LEGAL · DPA

Data processing **agreement.**

Version 1.1, in force since 28 October 2026. Issued by LT Telecom (UAB "LT telekomunikacijos").

Proof Holdings
PROOF.HOLDINGS · LEGAL

DOCUMENT
v1.1

title	**Data Processing Agreement**
governs	processing of customer end-user data under Article 28
issuer	LT Telecom (UAB "LT telekomunikacijos")
updated	2026-10-28
pdf	Download PDF · https://proof.holdings/legal/dpa.pdf
status	IN FORCE · 28 OCTOBER 2026

QUESTIONS hello@proof.holdings

This Data Processing Agreement ("DPA") is part of the Terms of Service between the customer — the business named in the account's company details, or the account

holder where none are given — ("Customer") and LT Telecom (UAB "LT telekomunikacijos"), registration code 304043870, Buivydiškių g. 118, Zujūnai, LT-14162 Vilniaus r., Lithuania, reachable at hello@proof.holdings ("Provider"). It applies whenever the Customer uses the Service to process personal data of its own users, and it is entered into by accepting the terms — no signature is needed. A printed copy of this version can be downloaded as a PDF; the same link is on the record sheet at the top of this page. This page is the agreement itself, not advice on the Customer's own obligations under the GDPR.

1. Roles and scope

For the personal data the Customer sends to the Service — identifiers of the Customer's users, the content of approval requests, and the results — the Customer is the **controller** and the Provider is the **processor** within the meaning of Article 28 of Regulation (EU) 2016/679 (the "GDPR"). For the Customer's own account data the Provider is a controller, as described in the Privacy Policy. The details of the processing are in Annex I.

2. Definitions

Terms such as personal data, processing, controller, processor, data subject, personal data breach and supervisory authority have the meaning given in the GDPR. "Subprocessor" means a third party the Provider engages to process Customer personal data. "Service" means Proof Holdings as described in the terms.

3. Processing on documented instructions

The Provider processes Customer personal data only on the Customer's documented instructions. The terms, this DPA and the Customer's use of the API and the dashboard are those instructions. If a law of the European Union or of a member state requires the Provider to process otherwise, the Provider tells the Customer before processing, unless that law forbids it. The Provider tells the Customer at once if, in its view, an instruction infringes the GDPR.

4. Confidentiality of personnel

Only people who need access to Customer personal data to run the Service have it, and each of them is bound by a duty of confidentiality.

5. Security

The Provider implements the technical and organisational measures in Annex II, taking into account the state of the art, the costs, and the risks of the processing, so as to ensure a level of security appropriate to those risks (Article 32 GDPR). The Provider may improve the measures over time but will not lower the overall level of protection.

6. Subprocessors

The Customer gives a general authorisation for the Provider to engage subprocessors. The categories engaged, what each does, the data it receives, where it processes and the basis for any transfer outside the EU are published at proof.holdings/subprocessors, which is Annex III of this DPA. The Provider dates the change on that page at least 30 days before a new category starts processing Customer personal data and tells account holders by email or in the dashboard, as for a material change to the terms. The Customer may object on reasonable data-protection grounds by writing to hello@proof.holdings within that period; if no solution is found within that period, the Customer may stop using the channel or feature that category serves, or end the agreement, without penalty; fees already due stay due. On request, and subject to confidentiality, the Provider discloses to the Customer the identity of the subprocessors behind the published categories.

The Provider imposes on each subprocessor, by contract, data-protection obligations equivalent to those in this DPA, and remains liable to the Customer for the subprocessor's performance.

7. Data-subject requests

The Service already limits what a request can touch: verification attempts and delivery records are deleted automatically 90 days after creation, a verification token carries a

hash of the identifier rather than the identifier, and the Customer can revoke a proof at any time through the API and the dashboard. For erasure of a specific record on a data subject's request, the Customer writes to hello@proof.holdings and the Provider completes it within 30 days. Where a data subject contacts the Provider directly about Customer personal data, the Provider refers the request to the Customer without undue delay and does not answer it on the Customer's behalf unless instructed. Taking into account the nature of the processing, the Provider assists the Customer with appropriate measures in responding to requests under Chapter III of the GDPR.

8. Assistance: security, breaches and impact assessments

The Provider assists the Customer in meeting its obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Provider. The Provider notifies the Customer of a personal data breach affecting Customer personal data without undue delay and in any case within 72 hours of becoming aware of it, with the information Article 33(3) requires as far as it is available, and follows up as more becomes known.

9. Deletion and return

At the Customer's choice the Provider returns Customer personal data — the Customer can take a complete export at any time through the dashboard — and, on termination of the Service or earlier on the Customer's instruction, deletes it within 30 days, except what Union or member-state law requires the Provider to keep, and except the records listed in the Privacy Policy's deletion section, which concern the Customer's own account and billing and hold none of the identifiers of the Customer's users. If a final invoice is unpaid, the Customer's account is locked at once and the deletion completes when the invoice is settled, as the Privacy Policy describes. Backups are overwritten on their normal rotation; if a backup is ever restored, deletions made since are applied again.

