
Filum and data protection: who is responsible for what

Roles, data paths, access requests and deletion. A sheet for whoever is responsible for data protection in the office.

As at 19.09.2026. The basis is the primary law (the Swiss Federal Act on Data Protection, FADP, and its ordinance in force since 1.9.2023, the Code of Obligations, the Labour Act and its Ordinance 3, the Civil Procedure Code), the practice of the Swiss data protection commissioner, and the code of Filum as it stands in the tree today. Not legal advice. Where a question calls for a decision, that is said explicitly.

1. The roles, before anything else is discussed

Most misunderstandings about mail archives come from mixing up the roles. With Filum they are unusually clear, because no service sits in between.

Who	Role	Why
The office	controller for the archive	It decides on purpose and means, and the data sit on its medium
bimover, core product	neither processor nor controller	The contents never reach bimover. Under prevailing Swiss doctrine, the mere possibility of taking notice is not processing
bimover, licence data	controller in its own right	bimover processes it for its own purpose, namely licensing and invoicing, not on the office's behalf
bimover, support in a specific case	processor, as soon as customer data is processed for the customer	For example when restoring an archive or reading a log containing contents

For the contract between office and bimover this means: the core product needs no data processing agreement, but it needs a confidentiality clause with a prohibition on use covering everything bimover can perceive during a support session. The support part needs the points required by art. 9 FADP and art. 7 of the ordinance. The transfer of licence data belongs in writing: which fields, what for, how long, where to.

2. What leaves the device

The question that decides everything is not «what does the software read?» but «what leaves the device towards bimover or a third party?».

Recipient	What goes there
Microsoft	the queries against one's own mailbox with the signed-in person's token
The office NAS	the messages, the attachments, the records
bimover.ch	one SHA-256 per archived mailbox instead of the address, the number of runs, the number of messages, an archive identifier without the project name, the licence evidence
Timestamp service	the hash of one record, nothing else

Subject lines, senders, recipients, text and attachments go nowhere except onto the office's own medium. A fixed list of forbidden field names in the tests holds that in place for the reports, and everything that could travel towards bimover for diagnostic purposes passes through a dedicated gate in the core. A diagnostic report is created only on request and names neither subject lines nor addresses.

Two notes belong with this. First: the SHA-256 of a mail address still counts as personal data even though it does not reveal the address. It therefore appears in this table as what it is, not as «anonymised». Second: the office has to inform its staff that licence data flows to bimover (art. 19 para. 2 let. c FADP, categories of recipients).

3. The design decision that carries the most weight

In Filum, only what a person has filed into the project folder themselves gets archived. That sounds like convenience and is in fact the load-bearing point.

Filum is not a monitoring or surveillance system within the meaning of art. 26 para. 1 of Ordinance 3 to the Labour Act. That provision prohibits systems intended to monitor employee behaviour at the workplace, and it turns on the purpose. Filum evaluates no traffic data, produces no statistics about people, measures no intensity of use and does not scan contents. The elements of the provision are therefore not met, and the question of justification never arises.

The default setting favours the data subject (art. 7 para. 3 FADP). The widespread practice reverses the presumption: whatever is not marked private counts as business and therefore as open to inspection. With Filum the opposite applies: whatever was not filed does not get archived.

The separation of private and business is made by the only person who can make it reliably (proportionality, art. 6 para. 2 FADP). There is no automatic classifier, no sampling and no employer discretion over someone else's mail.

Filing is a recognisable assignment of purpose (purpose limitation, art. 6 para. 3 FADP), including for external correspondents, whose message visibly becomes part of the project file.

It is equally clear what this design does not help with: the duty to inform under art. 19, the duty to delete under art. 6 para. 4, and a later access for a new purpose. Anyone searching the archive of a departed

employee in order to build a case against them faces exactly the assessment that led the Federal Supreme Court to find a violation of personality rights in 4A_518/2020.

4. What the office has to do itself

Filum does not take these points off the office's hands. They belong to the rollout.

Informing the staff before rollout (art. 19 FADP) and **consultation** under art. 48 of the Labour Act. This is the step most often overlooked.

Two sets of rules. A policy on use under art. 321d of the Code of Obligations states whether and to what extent private use is allowed, how private material is to be marked and what counts as misuse. An archiving policy states what gets archived and what expressly does not, where it sits, who has access, how long it is kept, how absence and departure are handled, what happens to a private message archived by mistake, and how an access request is processed.

Record of processing activities (art. 12 FADP). The exemption for companies with fewer than 250 employees does not apply once sensitive personal data is processed on a large scale, and assessing that question is itself work. In practice a lean record is cheaper than the assessment of whether you may omit one.

Data security (art. 8 FADP, art. 1 to 3 of the ordinance). The setup of the archive pays into this directly: a separate share, access through personal accounts, automatic backups that only the NAS administration can reach.

No access to an absent person's mailbox without a policy and without the four-eyes principle. That is the commissioner's practice and independent of Filum.

