antwortadresse, Betreff, Inhalt, Anhänge (auch Support-Pakete und Fehlerberichte auf dem Rückfallweg)	30 Tage	Versand; bei endgültig gescheiterten Mails die Anlage	automatisch (Fristenlöschung), einstellbar (Abschnitt 1); wartende Mails nie

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Push-Warteschlange	Empfänger, Zustelltoken, Titel, Text	7 Tage	Zustellung oder endgültiges Scheitern	automatisch (Fristenlöschung), einstellbar (Abschnitt 1); wartende Nachrichten nie
Messenger-Warteschlange	Empfänger, Text	30 Tage	Versand; bei endgültig gescheiterten Nachrichten die Anlage	automatisch (Fristenlöschung), einstellbar (Abschnitt 1); wartende Nachrichten nie
Eingehende Mails im Postfach	vollständige Mail	—	Übernahme in einen Vorgang	automatisch: Über IMAP wird die verarbeitete Mail im Postfach gelöscht, sofern kein Ordner für verarbeitete Mails eingestellt ist (dann wird sie dorthin verschoben). Über POP3 nur, wenn <i>Nachrichten nach Abruf löschen</i> eingeschaltet ist. Nicht verarbeitbare Mails gehen in den Fehlerordner

3.4 Alarmierung und Notfallmanagement

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Alarmprotokolle mit Empfängern, Zustellungen und Quittungen	Auslöser, Empfänger, Ergebnis, Quittung, Notiz	3 Jahre (mindestens 90 Tage)	Schließen des Alarms	automatisch , täglich 03:20 UTC, je Mandant. Offene Alarme nie – und echte Alarme lassen sich in dieser Fassung nicht schließen; die Frist greift deshalb nur für stille Tests (ID-29). Frist nur über die Schnittstelle änderbar (<code>PUT /api/v1/alerting/retention</code> , <code>bcm.plan.manage</code>)
Widerrufene Einwilligungen	Person, Weg, Erteilung, Widerruf	3 Jahre	Widerruf	automatisch mit den Alarmprotokollen. Geltende Einwilligungen bleiben
Bereitschaftsdienste	Person, Vertretung, Übergabenotiz	1 Jahr	Ende des Dienstes	von Hand (<code>bcm.crisis.operate</code>)
Alarmierungskontakte, Stabsbesetzung	Name, Mailadresse, Telefon, Notfallrufnummer	solange die Funktion besteht	Ende der Funktion	von Hand (<code>bcm.plan.manage</code> , <code>bcm.org.manage</code>)
Krisenstab: Einsatztagebuch, Lagemeldungen (mit Ortsangabe), Personenzählung, Maßnahmen	Verfasser, Freitext, Koordinaten	keine Vorgabe	Ende des Ereignisses	Lagemeldungen von Hand (<code>bcm.crisis.operate</code>); sonst keiner
Checklisten-Durchführungen	durchführende Person, Unterschrift, Notiz	3 Jahre	Abschluss	keiner
BCM-Offline-Notfall-Kits	Namen, Mailadressen, Rufnummern der Alarmierungslisten	7 Tage	Erzeugung	automatisch (Fristenlöschung), einstellbar (Abschnitt 1); das jüngste Kit bleibt immer , auch wenn es älter ist. Kopien außerhalb des Servers (ID-29, Abschnitt 6.1) löschen Sie selbst

3.5 CMDB, Inventar und Netz

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Benutzerkonten als CI	Spiegel des Kontos: Anmeldeame, Name, Mailadresse, Telefon, Abteilung, Verzeichnisattribute	mit dem Konto	Anonymisierung oder Löschung des Kontos	Der Spiegel folgt dem Konto alle 30 Minuten, archivierte CIs nicht. Von Hand löschen (<code>cmdb.ci.delete</code>); ein gelöscht Konto-CI kommt nicht wieder, solange das Konto deaktiviert bleibt (ID-21b)
CI-Stände (Baselines)	Kopie der CIs samt Kontoattributen	3 Jahre	Anlage des Stands	keiner

