
Filum und der Datenschutz: wer was verantwortet

Rollen, Datenwege, Auskunft und Löschung. Ein Blatt für die Person, die im Büro den Datenschutz verantwortet.

Stand 26.09.2026. Grundlage sind die Primärtexte (DSG und DSV in der Fassung seit 1.9.2023, OR, ArG und ArGV 3, ZPO), die Praxis des EDÖB und der Code von Filum, wie er heute im Baum steht. Keine Rechtsberatung. Wo eine Frage einen Entscheid verlangt, steht das ausdrücklich dabei.

1. Die Rollen, bevor irgendetwas anderes besprochen wird

Die meisten Missverständnisse beim Thema Mailarchiv entstehen daraus, dass die Rollen nicht auseinandergehalten werden. Bei Filum sind sie ungewöhnlich klar, weil kein Dienst dazwischensteht.

Wer	Rolle	Woran das liegt
Das Büro	Verantwortlicher für das Archiv	Es entscheidet über Zweck und Mittel, und die Daten liegen auf seinem Träger
bimover, Kernprodukt	weder Auftragsbearbeiter noch Verantwortlicher	Die Inhalte kommen nie an bimover. Die bloße Möglichkeit der Kenntnisnahme ist nach Schweizer Lehre keine Bearbeitung
bimover, Lizenzdaten	eigenständiger Verantwortlicher	bimover bearbeitet sie für den eigenen Zweck, nämlich Lizenz und Rechnung, nicht im Auftrag des Büros
bimover, Support im Einzelfall	Auftragsbearbeiter, sobald Kundendaten für den Kunden bearbeitet werden	Etwa beim Wiederherstellen eines Archivs oder beim Durchsehen eines Protokolls mit Inhalten

Daraus folgt für den Vertrag zwischen Büro und bimover: Für das Kernprodukt braucht es keinen Auftragsbearbeitungsvertrag, aber eine Geheimhaltungsklausel mit Verwendungsverbot für alles, was bimover bei einem Support-Zugriff wahrnehmen kann. Für den Support-Teil braucht es die Punkte nach Art. 9 DSG und Art. 7 DSV. Die Lizenzdatenübermittlung gehört beschrieben: welche Felder, wozu, wie lange, wohin.

2. Was das Gerät verlässt

Die Frage, die alles entscheidet, lautet nicht «was liest die Software?», sondern «was verlässt das Gerät Richtung bimover oder einen Dritten?».

Empfänger	Was hingeht	Wann
Microsoft	die Abfragen des eigenen Postfachs und der freigegebenen, mit dem Token der angemeldeten Person	beim Archivieren, beim Einsammeln, im Hintergrund
Das NAS des Büros	die Nachrichten, die Anhänge, die Belege, die öffentlichen Schlüssel der Absenderdomänen	bei jedem Lauf
bimover.ch, Anmeldung	aus dem Anmeldetoken von Microsoft Name, Mailadresse und Kennung der Person und die Kennung ihrer Organisation; eine Geräteerkennung und der Name des Rechners	beim Verbinden des Kontos, danach nur noch das eigene Token von bimover
bimover.ch, Lizenz	je Postfach, aus dem ein Projekt archiviert, ein SHA-256 statt der Adresse; nach dem Lauf dazu eine Kennung des Archivs, Kennung und Zeitpunkt des Laufs, die Prüfsumme des jüngsten Belegs, die Zahl der Nachrichten und der Belege	beim Einrichten, vor und nach jedem Lauf, auch im Hintergrund
bimover.ch, Support	Text der Anfrage, Name und Adresse für die Antwort, Plattform, Programmfassung, eine zurücksetzbare Installationskennung; der Diagnosebericht nur nach ausdrücklicher Freigabe	nur wenn jemand den Support anschreibt
Zeitstempeldienst	der Hash eines Belegs, sonst nichts	bei jedem Lauf, der etwas ablegt oder eine Löschung festhält, sonst beim ersten Lauf eines Tages
Namensdienst des Rechners und Namensserver der Absenderdomäne	Selektor und Domäne einer Unterschrift, um deren öffentlichen Schlüssel zu holen	beim Ablegen und im Hintergrund

