
What the archive carries in a dispute

Evidentiary value, deadlines, and what to do first in an emergency. A sheet for the management and its legal advisers.

As at 19.09.2026. The basis is the primary law (the Swiss Code of Obligations, the Ordinance on the Keeping and Preservation of Account Records known as GeBüV, the VAT Act, the Civil Procedure Code), three Federal Supreme Court decisions, and the code of Filum as it stands in the tree today. Not legal advice.

One word will not appear here: watertight. No archive in the world makes a dispute safe. What an archive can do is narrower and more useful: make your own account provable and carry the burden under art. 178 of the Civil Procedure Code when the other side substantiates its challenge to authenticity.

1. An .eml is a document, without a seal and without a certificate

Art. 177 CPC: «Documents are objects capable of proving legally relevant facts, such as writings, drawings, plans, photographs, films, sound recordings, electronic files and the like, as well as private expert reports by the parties.»

The concept is open and technology-neutral. An archived message needs no signature, no seal and no certification to be a document. The Federal Supreme Court expressly rejected the opposite view (6B_130/2012): the idea that only an electronic signature can confirm the sender's authenticity rests on a misunderstanding of what makes evidence admissible.

Three further provisions set the frame:

- **Art. 157 CPC:** the court assesses the evidence freely. There is no table from which the value of an archive could be read off.
- **Art. 178 CPC:** whoever relies on a document must prove its authenticity if the other party challenges it. The challenge must be sufficiently substantiated. Bare denial does not suffice.
- **Art. 179 CPC:** only public registers and public deeds provide full proof. A private message never reaches that, however it is archived.

2. What Filum contributes

The original rather than a printout

The court or the other party may demand production of the original where there are justified doubts about authenticity (art. 180 para. 1 CPC). As evidence, Filum stores the complete `.eml` in the state Microsoft 365 delivers it. Inside it are the things that matter in this situation: the complete chain of received headers, the Message-ID, the results of sender authentication and the DKIM signature of the sender's domain.

The archive file in `Mails/` is the reading copy by contrast. It is there to be read and printed. What goes to court is the `.eml`. The app extracts it at the press of a button and checks its bytes against the value recorded when it was filed.

One note on the DKIM signature, so that nobody expects more than it delivers: it is a genuine cryptographic signature by the sender's domain and it travels inside the `.eml`. But it is verifiable only as long as the matching public key is still published in that domain's DNS. After a key rotation at the sender it is not. Filum does not archive the key alongside today.

The chain of records and the timestamp

Every run writes a holding record: a hash over the entire holding, both identifiers per message, sorted, chained to the record of the previous run. On that record Filum obtains a timestamp under RFC 3161 from an independent service and stores it raw next to it.

The difference between the two matters, and it is usually blurred:

A self-generated chain proves internal consistency. It does not prove that the chain was not regenerated wholesale by someone with write access, and that person exists in every office. Against a party that substantiates its challenge, the value of a purely internal chain is therefore limited.

A third party's timestamp removes exactly that limit. It anchors the point in time outside the office. From then on it can be shown that a particular holding already existed in that form at a particular time, without anyone having to take the office's word for it. That is why stamping happens, and that is why one stamp per run suffices: the chain binds everything else.

Verification that works without the vendor

The archive contains a verification script that needs nothing but the Python standard library. It recomputes every file, the records, the chain and the signature of the timestamps, and names every missing or altered file with its path. The app computes the same thing on the project page, and a test keeps both verifiers tied to each other.

In a dispute that is worth more than any vendor assurance: the other party or a court expert can run the verification themselves, without bimover and without Filum. Every verification is stored in the archive as a log, with deviations named.

The procedural documentation and the logs

Every archive contains procedural documentation describing identifiers, chain, timestamp service and limits, plus one log per run with the sources, what was skipped and what failed. Together that is what makes a documented and repeatable procedure: whoever has to testify how the archive came about reads it there instead of recalling it.