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Gerätezuordnungen und Aussonderungen	empfangende Person, Übergabe- und Rückgabennotiz	3 Jahre	Rückgabe bzw. Aussonderung	keiner
Inventurläufe	Durchführende, scannende Person	3 Jahre	Abschluss	keiner
Organisation und Geschäftsverteilung	Funktionsinhaber, Vertretung, ausgegebene Organigramme	solange gültig, danach 3 Jahre	Ende der Gültigkeit	Zuordnungen von Hand (<code>gvp.manage</code>)
IP-Adressen, DHCP-Reservierungen, Erkennung	Hostname, MAC-Adresse, gegebenenfalls Anmeldename aus Action1	1 Jahr	zuletzt gesehen	keiner
Infrastrukturdokumentation (AD-Stände)	Benutzer, Gruppenmitgliedschaften, Rechte	3 Jahre	Abschluss des Stands	keiner

3.6 Weitere Module

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Prüfprotokoll	handelnde Person, IP-Adresse, Gerät, alte und neue Werte	3 Jahre	Eintrag	keiner; auch bei einer Anonymisierung nicht
Datenschutz: Verzeichnis, Freigaben, Folgenabschätzungen, Datenpannen	Verantwortliche, Entscheider, Unterschrift, Beschreibung	keine Vorgabe (Nachweispflicht)	—	Verfahren von Hand (<code>datenschutz.vvt.edit</code>)
Informationssicherheit: Risiken, Befunde, Schulungen, Dokumente	Verantwortliche, Freigebende, Schulungsteilnahme	keine Vorgabe (Nachweispflicht)	—	keiner
Selbstorganisation: persönliche Aufgaben, Übergaben	Eigentümer, Titel, Notiz	1 Jahr	Erledigung	von Hand durch den Eigentümer
Workflows	startende Person, Bearbeiter, Notiz	3 Jahre	Abschluss	keiner
Verträge und Lieferanten	interne Verantwortliche, Ansprechpartner	keine Vorgabe (Vertragsrecht)	Vertragsende	keiner
Lizenzzuordnungen	Person	1 Jahr	Rücknahme	keiner
Berichte: Zeitpläne und erzeugte Berichte	Empfängeradressen, erzeugende Person	1 Jahr	Erzeugung	keiner
Datensicherungs-Modul: Laufdaten	Prüfende, Notizen, Nachweise	180 Tage verdichten, 7 Jahre löschen	Lauf	automatisch , täglich 03:15 UTC; einstellbar in den Einstellungen des Moduls (<code>backup.manage</code>), Änderung im Prüfprotokoll
Datensicherungs-Modul: Meldungs-Postfach	Absender, Betreff, Auszug	90 Tage	Eingang, nur erledigte	automatisch mit den Laufdaten; nur wenn die Löschung der Tageswerte eingeschaltet ist

3.7 Außerhalb der Datenbank

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Datenbanksicherungen	alles oben Genannte	30 Tage	Erstellung	automatisch mit jeder Sicherung; einstellbar unter <i>Einstellungen</i> ▶ <i>Backup</i> (0 bis 3650 Tage, 0 = nie), jede Löschung steht im Sicherungsprotokoll

Kategorie	Personenbezogene Daten	Vorgabefrist	Fristbeginn	Löschweg heute
Betriebsprotokolle	maskierte Mailadressen, IP-Adressen, Benutzernamen	31 Dateien je Gruppe	Rotation	automatisch beim Rotieren; einstellbar unter <i>Einstellungen</i> ▶ <i>Protokolle (Logs)</i> (1 bis 3650 Dateien, <code>platform.hosting.manage</code>). Es zählt die Anzahl der Dateien, nicht Tage
Protokolle der Skripte	Benutzernamen, Pfade	Sicherung 30 Tage (höchstens 60 Dateien), Wiederherstellung 90 Tage (höchstens 30), Aktualisierung 30 Tage (höchstens 20)	Erstellung	automatisch , täglich 03:15 UTC. Nicht einstellbar
Aktualisierungsprotokolle unter <code>%ProgramData%\InfraDesk\update-logs</code>	Benutzernamen, Pfade	30 Tage , höchstens 20 Stände	Erstellung	automatisch mit den Protokollen der Skripte. Nicht einstellbar
Export eines gelöschten Mandanten	vollständige Datenbank des Mandanten	30 Tage	Löschung des Mandanten	keiner — bewusst nicht in der Sicherung. Von Hand unter <code>%ProgramData%\InfraDesk\TenantExports</code> löschen
Support-Paket	Protokolle, Systemangaben	—	Herunterladen	nach Versand oder Herunterladen gelöscht; ein nie heruntergeladenes Paket bleibt im Temp-Ordner des Servers
Windows-Ereignisprotokoll	Benutzernamen	nach Ihrer Windows-Einstellung	—	Windows überschreibt nach Größe