Betreff, Adressen, Text und Anhänge der Korrespondenz gehen nirgends hin ausser auf den Träger des Büros. Die Domäne eines Absenders sieht der Namensdienst, den der Rechner benutzt, und der Namensserver dieser Domäne; eine Adresse oder einen Inhalt sehen sie nicht. Eine feste Liste verbotener Feldnamen in den Tests hält das für die Meldungen an bimover fest, und alles, was zu Diagnosezwecken Richtung bimover gehen kann, läuft durch eine eigene Prüfstelle im Kern. Ein Diagnosebericht geht nur mit Freigabe hinaus, und die App zeigt ihn vorher ganz. Er nennt weder Betreff noch Adressen der Korrespondenz, wohl aber die eigene Kontoadresse, Projektname und Projektnummer und vom Ablagepfad den letzten Ordner. Die Kennung des Archivs entsteht beim Anlegen und trägt weder einen Projektnamen noch eine Adresse.

Zwei Hinweise, die dazugehören. Erstens: Der SHA-256 einer Mailadresse ist pseudonym, nicht anonym, und gilt datenschutzrechtlich weiterhin als Personendatum. Das Salz ist für alle gleich, damit dasselbe Postfach in zwei Projekten eine Lizenz bleibt; wer die Adresse kennt, kann den Hash also nachrechnen. Er steht in dieser Aufstellung deshalb nicht als «anonymisiert», sondern als das, was er ist. Zweitens: Das Büro muss seine Mitarbeiter darüber informieren, dass Lizenzdaten an bimover fließen (Art. 19 Abs. 2 lit. c DSGVO, Empfängerkategorien).

3. Die Entwurfsentscheidung, die im Datenschutz am meisten trägt

In Filum wird nur archiviert, was eine Person selbst einem Projekt gibt: indem sie es in den Projektordner legt oder indem sie Regeln setzt, etwa einen Kontakt oder die Projektnummer. Passt eine Mail zu mehreren Projekten oder trifft sie eine neue Regel, legt Filum sie ihr in «Zu klären» vor, und archiviert wird erst nach ihrem Entscheid. Das klingt nach Bequemlichkeit und ist in Wahrheit der tragende Punkt. Es gilt auch im Hintergrund: Stimmt eine Person nach dem ersten Lauf zu, archiviert Filum alle zwei Stunden, was in ihren Projektordnern liegt und was ihre Regeln einem Projekt geben, und nichts sonst. Abschalten kann sie es jederzeit.

Filum ist kein Überwachungs- oder Kontrollsystem im Sinn von Art. 26 Abs. 1 ArGV 3. Die Norm verbietet Systeme, die das Verhalten der Mitarbeiter am Arbeitsplatz überwachen sollen, und stellt auf die Zweckbestimmung ab. Filum wertet keine Randdaten über Personen aus, erstellt keine Statistik über Personen, misst keine Nutzungsintensität und liest Inhalte nur, um eine Mail einem Projekt zuzuordnen: auf dem Mac der Person, nach Regeln, die nur sie selbst setzt. Ins Archiv kommt davon, was eine Regel oder die Person einem Projekt gibt; bimover erhält nichts davon. Damit ist der Tatbestand nicht erfüllt, und die Frage der Rechtfertigung stellt sich gar nicht erst.

Über den Projektordner hinaus liest Filum drei Dinge, alle nur auf dem Rechner der Person. Sammelt ein Projekt über Regeln, liest es Posteingang und gesendete Post samt dem Text praktisch jeder Mail und sucht darin Projektnummer und Projektname; ins Archiv kommt nur, was eine Regel oder die Person dem Projekt gibt, und was zu mehreren Projekten passt, sieht nur sie in «Zu klären». Beim Einsammeln, wenn sie Vorschläge will, zeigt es Betreff, Absender und Datum der neuesten Nachrichten aus Posteingang und gesendeter Post, damit sie entscheiden kann, was zum Projekt gehört. Und läuft Filum im Hintergrund, holt es die Kopfzeilen der neuesten Nachrichten im Posteingang, ohne Text und ohne Anhänge. Darin stehen auch Absender und Betreff, aber Filum wertet nur die Zeile aus, mit der eine Absenderdomäne ihre Nachricht unterschreibt, und behält vom Rest nichts. Aus dieser Zeile nimmt es Domäne und Selektor, um den öffentlichen Schlüssel zu holen, solange die Domäne ihn noch veröffentlicht. Die Schlüssel liegen in einem Vorrat auf dem Rechner; ins Archiv kommt nur, was zu einer archivierten Nachricht gehört, und was zwölf Monate niemand braucht, fällt weg. Eine Aussage über das Verhalten einer Person entsteht aus keinem davon.

