What we see — and what we don't



Family Memories is a private place for a family's memories. Content is end-to-end encrypted on the family's devices: **only your family can read photos, videos and stories – not even we can.**

Only your family can read

- photos and videos, voice recordings
- stories and their chapters
- captions, comments, tags, album titles
- dates and the places photos were taken
- the family's name, motto, picture and logo
- profile pictures

Encryption happens on the device before anything is uploaded. The keys never leave the devices unencrypted.

What we see

- who is in which family, in which role
- profile names and email addresses
- when something was uploaded or changed
- number, size and type of files
- which entries belong together, access patterns, coarse map requests
- time zone, language, day of last use
- for a book order: name and delivery address

Only if you agree

- **Printing:** for a printed book, our print service and Gelato read the content. We delete the print PDF 30 days after delivery.
- **Translation:** only at the press of a button; the text goes through our server to DeepL; neither our server nor DeepL stores it.
- **Shared links:** whoever has the link can open the selection. The key is only in the link and never reaches a server.
- **Support:** screenshots and attachments you send are seen by our team and deleted after 90 days. The chat assistant Lumi only sees what you type.

Where the limits are

- **Web app:** whoever serves a website could serve modified code. Strict browser rules protect against foreign code, not against us as the operator. The Android app ships its code and only gets new code through signed updates.
- **New members:** on the very first contact, the service could present a false key. The safety code that two people can compare reveals this.

Check for yourself

- White paper with all details and limits: **family-memories.eu/en/sicherheit/whitepaper**
- Crypto core, source available for review: **github.com/family-memories-eu/krypto-kern**
- Mozilla HTTP Observatory: grade A+ · Webbkoll: no third-party cookies · exodus: 0 trackers in the Android app 1.0.17 (all on 27 Oct 2026)
- No tracking, no advertising. Servers in the EU, the core services in Germany.