Beim Hersteller: Der Push-Vermittler speichert Gerätetoken nur als Hashwert. Seine Aufräumregel entfernt Token-Bindungen nach **180 Tagen** ohne Nutzung und sein Zugriffsprotokoll nach **90 Tagen**. Fehlerberichte gehen an den Support und werden dort als Vorgang geführt.

4 Automatische Löschläufe im Überblick

Lauf	Zeit	Umfang	Protokoll
<i>Alarmprotokolle nach Aufbewahrungsfrist entfernen</i>	täglich 03:20 UTC, je Mandant	Abschnitt 3.4	Betriebsprotokoll: Anzahl
<i>Datensicherung: Aufbewahrung der Laufdaten</i>	täglich 03:15 UTC, je Mandant	Abschnitt 3.6	Betriebsprotokoll: Anzahl
<i>Monitoring-Rohereignisse kürzen</i>	täglich 03:15 UTC, je Mandant	Abschnitt 3.2	Betriebsprotokoll
<i>Protokolle aufräumen</i>	täglich 03:15 UTC, einmal für den Server	Abschnitt 3.7	Betriebsprotokoll: Anzahl der Dateien
<i>Fristenlöschung nach dem Löschkonzept</i>	täglich 03:25 UTC, je Mandant	die als „einstellbar“ bezeichneten Kategorien in Abschnitt 3	Betriebsprotokoll: Anzahl je Kategorie
Windows-Aufgabe <code>InfraDesk-DailyBackup</code>	nach Ihrem Zeitplan	Abschnitt 3.7	Sicherungsprotokoll

Abbildung 1 zeigt, was die Fristenlöschung je Eintrag entscheidet.

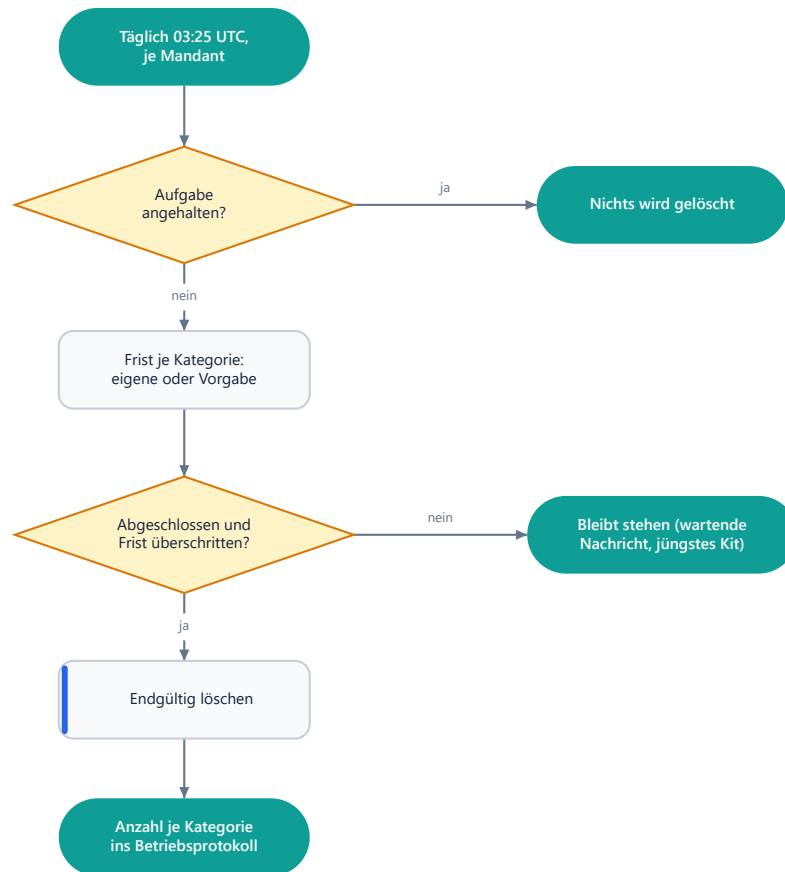


Abb. 1 – Die Fristenlöschung. Gelöscht wird nur Abgeschlossenes, dessen Frist abgelaufen ist; eine angehaltene Aufgabe löscht nichts.