Die Voreinstellung steht zugunsten der betroffenen Person (Art. 7 Abs. 3 DSGVO). Die verbreitete Praxis kehrt die Vermutung um: was nicht als privat gekennzeichnet ist, gilt als geschäftlich und damit als einsehbar. Bei Filum gilt das Umgekehrte: was die Person weder einsortiert noch mit einer Regel einem Projekt gegeben hat, wird nicht archiviert, und was sie als privat bezeichnet, in keinem Projekt.

Die Trennung privat und geschäftlich nimmt die einzige Person vor, die sie zuverlässig vornehmen kann (Verhältnismässigkeit, Art. 6 Abs. 2 DSGVO). Es gibt keinen Klassifikator des Arbeitgebers, keine Stichprobe und kein Ermessen des Arbeitgebers über fremde Post: Die Regeln setzt jede Person selbst und nur für sich.

Einsortieren und Regel sind eine Zweckzuweisung der Person (Zweckbindung, Art. 6 Abs. 3 DSGVO): Eine Nachricht wird Teil der Projekttakte, weil die Person sie einem Projekt gegeben hat: von Hand, über eine ihrer Regeln oder weil sie zu einem Gespräch gehört, das schon dort liegt.

Ebenso klar ist, wobei dieser Entwurf nicht hilft: bei der Informationspflicht nach Art. 19, bei der Löschpflicht nach Art. 6 Abs. 4 und gegen einen späteren Zugriff zu einem neuen Zweck. Wer das Archiv eines ausgeschiedenen Mitarbeiters durchsucht, um ihm etwas nachzuweisen, steht vor genau der Prüfung, die das Bundesgericht in 4A_518/2020 zu einer Persönlichkeitsverletzung führte.

4. Was das Büro selbst erledigen muss

Filum nimmt dem Büro diese Punkte nicht ab. Sie gehören zur Einführung.

Information der Mitarbeiter vor der Einführung (Art. 19 DSGVO) und **Anhörung** nach Art. 48 ArG. Das ist der am häufigsten übersehene Schritt.

Zwei Reglemente. Ein Nutzungsreglement nach Art. 321d OR sagt, ob und in welchem Umfang private Nutzung erlaubt ist, wie Privates zu kennzeichnen ist und was als Missbrauch gilt. Ein Archivierungsreglement sagt, was archiviert wird und was ausdrücklich nicht, wo es liegt, wer Zugriff hat, wie lange aufbewahrt wird, wie bei Abwesenheit und Austritt vorgegangen wird, was bei einer versehentlich archivierten Privatmail geschieht und wie ein Auskunftsbegehren abläuft.

Bearbeitungsverzeichnis (Art. 12 DSGVO). Die Ausnahme für Unternehmen unter 250 Mitarbeitern greift nicht, sobald besonders schützenswerte Daten in grossem Umfang bearbeitet werden, und die Beurteilung dieser Frage ist selbst Arbeit. In der Praxis ist ein schlankes Verzeichnis billiger als die Prüfung, ob man es weglassen darf.

Datensicherheit (Art. 8 DSGVO, Art. 1 bis 3 DSV). Hier zahlt die Einrichtung des Archivs direkt ein: ein eigenes Share, Zugriff über die persönlichen Konten, automatische Sicherungen, an die nur die NAS-Verwaltung herankommt.

Kein Zugriff auf das Postfach eines Abwesenden ohne Reglement und ohne Vier-Augen-Prinzip. Das ist Praxis des EDÖB und unabhängig von Filum.