3. What the law actually requires for a NAS

The widespread assumption that electronic archiving requires unalterable media is wrong.

GeBüV art. 3: the standard is that changes cannot be made without that being detectable.

A NAS is expressly a changeable medium under **art. 9 para. 2 GeBüV**. It is permissible nonetheless, under the four cumulative conditions of **art. 9 para. 1 let. b**. Filum addresses them as follows:

Condition	With what
Technical procedures ensuring integrity	hash per message, holding record over the entire holding, chained
Unfalsifiable point in time of storage	third-party timestamp under RFC 3161 on every record
Compliance with the rules for using the procedures, documented	procedural documentation in the archive, run logs
Retention of the auxiliary data including logs	records, timestamps, record files and logs all sit in the archive

Alongside come **art. 10 para. 1 GeBüV**, the regular check of integrity and legibility, which in Filum is a button that leaves a log, and **art. 8 GeBüV**, the logging of access: that is the NAS's job, and how to switch it on for Synology and QNAP is in the setup sheet.

What follows is uncomfortable and correct: Filum does not prevent changes to the archive. It makes them detectable, and the NAS backup brings back what is missing. That is precisely the route the law provides for changeable media.

4. What an archive never proves

Receipt by the addressee. In 5A_514/2022 the Federal Supreme Court held that merely sending a message does not establish successful communication, and that a printout of one's own message does not suffice for that. An archive of one's own sent mail proves the existence and content of the message, not its arrival.

A practical rule follows: **the recipient's copy is stronger evidence than the sender's copy**. A received message with a complete chain of received headers documents delivery into one's own sphere. Whoever wants to be able to prove an important notification watches for the reply to it.

Lawfulness of how the evidence was obtained. Admissibility is as a rule decided by art. 152 para. 2 CPC, not by archiving technology: unlawfully obtained evidence is considered only if the interest in ascertaining the truth prevails. In 4A_518/2020 mails were rejected and damages for satisfaction were added on top. What tipped it was the unlawful acquisition, the availability of milder means and a purely pecuniary dispute.

This is the most elegant argument Filum has, and it is substantively correct: an archive that only takes in what someone designated as a project file is not merely privacy-friendly. It is in the better position evidentially as well.

5. How long all this has to stay within reach

The periods that set the horizon for a planning office are not the ones named first.

Period	Provision	Starts
10 years	CO 958f para. 1, accounting vouchers	end of the financial year
10 years	VAT Act 70 para. 2 with 42 para. 6, business papers	end of the tax period
20 years	VAT Act 70 para. 3, immovable property	as provided
5 years	CO 371 para. 2, defect rights in immovable works, expressly against architects and engineers	acceptance of the work
10 years	CO 127 and 130, contractual and fee claims	when due
20 years absolute	CO 128a, personal injury from breach of contract	the harmful conduct

Three reasons why the building trade thinks beyond ten years:

When the clock starts. The five years under CO 371 para. 2 run from acceptance, not from the planning work. With a four-year project, correspondence from the preliminary design has to be findable nine years later. Since 1 January 2026 this period can no longer be shortened to the client's detriment under CO 371 para. 3.

The notification period for drawings. CO 370 para. 4 let. b, in force since 1 January 2026, covers defects in a work produced by an architect or engineer and used as intended as the basis for an immovable work. Notice within 60 days of discovery, shorter agreements ineffective. Disputes will therefore often turn on when what was communicated. That sits in the header of the message.

The burden of proof. The architect is a mandatee. Under CO 97 para. 1 he must exculpate himself, and under CO 400 para. 1 he owes an account at any time on request. Whoever cannot show after eight years that he gave a warning, did not give one.

6. What to do in practice when a dispute starts

1. **Set the deletion block before anything else.** A pending or foreseeable proceeding blocks every deletion in Filum, including the administrator's. Setting and lifting are recorded with person, time and reason and never deleted. This is not a formality: deleting after learning of a proceeding rebounds on the office in the assessment of evidence, and duties to produce documents exist under art. 160 CPC.