10. Audit

The Provider makes available to the Customer the information necessary to demonstrate compliance with Article 28 of the GDPR, including the named subprocessor list (section 6), a fuller description of the measures in Annex II than this page carries, and the record of any personal data breach affecting Customer personal data, on request to hello@proof.holdings. Where that information is not sufficient, the Customer may, once in any twelve-month period and on 30 days' written notice, conduct or mandate an independent audit limited to the processing under this DPA, at the Customer's cost, at a time agreed with the Provider and under confidentiality.

11. International transfers

Where the data is. The Provider runs the Service and stores Customer personal data in the European Union.

Subprocessors outside the EU. Some subprocessor categories process data in the United States or from servers worldwide. For each such category the register in Annex III states the basis for the transfer. Where the Provider has a contract with the subprocessor, that basis is the European Commission's standard contractual clauses (Decision (EU) 2021/914) or another safeguard recognised under Chapter V of the GDPR.

Messaging platforms. Telegram and WhatsApp are not the Provider's subprocessors. The data subject starts the conversation from their own account on a platform they already use, and the platform processes it as the data subject's own service under its own terms; the Provider only sends the messages of that conversation. Annex III states this for that category.

Customers outside the EEA. If the Customer is established outside the European Economic Area and is not itself bound by the GDPR, sending verification results back to the Customer is itself a transfer out of the EU. For that transfer the parties agree that the standard contractual clauses apply (Decision (EU) 2021/914, module four, processor to controller), with Annex I and Annex II of this DPA providing the information those clauses require.

12. Liability

The liability of each party under this DPA is subject to the limitations and exclusions in the Terms of Service, to the extent the GDPR allows; nothing in this section limits a data subject's rights under Article 82 GDPR.

13. Term and precedence

This DPA applies for as long as the Provider processes Customer personal data. If this DPA and the Terms of Service conflict on a matter of data protection, this DPA prevails. The version and date at the top of this page identify the DPA in force; the Provider tells the Customer of material changes as described in the terms.

Annex I — Details of the processing

Subject matter. Verification of control over identifiers, delivery and recording of human approvals, and issuance of signed proof tokens, as the Customer configures through the Service.

Duration. For the term of the Terms of Service, plus the deletion period in section 9.

Retention. Verification attempts and webhook delivery records are deleted automatically 90 days after creation; proof tokens are kept until the expiry set when they are created, and a revoked token stays listed as revoked; daily backups are kept for 90 days and one monthly backup for a year; everything else is kept for the term plus the deletion period in section 9.

Nature and purpose. Sending and receiving verification and approval messages over the channels the Customer and the data subject select; checking the identifier's control; recording the outcome; signing a proof token; delivering results to the Customer's endpoints.

Categories of data subjects. The Customer's users, customers, employees, agents and approvers — the people whose identifiers the Customer verifies or whose approval the Customer requests.

Categories of personal data. Phone numbers, email addresses, domain names and other identifiers the Customer submits; messaging-platform identifiers; the verification messages the Service sends and receives (codes and links); approval requests and the approvers' replies, which the Service accepts only in encrypted form and cannot read — they are encrypted end to end between the Customer and its approvers; approval decisions (approved or denied) and their timestamps; IP addresses and user-agent strings recorded for security; for SMS verifications, a risk record (country of the phone number and of the IP address, whether they match, VPN or proxy detection, a risk score). The Service does not request identity documents, legal names or addresses from data subjects.

Special categories of data. None are requested or needed. The Customer must not send them.

Annex II — Technical and organisational measures

- **Encryption in transit.** All traffic to the site and the API is over HTTPS; the origin servers accept connections only from the edge network in front of them.
- **Encryption at rest.** Identifiers and credentials in the database are encrypted at the field level with AES-256-GCM; verification tokens carry a SHA-256 hash of the identifier, not the identifier; a delegation token names its domain and artifact in clear, since that is what it states.
- **End-to-end encryption of approvals.** Approval requests and the approvers' replies are encrypted by the Customer and its approvers with keys the Provider does not hold; the Service refuses an approval request sent in plain text and stores only ciphertext it cannot read.
- **Access control.** Access to production systems is limited to the operators who run it; secrets are kept in a managed secrets store and rotated on a schedule; customer API keys are stored hashed and can be scoped to a sub-account; deleting the account, removing a sign-in identifier or revoking an API key in the dashboard requires a second factor.
- **Logging and monitoring.** Administrative actions on accounts and every change to a delegation are written to audit logs; identifiers are masked in application logs; uptime and errors are monitored continuously.

- **Backups and recovery.** Backups are taken daily and encrypted, with a copy off the primary servers; daily backups are kept for 90 days and one monthly backup for a year; recovery steps, including replaying deletions after a restore, are documented.
- **Data minimisation and retention.** Delivery and attempt records expire automatically; account deletion runs a documented workflow with a short grace period and a 30-day completion deadline.
- **Development practice.** Changes go through code review and an automated test and drift-check suite before deployment; dependencies are audited for known vulnerabilities in continuous integration.

Annex III – Subprocessors

The register of subprocessor categories, with purpose, data, location, transfer basis and status, is published at proof.holdings/subprocessors and forms part of this DPA.