5. Auskunft

Jede betroffene Person kann Auskunft verlangen (Art. 25 DSGVO), und die Auskunft ist in der Regel innert 30 Tagen zu erteilen (Art. 18 DSV). Ein Vorausverzicht darauf ist nichtig (Art. 25 Abs. 5 DSGVO).

Filum hilft dabei an einer konkreten Stelle: «Auskunft und Löschung» sucht über alle Projekte eines Abgelegtorens nach Adresse oder nach Kennung und zeigt die Treffer mit Fundort. Die Lesesicht macht die

Gespräche zusammen lesbar, statt eine Person durch hunderte Einzeldateien zu schicken. Ohne ein solches Werkzeug ist ein Auskunftsbegehren in einem gewachsenen Mailbestand kaum in dreissig Tagen zu bewältigen.

Die Grenze gehört mitgesagt: Ein Gespräch enthält fast immer Daten Dritter. Die ganze Konversation herauszugeben, ohne die Interessen dieser Dritten zu prüfen, ist nicht zulässig (Art. 26 Abs. 1 lit. b DSGVO). Diese Prüfung nimmt Filum niemandem ab.

6. Löschen

Hier wird am häufigsten falsch dargestellt, was gilt, auch von Anbietern.

Die Schweiz kennt kein eigenständiges Löschrecht. Art. 32 Abs. 1 DSG gibt einen Berichtigungsanspruch für unrichtige Daten. Die Löschung läuft über Art. 32 Abs. 2 lit. c als Klagebegehren und setzt eine widerrechtliche Persönlichkeitsverletzung voraus. Ein Pendant zu Art. 17 DSGVO gibt es nicht.

Die Pflicht besteht trotzdem, und zwar von sich aus. Art. 6 Abs. 4 DSGVO verlangt Vernichtung oder Anonymisierung, sobald die Daten für den Zweck nicht mehr erforderlich sind. Wer diese Pflicht verletzt, verletzt einen Grundsatz nach Art. 6, und genau das begründet die Persönlichkeitsverletzung, aus der dann doch ein Löschungsanspruch folgt. Der Kreis schliesst sich.

Wie Filum es umsetzt. Die Löschung entfernt das Original und die Lesefassung samt den Anhängen, die keine andere Nachricht braucht. Die Zeile in der Satzdatei wird geschwärzt: die beiden Kennungen bleiben, Adressen, Betreff und Texte gehen. Daneben entsteht ein Vermerk mit Zeitpunkt, Person und Grund. Absender und Betreff der Nachricht stehen danach in keinem Dateinamen und in keiner Datei mehr, die Filum zur Nachricht führt. Nur ein älteres Protokoll, das die Nachricht wegen eines Befunds beim Namen nannte, behält diese Zeile: Protokolle sind Nachweis und bleiben, wie sie geschrieben wurden. Die Nachricht ist weg, der Nachweis, dass dort eine lag, bleibt, und die Belegkette bleibt gültig, weil sie über die Kennungen rechnet. Hashes ohne Original sind keine Personendaten mehr.

Das ist die Struktur, die beide Anforderungen zugleich erfüllt: tatsächliche Vernichtung auf der Inhaltsebene und Nachvollziehbarkeit auf der Satzebene. Ein Archiv, das grundsätzlich nicht löschen kann, könnte Art. 6 Abs. 4 nicht erfüllen und kein Löschurteil vollziehen.

Der Fehlgriff ist behebbar. Sortiert jemand versehentlich eine private Nachricht in einen Projektordner, lässt sie sich mit demselben Weg wieder entfernen. Das ist wichtiger, als es klingt: Ohne diesen Weg erzeugte ein Bedienfehler eine dauerhafte Persönlichkeitsverletzung.

Die Prüfung unterscheidet Löschung und Verlust. Sie kennt drei Ergebnisse statt zwei: vorhanden, entfernt mit Vermerk, fehlend ohne Vermerk. Ohne diese Unterscheidung sähe eine rechtmässige Löschung aus wie eine Manipulation, und die Verwaltung holte sie aus der Sicherung zurück.

Der Grund wird mitgeschrieben. Enthält er eine Mailadresse, warnt Filum vorher, denn der Grund bleibt im Vermerk stehen.