Die Läufe erscheinen unter *Einstellungen* ► *Geplante Aufgaben* und lassen sich dort anhalten (ID-40, Abschnitt 5). Ein **angehaltener Löschlauf löscht nicht mehr** – prüfen Sie deshalb bei der jährlichen Kontrolle, dass alle Läufe aktiv sind. Protokolliert wird, **wie viele** Datensätze ein Lauf gelöscht hat, nicht welche; ihr Inhalt steht damit in keinem Protokoll.

5 Löschen von Hand

5.1 Betroffenenanfrage: Auskunft, Anonymisierung, Einschränkung

Mit dem Recht `privacy.manage` geben Sie über Konto, Anmeldename, Name oder Mailadresse einer Person aus, welche Daten sie in allen Bereichen betreffen (ID-40, Abschnitt 19), und anonymisieren sie danach über dieselbe Suche – erst, wenn die Auskunft zu genau dieser Person vorliegt (höchstens 24 Stunden alt, erstellt von Ihnen). Abbildung 2 zeigt den Ablauf.

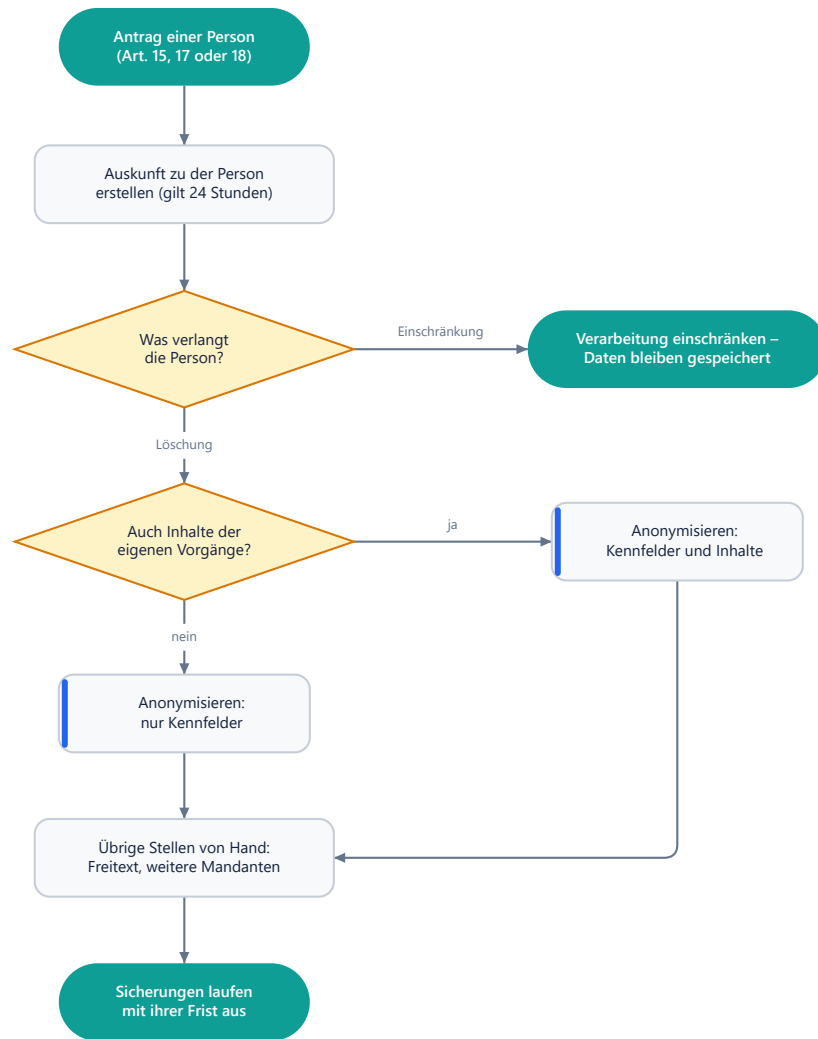
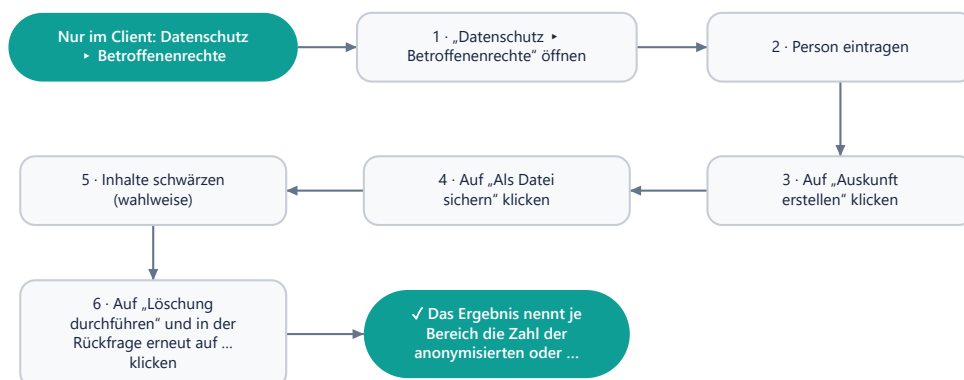


