PRIVACY POLICY

# Root-ling Marketplace

GDPR-Compliant Privacy Policy — Republic of Lithuania
**Version:** 3.1 | **Effective date:** 2 May 2026 | **Last revised:** 28 October 2026

*This version applies from 28 October 2026. Earlier versions are available on request at info@root-ling.com.*

This Privacy Policy explains how Root-ling ("we", "us", "our") collects, uses, and shares your personal data when you use the Root-ling platform, including our website (root-ling.com) and mobile application.

By using the Platform, you acknowledge and confirm that you have read and understood this Privacy Policy. The processing of your personal data is carried out in accordance with the legal bases described in this Policy.

Root-ling acts as the **data controller** for the personal data described in this Privacy Policy.

## 1. Introduction

Root-ling operates a two-sided task marketplace connecting Task Makers (individuals who post tasks) with Taskers (independent service providers). To provide this service, we collect and process certain personal data about our users.

We are committed to protecting your privacy in accordance with **Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR")** and the **Lithuanian Law on Legal Protection of Personal Data**. If you do not agree with our practices, please do not use the Platform.

## 2. Data Controller Information

The data controller responsible for your personal data is:

**UAB Root-ling**
Laisvės al. 85E-5, LT-44297 Kaunas, Republic of Lithuania
Registration code: 307894328
**Data Protection / Legal:** info@root-ling.com
**General Support:** support@root-ling.com
**Phone:** +370 622 47542
**Website:** https://www.root-ling.com

For data protection inquiries, please contact us at **info@root-ling.com**. We will make reasonable efforts to respond to data protection inquiries in a timely manner.

# 3. Types of Personal Data We Collect

## 3.1 Account Data

- Full name
- Email address
- Phone number
- Password (stored in encrypted/hashed form — never in plain text)
- User role (Task Maker or Tasker, assigned automatically based on activity)
- Profile photo (if uploaded)
- Bio, languages, vehicle access, service categories
- Account creation date and last login

## 3.2 Identity Verification Data

When required (e.g., for Stripe Connect payouts), we may collect:

- Government-issued ID documents
- A live selfie for face-matching (biometric data)
- Verification status (stored internally as verified/unverified — not publicly displayed)

Verification documents are **retained for 12 months** from successful verification for fraud and dispute investigation purposes, then deleted. The verification status flag is retained while the account is active.

## 3.3 Location Data

We collect approximate location data to match users with nearby tasks. Specifically:

- City/municipality level location (provided by you during registration or task posting)
- GPS coordinates (requested with your permission on mobile devices for proximity-based task matching)

**We do not continuously track your real-time location.** Location is used only when actively using the task matching features of the Platform.

## 3.4 Communication Data

- Messages sent between users via the in-app chat system
- Message timestamps and read status
- Support tickets and feedback

**All in-platform messages are monitored** for content policy violations (e.g., contact information sharing, prohibited content). Messages are not sold to third parties.

## 3.5 Transaction Data

- Task budget amounts and payment status
- Stripe payment intent IDs and transaction references
- Service fee records
- Task boost payment records

- Subscription payment records
- Promo code redemptions and ambassador commissions

**Root-ling does NOT store full card numbers, CVV codes, or complete payment credentials.** All sensitive payment data is processed and stored exclusively by Stripe.

### 3.6 Usage & Activity Data

- Tasks posted, accepted, and completed
- Swipe interactions (task interest/skip actions)
- Ratings and reviews submitted
- Login timestamps and session activity

### 3.7 Device & Technical Data

- IP address
- Browser type and version
- Device type and operating system
- Referral source and pages visited
- Cookie identifiers (subject to your cookie consent)

## 4. How We Use Your Personal Data

| Purpose | Data Used | Legal Basis |
|---|---|---|
| Account creation and authentication | Account data | Contract performance |
| Matching tasks with nearby Taskers | Location, usage data | Contract performance |
| Processing task payments via Stripe | Transaction data | Contract performance |
| Facilitating in-app communication | Communication data | Contract performance |
| Ratings and reviews system | Account, task data | Contract performance |
| Subscription and ambassador programmes | Account, transaction data | Contract performance |
| Content moderation (chat, reviews) | Communication data | Legitimate interest |
| Identity verification for payouts | Verification data | Legal obligation / Contract |
| Platform analytics and improvement | Usage, device data | Consent / Legitimate interest |
| Sending service notifications | Email, push token | Contract performance |
| Fraud prevention and security | All data categories | Legitimate interest |
| Legal compliance and dispute resolution | All relevant data | Legal obligation |
| Marketing communications (opt-in only) | Email, usage data | Consent |

# 5. Legal Basis for Processing (GDPR Article 6)

**Contract Performance (Art. 6(1)(b)):** Processing necessary to provide the Platform services — account management, task matching, payment processing, and communication features.

