

Data processing agreement

Template · as at 20 September 2026 · tunnl.ch, a service of xoox ag

We wrote this template ourselves and it has not been reviewed by lawyers. It truthfully describes what tunnl. does – it does not replace legal advice. If you intend to sign it, have your own legal department look at it; we are open to changes.

1. Parties

Controller (client): _____

Address: _____

Represented by: _____

Processor: xoox ag, Unter Sidhalden 16, 6010 Kriens, Switzerland (UID CHE-210.624.108), operator of the tunnl. service at tunnl.ch.

2. Subject and duration

The subject is the provision of tunnl.: a service with which the client hands over messages and files end-to-end encrypted. The agreement applies as long as the client uses tunnl. and ends when their account is deleted.

3. Nature, purpose and scope of processing

The sole purpose is the confidential handover of messages and files including a reply channel. tunnl. stores:

- **Encrypted contents** of messages and files including file names. Keys are created in the browser and live in the part of the link after “#”; they never reach the server. **The processor cannot decrypt the contents.**
- **Hashes** of access tokens and access keys.
- **Technical data without content:** times of creation, sending, pickup and expiry, number of messages, size and deadline of files, whether a password is set, number of failed attempts.
- **Account data:** e-mail address encrypted and as a hash, chosen option, alert settings.
- **For branded sending (option “gotthrd”):** company name, reply address and logo in clear text because they appear in the e-mail. Address book and text blocks are stored encrypted.
- **When sending mail:** recipient address, subject and covering text are processed at the moment of sending and not stored.

Not stored: IP addresses, browser identifiers, location data, advertising cookies.

4. Categories of data subjects

Employees, customers, suppliers and other people to whom the client hands over messages or files, or from whom it receives them. Which personal data are inside the encrypted contents is determined by the client alone; they are not accessible to the processor.

5. Instructions

The processor processes personal data only on documented instructions from the client. Using the service counts as an instruction. If the processor considers an instruction unlawful it says so and may suspend it.

6. Confidentiality

Everyone with access to the processor's systems is bound to confidentiality. The number of such people is kept small; access is protected with two-factor authentication.

7. Technical and organisational measures

- **End-to-end encryption in the browser:** AES-256-GCM, key derivation HKDF-SHA-256, PBKDF2 with 600,000 rounds for passwords. Files are encrypted chunk by chunk with the chunk index bound in.
- **The server holds no keys.** Access tokens exist only as hashes.
- **Transport:** HTTPS only, with HSTS; strict content and permission policies; no third-party scripts, no external fonts, no analytics.
- **Attachments** are stored outside the web folder with their own lock; every file has a deadline and is deleted when it passes.
- **Automatic deletion:** conversations expire after the chosen deadline; after ten failed attempts a conversation is deleted. Tombstones disappear after seven days.
- **Access protection:** sign-in by one-time code or passkey, sessions stored as hashes, "sign out on all devices" in the account.
- **Security log** without IP addresses and without content, kept for 90 days.
- **Operation** in data centres in Switzerland; access for a small number of authorised people only.

The measures reflect the state at the time of signing and may evolve as long as the level of protection does not drop. The current state is published at tunnl.ch/sicherheit.

8. Sub-processors

The client agrees to the following sub-processors:

- **METANET AG**, Josefstrasse 218, 8005 Zurich, Switzerland – hosting and mail delivery, data centres in Switzerland.

Further sub-processors will be announced in advance. The client may object within 30 days and may then terminate the agreement.

9. Place of processing

Switzerland. No disclosure abroad takes place, unless the client or its recipients access the service from abroad or the recipient address is hosted by a foreign mail provider.

10. Support for the client

The processor supports requests for access, rectification and erasure as far as it can without knowing the contents. **It cannot provide information about contents** because it cannot decrypt them; the client does that from its own account. Deleting a conversation is possible at any time in the account and takes effect immediately.

11. Reporting breaches

If the protection of personal data is breached, the processor notifies the client without delay, at the latest 48 hours after becoming aware, with all available details.

12. Evidence and audits

On request the processor demonstrates compliance with this agreement. An on-site audit is possible by prior appointment during business hours, at most once a year, provided it does not disrupt operations.

13. Deletion after the agreement ends

When the agreement ends, the account and its data are deleted. Encrypted contents expire after their deadline anyway. Encrypted data may remain in the hosting provider's backups until the respective backup expires.

14. Liability and law

Swiss law applies, excluding conflict-of-law rules; the place of jurisdiction is Lucerne. Where the GDPR applies to the client, this agreement serves as the arrangement under Art. 28(3) GDPR.

15. Signatures

Place, date: _____

Place, date: _____

For the client

For xoox ag

Name, function

Name, function

To sign: [as a PDF \(DE\)](#) · [PDF \(EN\)](#) · [Privacy policy](#)