Abb. 2 – Eine Betroffenenanfrage bearbeiten. Ohne Auskunft nimmt der Server keine Anonymisierung an.

Nur im Client: Datenschutz ▶ Betroffenenrechte · [privacy.manage](#) — Das Portal bietet die Betroffenenrechte nicht an.

Pflichtreihenfolge — erst die Auskunft, dann die Anonymisierung; sie lässt sich nicht zurücknehmen.



Klickweg – Betroffenenanfrage: Auskunft, Anonymisierung, Einschränkung

1. Öffnen Sie *Datenschutz ▶ Betroffenenrechte*.
2. Tragen Sie in das Suchfeld (*Konto, Anmeldename, Name oder E-Mail-Adresse der betroffenen Person*) die Angabe zur Person ein.
3. Klicken Sie auf *Auskunft erstellen*.

4. Klicken Sie auf *Als Datei sichern* und verwahren Sie die Auskunft als Nachweis.
5. Aktivieren Sie bei Bedarf *Auch Betreff, Beschreibung, Verlauf und Anhänge der selbst gemeldeten Vorgänge schwärzen*.
6. Klicken Sie auf *Löschung durchführen* und in der Rückfrage erneut auf *Löschung durchführen*.

✓ **Ergebnis:** Das Ergebnis nennt je Bereich die Zahl der anonymisierten oder entfernten Einträge und die Frist, bis zu der die Person noch in Sicherungen steht. Die Anonymisierung steht im Prüfprotokoll, mit Zahlen und ohne Mailadresse.

Was die Anonymisierung erfasst. Im angemeldeten Mandanten überschreibt sie Anmeldename, Name, Mailadresse, Telefon, Abteilung, Verzeichnisattribute und Kennwort und deaktiviert das Konto; Systemkonten sind ausgenommen. Sie anonymisiert die mandantenübergreifende Kopie des Kontos (zentrale Anmeldung), entfernt Sitzungen, zweite Faktoren, Mobilgeräte und Beobachtungen, anonymisiert Kontakte, Melderadresse und Entscheidung in Vorgängen, Termine, Alarmempfang, Konto-CIs und Geräteübergaben und entfernt Benachrichtigungen sowie Mails und Push-Nachrichten der Warteschlangen an die Person. Inhalte der selbst gemeldeten Vorgänge – Betreff, Beschreibung, Verlauf – werden nur auf die Wahl in Schritt 5 geschwärzt; ihre Anhänge werden dann storniert und ihr Inhalt entfernt.

⚠ **Nicht erfasst** werden: das Prüfprotokoll, Stellen, an denen die Person nur im Freitext vorkommt, die Messenger-Warteschlange, Alarmierungskontakte mit von Hand eingetragenen Namen ohne Konto und Adresse, Daten in **anderen Mandanten** (dort wiederholen Sie die Anfrage nach einem Mandantenwechsel), die Betriebsprotokolle und die Datensicherungen bis zum Ablauf ihrer Aufbewahrung. Diese Stellen bearbeiten Sie von Hand, soweit Sie dazu verpflichtet sind.