**Legal Obligation (Art. 6(1)(c)):** Processing required by law — identity verification for financial services, tax compliance, and responding to lawful authority requests.

**Legitimate Interests (Art. 6(1)(f)):** Processing for fraud prevention, platform security, content moderation, and improving our services, where these interests are not overridden by your rights.

**Consent (Art. 6(1)(a)):** Processing based on your explicit consent — analytics cookies, marketing cookies, and optional marketing communications. You may withdraw consent at any time without affecting the lawfulness of prior processing.

**Special Category Data (Art. 9(2)(a)):** For biometric data from selfies used for face-matching during identity verification, our legal basis is your **explicit consent**, given when you complete identity verification.

# 6. Sharing of Personal Data

## 6.1 With Other Users

When you use the Platform, certain information is visible to other users as necessary for the service:

- Your **first name** and profile photo (if uploaded) are visible on task applications and chat
- Your **ratings and reviews** are visible on your public profile
- Your **approximate location** (city level) is visible on task listings
- Tasks you have completed (count and aggregate rating)

## 6.2 With Stripe (Payment Processor)

Payments are processed by Stripe, Inc. (USA) and Stripe Payments Europe Ltd. (Ireland). We share necessary transaction data with Stripe to process payments. Stripe processes data as an independent data controller under their own privacy policy. **Root-ling does not store full payment card details.**

## 6.3 With Service Providers (Processors)

We share data with trusted third-party service providers who assist in operating the Platform:

- **Stripe Payments Europe Ltd.** (Ireland) — payment processing and identity verification
- **Cloudinary** (USA, EU servers) — media (image/video) storage
- **SendGrid / Twilio** (USA) — transactional email and SMS delivery
- **Microsoft Azure (Translator API)** (EU) — translation service
- **Vercel** and **Railway** (USA, EU regions) — hosting and infrastructure
- **Google Analytics** (subject to your cookie consent) — usage analytics

All processors are contractually bound to process data only on our instructions and in compliance with GDPR-compliant data processing agreements.

### 6.4 Legal Requirements

We may disclose personal data to competent authorities, courts, or law enforcement where required by applicable law, or to protect the rights, property, or safety of Root-ling, its users, or the public.

### 6.5 Business Transfers

In the event of a merger, acquisition, or sale of assets, your personal data may be transferred as part of that transaction. We will notify you before your data becomes subject to a different privacy policy.

We do **not** sell your personal data.

## 7. International Data Transfers

Root-ling primarily processes data within the European Economic Area (EEA). However, some service providers (including Stripe and SendGrid) may process data outside the EEA. Where data is transferred outside the EEA, we ensure appropriate safeguards are in place, including:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission
- **Adequacy decisions** by the European Commission
- Other lawful transfer mechanisms under Art. 46 GDPR

Stripe processes data in the United States under applicable data transfer frameworks. For more information, see Stripe's Privacy Policy at stripe.com/privacy. A copy of the relevant safeguards may be requested at info@root-ling.com.

## 8. Data Retention

We retain personal data only for as long as necessary for the purposes described in this policy, or as required by law:

| Data category | Retention period |
|---|---|
| Account data | Duration of account + 6 months after deletion |
| Identity verification documents (ID, selfie) | 12 months from verification, then deleted |
| Verification status flag | While the account is active |
| Transaction & payment records | 10 years (LR Buhalterin■s apskaitos ■statymas) |
| Tax-relevant records | 10 years (LR Mokes■i■ administravimo ■statymas) |
| Communication data (messages) | 24 months from last activity |
| Reviews | Indefinitely (as part of public marketplace record) |
| Usage and analytics data | Up to 26 months |
| Location data | Not stored permanently — used in real time only |
| Marketing consent records | Until consent withdrawn |
| Support tickets | 3 years |

| | |
|---|---|
| Server logs | 12 months |

When data is no longer needed, it is securely deleted or anonymised.