2. **Verify, and keep the log.** The check names every deviation with its path. A log created before the dispute weighs more than one created after.
3. **Extract the original, not the reading copy.** The app checks the bytes against the recorded identifier and says so if something does not match.
4. **Prepare the history through the conversation.** The reading view shows the exchange with everyone involved and links the original for each message.

2024-0042 **Lindenhof: defects list from the apartment handover of 12 May**

23 messages 12 incoming · 11 outgoing 2025-06-09 to 2025-08-20

PARTICIPANTS

Sender	jonas.keller@studiohartmann.example	6 sent	2025-06-09 to 2025-08-20
Sender	S Wyss <s.wyss@baurea.example>	5 sent	2025-06-09 to 2025-08-20
Sender	lea.hartmann@studiohartmann.example	5 sent	2025-06-09 to 2025-08-20
Sender	m.fontana@fontana-immob.example	2 sent	2025-06-09 to 2025-08-20
Sender	r.brunner@fontana-immob.example	2 sent	2025-06-09 to 2025-08-20
Sender	r.odermatt@odermatt-bau.example	1 sent	2025-06-11 to 2025-08-09
Sender	offerte@fenora.example	1 sent	2025-06-13 to 2025-06-15
Sender	p.steiner@ingena.example	1 sent	2025-07-03 to 2025-07-05

MESSAGES

S Wyss <s.wyss@baurea.example> To: lea.hartmann@studiohartmann.example, m.fontana@fontana-immob.example
Cc: jonas.keller@studiohartmann.example, r.brunner@fontana-immob.example
2025-06-09 18:40 MESZ · Incoming · Message 1

Dear Ms Hartmann, dear Mr Fontana

The handover of apartments 1.1 to 3.4 was completed today at 16.30. Across the twelve units we recorded a total of 87 items, 9 of which were classified as substantial.

Main areas: parquet in the living areas showing joint gaps in five apartments, silicone joints in the wet rooms poorly executed, three apartment doors rubbing against the stop. In apartment 2.3 the cover of the blind box is missing entirely.

The list is attached, sorted by apartment and trade. Please let me know by Friday which items you as the client wish to track yourselves.

Kind regards
Stefan Wyss

Attachments
[Defects_list_handover_apartments_12-05.pdf](#)

Archive file (DDE(A) - Original (.eml))
128 B · text/csv

A conversation from the sample project: who wrote what and when, with attachments, and for each message the way to the archive file and to the original. This is exactly the view legal advisers start from.

5. **Do not tidy up yourself.** Whoever cleans up the archive while a dispute is running damages their own position more than the cleanup ever helps.

7. What is open today

- The DKIM key of the sender's domain is not archived alongside. After a key rotation at the sender, the signature of an old message can no longer be verified.
- Access to the archive is logged by the NAS, not by Filum. That is a setting, not a gap: the setup sheet gives the route for Synology and QNAP. It still has to be switched on, and nobody but the office checks that.
- Filum archives what someone filed. A statement about the completeness of all mail traffic is therefore not possible, and the coverage report expressly measures only the conversations of which something has already been filed.

- Technology does not help against restoring the whole archive from a backup older than a deletion. For that the office keeps the deletion log, and Filum finds the affected messages again by their identifier.

8. Where it is written more precisely

Question	File
What Filum holds, provision by provision	docs/aufbewahrung.md
Tamper protection and the attacks tested against	docs/audit-veraenderbarkeit.md , docs/audit-angriff-protokoll.md
The office's deletion concept and deletion log	docs/loeschkonzept-vorlage.md
The legal dossiers with the primary sources	docs/geborgen/recht-schweiz.md , docs/geborgen/recht-eu.md
Data protection and the allocation of roles	docs/whitepaper-datenschutz-en.md