7. Aufbewahrungspflicht gegen Löschpflicht

Eine gesetzliche Aufbewahrungspflicht rechtfertigt die weitere Bearbeitung und blockiert die Löschung für ihre Dauer (Art. 31 Abs. 1 DSGVO). Die Fristen laufen aber nicht für alles gleich:

Was	Frist	Norm
Buchungsbelege	10 Jahre ab Ende des Geschäftsjahres	OR 958f Abs. 1 i.V.m. 957a Abs. 3
Geschäftspapiere und sonstige Aufzeichnungen	10 Jahre ab Ende der Steuerperiode	MWSTG 70 Abs. 2 i.V.m. 42 Abs. 6
Unterlagen zu unbeweglichen Gegenständen	20 Jahre	MWSTG 70 Abs. 3
Projektkorrespondenz ohne Belegcharakter	keine eigene Pflicht, faktisch an die Verjährung gekoppelt	OR 127, OR 371 Abs. 2

Eine Nachricht mit der Frage nach einer Terminverschiebung ist kein Buchungsbeleg. Eine Nachricht mit einer Leistungsfreigabe oder einer Nachtragsvereinbarung sehr wohl. Ein brauchbares Aufbewahrungskonzept arbeitet deshalb mit Kategorien und nicht mit einer Pauschalfrist, und genau das verlangt auch die Auskunft nach Art. 25 Abs. 2 lit. d.

In Filum steht die Frist je Projekt im Archivstand, nicht in der App: Beginn ist der Projektabschluss, die Dauer wird in Jahren gesetzt, der Sockel ist zehn Jahre. Die Frist informiert, sie löscht nicht von selbst. Einmal im Jahr zeigt der Jahresdurchgang über alle Projekte, wo eine Frist abgelaufen ist, und hält den Durchgang als Text fest.

Dazu kommt die Löschsperre: Ein laufendes oder absehbares Verfahren blockiert jede Löschung, auch die der Verwaltung. Setzen und Aufheben werden mit Person, Zeitpunkt und Grund festgehalten und nie gelöscht. Mehr dazu im Blatt zum Streitfall.

8. Büros mit Standorten in der EU

Filum wird heute für die Schweiz gebaut. Wer in der EU tätig ist, hat drei zusätzliche Punkte auf dem Tisch, die hier der Vollständigkeit halber stehen:

- Ein Auftragsbearbeitungsvertrag nach Art. 28 DSGVO wird verlangt, sobald Support Daten für den Kunden bearbeitet. Für das Kernprodukt gilt dieselbe Überlegung wie nach DSGVO.
- Die Schweiz gilt als Drittland mit Angemessenheitsbeschluss, was die Übermittlung von Lizenzdaten trägt.
- Mitbestimmung: In Deutschland ist die Einführung eines Mailarchivs regelmässig mitbestimmungspflichtig, Österreich ist strenger, Frankreich greift ab elf Beschäftigten, Italien kennt mit Art. 4 des Statuto dei Lavoratori die schärfste Regel. Das ist eine Frage der Einführung, nicht der Software.

9. Was ein Anwalt entscheiden muss

- Ob das Büro ein Bearbeitungsverzeichnis führen muss oder die Ausnahme greift.
- Welche Aufbewahrungskategorien das Büro bildet und mit welchen Fristen.
- Wie das Nutzungs- und das Archivierungsreglement im Einzelnen lauten.
- Ob im konkreten Fall ein Löschbegehren gegen eine Aufbewahrungspflicht durchdringt.

10. Unterlagen, die mitkommen

Unterlage	Was sie leistet	Wo
Vorlagen für Löschkonzept, Reglemente, Verzeichnis und Datenschutztexte	zum Ausfüllen und Anpassen	offen unter github.com/bimover/mailarchiv-vorlagen
Datenschutzerklärung zu Filum	was die App mit Daten macht und was an bimover geht	www.bimover.ch/filum/privacy
.filum/verfahren.txt	die Verfahrensdokumentation	in jedem Archiv
Was Filum hält, Norm für Norm	mit den offenen Punkten	beim Support auf Anfrage
Vorgabeblatt zur Einrichtung	Archiv-Share und Sicherungen	beim Support auf Anfrage