## 9. Your Rights Under GDPR

As a data subject under GDPR, you have the following rights:

- **Right of Access (Art. 15):** Request a copy of all personal data we hold about you.
- **Right to Rectification (Art. 16):** Request correction of inaccurate or incomplete data.
- **Right to Erasure (Art. 17):** Request deletion of your personal data, subject to legal retention obligations.
- **Right to Restrict Processing (Art. 18):** Request that we limit how we use your data in certain circumstances.
- **Right to Data Portability (Art. 20):** Request your data in a structured, machine-readable format.
- **Right to Object (Art. 21):** Object to processing based on legitimate interests or for direct marketing.
- **Right to Withdraw Consent (Art. 7(3)):** Withdraw consent at any time without affecting prior processing.
- **Rights regarding Automated Decision-Making (Art. 22):** We do not currently make solely automated decisions with legal effects, though we use automated tools for fraud detection and matching. You may request human review of any decision that significantly affects you.
- **Right to Lodge a Complaint:** Lodge a complaint with the State Data Protection Inspectorate of Lithuania (vdai.lrv.lt).

To exercise any of these rights, contact us at **info@root-ling.com**. We will respond within **30 days** as required by Art. 12 GDPR. We may need to verify your identity before processing your request.

## 10. Cookies & Tracking Technologies

We use cookies and similar technologies on our website and mobile application. A cookie consent banner is displayed on your first visit, allowing you to manage your preferences.

### 10.1 Types of Cookies

- **Necessary Cookies:** Required for the Platform to function. Always active — cannot be disabled.
- **Analytics Cookies:** Help us understand user behavior (e.g., Google Analytics). Active only with your consent.
- **Marketing Cookies:** Enable targeted advertising. Active only with your explicit consent.

### 10.2 Managing Cookies

You can manage or withdraw cookie consent at any time through the cookie settings on the Platform. You can also configure your browser to block or delete cookies. Disabling necessary cookies may affect Platform functionality.

### 10.3 Google Analytics

We use Google Analytics (Google LLC, USA) to analyze Platform usage. We have configured Google Analytics with IP anonymization and consent mode — analytics data is only collected after you provide consent. See Google's Privacy Policy at policies.google.com/privacy.

## 11. Security Measures

We implement appropriate technical and organizational measures to protect your personal data, including:

- Encryption of data in transit (HTTPS/TLS)
- Encrypted storage of passwords (bcrypt hashing)
- Access controls limiting data access to authorized personnel only
- Secure payment processing via Stripe (PCI DSS compliant)
- Regular security reviews and monitoring
- Staff confidentiality obligations

**Note:** No system can guarantee absolute security. In the event of a data breach that poses a risk to your rights, we will notify you and the relevant supervisory authority within **72 hours** as required by GDPR Article 33.

## 12. Children's Data

The Root-ling Platform is not intended for individuals under the age of 18. We do not knowingly collect personal data from minors. If you believe a minor has provided us with personal data, please contact us immediately at info@root-ling.com and we will delete the data promptly.

## 13. Marketing Communications

We send marketing communications only with your consent, which you give during registration or in account settings. Each marketing email contains an unsubscribe link. You can also withdraw consent in account settings at any time.

We may send **transactional communications** (e.g. payment receipts, Task notifications, security alerts) without separate consent, as these are necessary for performing our contract with you.

## 14. Automated Decision-Making and Profiling

We use limited automated tools for:

- matching Task Makers with Taskers based on category, location, and rating;
- detecting fraudulent activity (e.g. unusual login patterns);
- moderating content (e.g. detecting contact information in messages).

These do not produce legal or similarly significant effects on you. If a decision (e.g. account suspension following automated fraud detection) significantly affects you, you have the right to request human

review and contest the decision.

## 15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or Platform features. We will notify you of material changes by email or by displaying a prominent notice on the Platform at least **30 days** before the changes take effect.

Continued use of the Platform after changes take effect constitutes acceptance of the updated policy.