Statt zu löschen, lässt sich die Verarbeitung nach Art. 18 **einschränken** (Karte *Verarbeitung einschränken* auf derselben Seite), etwa solange die Richtigkeit bestritten ist oder die Person die Daten für einen Rechtsanspruch braucht. Die Daten bleiben dann gespeichert. Die Person kann sich nicht anmelden und wird weder alarmiert noch benachrichtigt. Ihre Vorgänge und Kontakte sind nur noch lesbar. Die Einzelheiten und was die Einschränkung nicht erfasst, stehen in ID-40, Abschnitt 19. Die Löschläufe aus Abschnitt 4 löschen auch bei einer eingeschränkten Person, was seine Frist erreicht hat. Vorgänge, Kontakte und Konten löschen sie heute nicht.

5.2 Weitere Löswege

Was	Wo	Recht	Wirkung
Kontakt	Kontaktverwaltung	<code>contacts.manage</code>	endgültig gelöscht
Anhang	am Vorgang oder Objekt	Recht am Objekt	endgültig gelöscht; Anhänge, die als Nachweis dienen, werden ungültig gestellt statt gelöscht
CI, auch Konto-CI	CMDB	<code>cmdb.ci.delete</code>	endgültig gelöscht, im Prüfprotokoll
Problem	Problem-Management	<code>tickets.delete</code>	endgültig gelöscht
Benutzerkonto	Benutzerverwaltung	<code>identity.users.manage</code>	nur deaktivieren; löschen geht nicht, anonymisieren über 5.1
Sitzung	Benutzerverwaltung	<code>identity.sessions.manage</code>	beendet; der Eintrag fällt mit der Fristenlöschung weg
Zweiter Faktor	Benutzerverwaltung	<code>identity.users.manage</code>	MFA zurücksetzen löscht ihn sofort
Integrations-Token	<i>Einstellungen</i> ▶ <i>Integrations-Token</i>	<code>platform.integrationtoken.manage</code>	widerrufen und entfernt, im Prüfprotokoll
Eigene Benachrichtigungen	Glocke	eigenes Konto	einzelnen oder alle gelesen
Mandant	<i>Einstellungen</i> ▶ <i>Mandanten</i>	<code>tenant.manage</code>	erst archivieren, dann löschen; vorher eine Sicherung des Mandanten als Export, dann die Datenbank entfernt. Die zentralen Anmeldekonto bleiben

Netzdaten beim Löschen eines Mandanten. Alles aus *Netz* liegt in der Datenbank des Mandanten: Netze, Adressen, VLANs, SSIDs, DHCP- und DNS-Bestand, Prüfläufe, die Anschlüsse in der CMDB und die Zugangsdaten für den DHCP-Abruf im Tresor. Es geht mit dem Export und verschwindet mit der Datenbank. **Außerhalb** der Mandanten-Datenbank bleibt nur, was allen Mandanten des Servers gemeinsam gehört:

Was	Wo	Beim Löschen eines Mandanten
Tresorschlüssel	<code>%ProgramData%\InfraDesk\secret.key</code> oder <code>CredentialVault:EncryptionKey</code>	bleibt – er gilt für alle Mandanten. Die Zugangsdaten im Export sind damit verschlüsselt und nur auf diesem Server (oder mit diesem Schlüssel) lesbar
Export des Mandanten	<code>%ProgramData%\InfraDesk\TenantExports</code>	bleibt, bis Sie ihn löschen (Frist in Abschnitt 3.7)

Mandanteneigene Netzdaten außerhalb der Datenbank – etwa hochgeladene Zonendateien oder abgelegte Zugangsdaten – gibt es nicht: Zonendateien werden beim Einlesen gelesen und nicht abgelegt.

5.3 Daten in Sicherungen

Eine Löschung in der Datenbank erreicht vorhandene Sicherungen nicht. Die Daten verschwinden dort mit dem Ablauf der Sicherungsaufbewahrung (Vorgabe 30 Tage). Nach dem Zurückspielen einer Sicherung sind die Löschungen und Anonymisierungen zu wiederholen, die seit ihrer Erstellung erfolgt sind – führen Sie dafür eine Liste der Anonymisierungen (das Prüfprotokoll nennt sie mit Zeitpunkt, aber ohne Person).