5. Access requests

Any data subject can request information (art. 25 FADP), and the information is generally due within 30 days (art. 18 of the ordinance). Waiving that right in advance is void (art. 25 para. 5 FADP).

Filum helps at one concrete point: «Auskunft und Löschung» searches across all projects in a storage location by address or by identifier and shows the hits with their location. The reading view makes conversations legible together instead of sending a person through hundreds of individual files. Without such a tool, an access request in a grown mail holding is hard to handle within thirty days.

The limit belongs in the same breath: a conversation almost always contains data about third parties. Handing over the whole exchange without assessing those third parties' interests is not permissible (art. 26 para. 1 let. b FADP). Filum does not take that assessment off anyone's hands.

6. Deleting

This is where what applies is most often misrepresented, including by vendors.

Switzerland has no free-standing right to erasure. Art. 32 para. 1 FADP gives a right to rectification of incorrect data. Erasure runs through art. 32 para. 2 let. c as a claim in court and requires an unlawful violation of personality rights. There is no counterpart to art. 17 GDPR.

The duty nevertheless exists, and it exists on the controller's own initiative. Art. 6 para. 4 FADP requires destruction or anonymisation as soon as the data are no longer necessary for the purpose. Breaching that duty breaches a principle under art. 6, and that is precisely what establishes the violation of personality rights from which a claim for erasure then does follow. The circle closes.

How Filum implements it. Deletion removes the original and the reading copy together with the attachments no other message needs. The line in the record file is redacted: the two identifiers stay, addresses, subject and text go. Next to it a note is created with time, person and reason. The message is gone, the evidence that one was there remains, and the chain of records stays valid because it computes over the identifiers. Hashes without an original are no longer personal data.

That is the structure which satisfies both requirements at once: actual destruction at the content level and traceability at the record level. An archive that fundamentally cannot delete could not satisfy art. 6 para. 4 and could not carry out a court order.

A misfile can be undone. If someone accidentally files a private message into a project folder, it can be removed the same way. That matters more than it sounds: without that route, an operating error would create a lasting violation of personality rights.

The check distinguishes deletion from loss. It has three outcomes rather than two: present, removed with a note, missing without one. Without that distinction a lawful deletion would look like tampering, and the administration would restore it from the backup.

The reason is recorded. If it contains a mail address, Filum warns beforehand, because the reason stays in the note.

7. Retention duty against duty to delete

A statutory retention duty justifies further processing and blocks erasure for its duration (art. 31 para. 1 FADP). The periods do not run equally for everything:

What	Period	Provision
Accounting vouchers	10 years from the end of the financial year	CO 958f para. 1 in conjunction with 957a para. 3
Business papers and other records	10 years from the end of the tax period	VAT Act 70 para. 2 with 42 para. 6
Records concerning immovable property	20 years	VAT Act 70 para. 3
Project correspondence without voucher character	no duty of its own, in practice tied to limitation periods	CO 127, CO 371 para. 2

A message asking to move a meeting is not an accounting voucher. A message approving work or agreeing a variation very much is. A workable retention concept therefore uses categories rather than one flat period, and that is also what an access request under art. 25 para. 2 let. d requires.

In Filum the period sits per project in the archive itself, not in the app: it starts at project completion, the duration is set in years, the base is ten years. The period informs; it does not delete by itself. Once a year the annual review shows, across all projects, where a period has expired, and records the review as text.

On top of that comes the deletion block: a pending or foreseeable proceeding blocks every deletion, including the administrator's. Setting and lifting it are recorded with person, time and reason and never deleted. More on that in the sheet about disputes.

8. Offices with locations in the EU

Filum is built for Switzerland today. Anyone operating in the EU has three additional points on the table, listed here for completeness:

- A data processing agreement under art. 28 GDPR is required as soon as support processes data for the customer. For the core product the same reasoning applies as under the FADP.
- Switzerland counts as a third country with an adequacy decision, which carries the transfer of licence data.
- Works council participation: in Germany the introduction of a mail archive is regularly subject to code-termination, Austria is stricter, France applies from eleven employees, and Italy has the strictest rule in art. 4 of the Workers' Statute. That is a question of rollout, not of software.

9. What a lawyer has to decide

- Whether the office must keep a record of processing activities or the exemption applies.
- Which retention categories the office forms and with which periods.
- How the policy on use and the archiving policy read in detail.
- Whether, in a specific case, a request for erasure prevails over a retention duty.

10. Documents that come with it

Document	What it provides
<code>docs/loeschkonzept-vorlage.md</code>	template for the office's deletion concept including the deletion log
<code>docs/aufbewahrung.md</code>	what Filum holds, provision by provision, with the open points
<code>docs/backup-vorgabebblatt.md</code>	setting up the archive share, the backups and access logging
<code>.filum/verfahren.txt</code>	the procedural documentation, present in every archive
<code>PRIVACY.md</code>	what counts as data collection in bimover apps