6 Ihre Fristen dokumentieren

Im Modul Datenschutz hinterlegen Sie je Verarbeitungstätigkeit Löschfristen mit Rechtsgrundlage (ID-32). Sie erscheinen im Export des Verzeichnisses. **Diese Fristen steuern keinen Löschlauf** — sie dokumentieren Ihre Festlegung. Die Tabellen aus Abschnitt 3 dienen als Grundlage; Ihre eigenen Fristen kommen hinzu.

7 Bekannte Grenzen

Offen gesagt, damit Sie sie in Ihrer Planung berücksichtigen können:

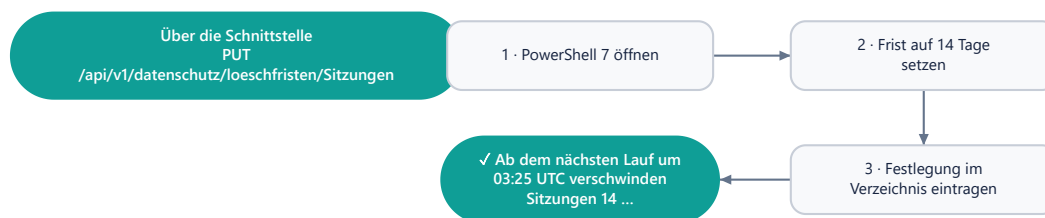
- **Viele Kategorien haben noch keinen Löschlauf.** Das betrifft Vorgänge, Kontakte, deaktivierte Konten, Benachrichtigungen, das Prüfprotokoll, die Aufrufprotokolle der Wissensdatenbank und Mandanten-Exporte. Sie folgen, sobald die Vorgabefristen abgestimmt sind; bis dahin setzen Sie sie von Hand um.
- **Fristen sind nur über die Schnittstelle einstellbar**, noch nicht in Client oder Portal. Die Frist der Monitoring-Rohereignisse und der Skriptprotokolle lässt sich gar nicht ändern.
- **Deaktivierte Konten tragen kein Deaktivierungsdatum.** Den Fristbeginn „Deaktivierung“ entnehmen Sie bis auf Weiteres dem Windows-Ereignisprotokoll (Ereignis 2004 „Benutzerkonto deaktiviert“).
- **Die Anonymisierung** erfasst keine Freitexte, keine Messenger-Warteschlange, keine anderen Mandanten, keine Betriebsprotokolle und keine Datensicherungen (Abschnitt 5.1).
- **Das Anhalten eines Löschlaufs** steht nicht im Prüfprotokoll.

8 Beispiele aus der Praxis

8.1 Beispiel: Sitzungsdaten nach 14 Tagen löschen

Ausgangslage: Die Datenschutzbeauftragte der Gemeinde Musterstadt legt fest, dass IP-Adressen aus Anmeldesitzungen nach 14 statt 30 Tagen gelöscht werden.

Über die Schnittstelle: PUT /api/v1/datenschutz/loeschfristen/Sitzungen ·  privacy.manage



Klickweg – Beispiel: Sitzungsdaten nach 14 Tagen löschen

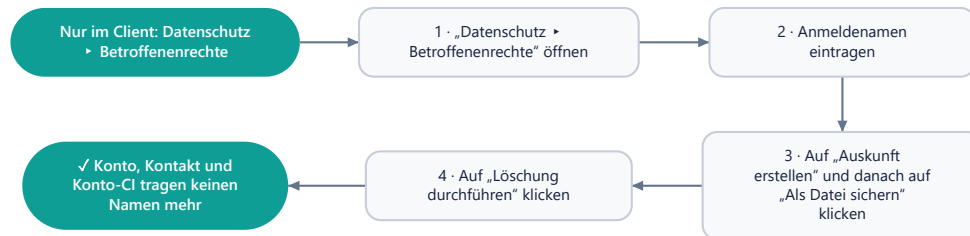
1. Öffnen Sie PowerShell 7 und melden Sie sich an (ID-60, Beispiel 7.1).
2. Setzen Sie die Frist mit dem Rumpf `{ "tage": 14 }` (Abschnitt 1.1, Schritt 3).
3. Tragen Sie die Festlegung beim Verfahren *Benutzer- und Zugriffsverwaltung* im Verzeichnis ein (ID-32).

✓ **Ergebnis:** Ab dem nächsten Lauf um 03:25 UTC verschwinden Sitzungen 14 Tage nach Ablauf oder Ende. Das Prüfprotokoll zeigt „Löschfrist „Sitzungen und Erneuerungstoken“ geändert: 30 → 14 Tage.“

8.2 Beispiel: Löschantrag eines ausgeschiedenen Mitarbeiters

Ausgangslage: Max Mustermann hat die Stadtverwaltung Musterstadt verlassen und verlangt die Löschung seiner Daten. Sein Konto `max.mustermann` ist seit einem halben Jahr deaktiviert. Seine gemeldeten Vorgänge sollen als Nachweis lesbar bleiben.

 **Nur im Client:** *Datenschutz* ▶ *Betroffenenrechte* ·  `privacy.manage` — Das Portal bietet die Betroffenenrechte nicht an.



Klickweg – Beispiel: Löschantrag eines ausgeschiedenen Mitarbeiters

1. Öffnen Sie *Datenschutz* ▶ *Betroffenenrechte*.
2. Tragen Sie `max.mustermann` in das Suchfeld ein.
3. Klicken Sie auf *Auskunft erstellen* und danach auf *Als Datei sichern*.
4. Klicken Sie auf *Löschung durchführen*, ohne die Inhalte schwärzen zu lassen, und bestätigen Sie die Rückfrage.

✓ **Ergebnis:** Konto, Kontakt und Konto-Cl tragen keinen Namen mehr; die Vorgänge bleiben mit ihrem Inhalt stehen, der Melder ist nicht mehr erkennbar. Freitext, in dem Herr Mustermann namentlich genannt ist, und weitere Mandanten prüfen Sie von Hand.

9 Häufige Fragen

Löscht Ordvis IT alte Vorgänge von selbst? Nein. Vorgänge, Kontakte und Konten haben noch keinen Löschlauf (Abschnitt 7). Die Vorgabefrist von 3 Jahren ist eine Empfehlung.

Warum lässt sich ein Benutzerkonto nicht löschen? Vorgänge, Prüfprotokoll und Nachweise verweisen darauf. Statt zu löschen, wird das Konto anonymisiert (Abschnitt 5.1).

Kann ich eine Anonymisierung rückgängig machen? Nein. Deshalb verlangt der Server vorher die Auskunft. Nur das Zurückspielen einer Sicherung stellt den alten Stand her – samt allen späteren Änderungen anderer Daten.

Warum steht die Person noch im Prüfprotokoll? Das Prüfprotokoll ist Nachweis und bleibt bewusst unverändert (Abschnitt 3.6).

Wo sehe ich, was ein Löschlauf gelöscht hat? Im Betriebsprotokoll des Servers steht die Anzahl je Kategorie, nicht welche Einträge (Abschnitt 4).

Kann ich eine Frist kürzer als einen Tag setzen? Nein, die Fristenlöschung nimmt 1 bis 3650 Tage an.

Wer darf die Fristen ändern? Wer `privacy.manage` trägt; die Frist der Alarmprotokolle ändert, wer `bcm.plan.manage` trägt.

Was passiert mit Daten in den Sicherungen? Sie verschwinden erst mit dem Ablauf der Sicherung (Abschnitt 5.3).

Die Anonymisierung meldet „Erst die Auskunft zu dieser Person erstellen — die Anonymisierung lässt sich nicht zurücknehmen. Die Auskunft gilt 24 Stunden.“ Die Auskunft fehlt, ist älter als 24 Stunden, wurde von jemand anderem erstellt oder der Server wurde seither neu gestartet. Erstellen Sie die Auskunft erneut.

Verwandte Themen

- ID-55 – Technische und organisatorische Maßnahmen
- ID-57 – Verarbeitungstätigkeiten (VVT-Beitrag)
- ID-32 – Datenschutz (Verarbeitungsverzeichnis)
- ID-40 – Administrationshandbuch: Betroffenenrechte (Abschnitt 19)
- ID-53 – Produktsicherheit: sichere Außerbetriebnahme und Datenlöschung
- ID-50 – Betriebshandbuch: Sicherung und Protokolle
- ID-60 – API-Referenz

- ID-29 – BCM (Offline-Notfall-Kit)
- ID-32a – Anlage Alarmierung und Mitbestimmung