## 16. Contact Information

For any questions, concerns, or requests regarding this Privacy Policy or your personal data:

**UAB Root-ling**
Laisvės al. 85E-5, LT-44297 Kaunas, Republic of Lithuania
**Data Protection / Legal:** info@root-ling.com
**General Support:** support@root-ling.com
**Phone:** +370 622 47542
**Website:** https://www.root-ling.com

You also have the right to lodge a complaint with the Lithuanian supervisory authority:

**State Data Protection Inspectorate** (Valstybin■ duomen■ apsaugos inspekcija)
L. Sapiegos g. 17, 10312 Vilnius
Email: ada@ada.lt
Phone: +370 5 271 2804
Website: vdai.lrv.lt

*© 2026 UAB Root-ling. All rights reserved. This Privacy Policy was prepared based on the actual data flows and behavior of the Root-ling platform combined with current GDPR and Lithuanian legal frameworks. It is not a substitute for professional legal advice.*

# 17. WhatsApp Business Messaging Services

*Added in Version 3.1 (effective 28 October 2026). Sections 1–16 above are unchanged and continue to apply to the Root-ling Marketplace. This section applies only to the WhatsApp Business Messaging Services described below.*

## 17.1 What this service is

In addition to the Marketplace, Root-ling provides businesses (**Business Customers**) with software that connects their own WhatsApp Business account to the WhatsApp Business Platform (Cloud API) operated by Meta. Typical uses are an automated assistant that answers customer questions (for example about product availability) and hands the conversation over to the business's staff, and a website or catalogue that shows the business's products. People who message a Business Customer on WhatsApp are referred to as **End Customers**.

## 17.2 Who is responsible (controller and processor)

- For End Customers' data, the **Business Customer is the data controller**. Root-ling acts as a **data processor** (Article 28 GDPR) and processes that data only on the Business Customer's documented instructions, as set out in section 22 of our Terms of Service.
- For the Business Customer's own account and contact data, Root-ling is the data controller.
- WhatsApp itself is operated by Meta (WhatsApp Ireland Limited / Meta Platforms Ireland Limited), which processes message data under its own terms and privacy policy.
- If you are an End Customer, please also read the privacy notice of the business you are messaging.

## 17.3 Data we process for this service

- **End Customers:** WhatsApp phone number and profile name; message content; message metadata (time, message ID, delivery status); notes needed to hand a conversation over to the business's staff; per-customer settings set by the Business Customer (for example a discount level linked to a phone number, or that the assistant is paused for a conversation). Media messages (photos, voice notes) are passed to the business's staff and are not analysed.
- **Business Customers:** business name, contact person, email address and phone number; WhatsApp Business Account and phone number identifiers; access tokens issued by Meta (stored encrypted, never shown in plain text); the product catalogue, stock and price data the business provides; billing information.

## 17.4 Purposes

- answering End Customers' messages on behalf of the Business Customer, including searching the business's catalogue;
- handing conversations over to the Business Customer's staff when needed or requested;
- operating the Business Customer's website or catalogue pages;
- preventing duplicate processing, abuse and excessive use (for example daily usage limits);
- security, troubleshooting and technical support.

We do not use End Customers' data for our own marketing, we do not sell it, and we do not use it to train artificial intelligence models.

## 17.5 Automated replies

Replies may be generated automatically, partly with the help of an AI language model, based on the Business Customer's own catalogue and instructions. Information in automated replies (for example stock

or price) is indicative and is confirmed by the business. An End Customer can ask for a human at any time, and the conversation is then passed to the business's staff. The service does not make decisions that produce legal or similarly significant effects within the meaning of Article 22 GDPR.

### 17.6 Sub-processors

- **Meta** (WhatsApp Ireland Limited / Meta Platforms Ireland Limited) — WhatsApp Business Platform, message delivery.
- **Cloudflare, Inc.** — hosting, application runtime and database (global network).
- **Anthropic, PBC** (USA) — AI language model used for automated replies, under commercial terms that do not allow the data to be used for model training.
- **Microsoft** — only if a Business Customer chooses to load its stock file from its own OneDrive; the file is read in the Business Customer's own browser session.

Transfers outside the EEA are covered by the EU–US Data Privacy Framework where the recipient is certified, or by Standard Contractual Clauses. We inform Business Customers in advance of any new sub-processor, and they may object.

### 17.7 Retention

- conversation history used to understand follow-up messages: **7 days**, then deleted automatically;
- technical message identifiers used to avoid processing the same message twice: **3 days**;
- notes for conversations handed over to staff: **30 days**;
- catalogue, stock and per-customer settings: while the service is active;
- after the service ends: all End Customer data and access tokens are deleted within **30 days**, unless the Business Customer asks for a copy first or the law requires us to keep it.

### 17.8 Your rights and data deletion

End Customers can exercise their GDPR rights (section 9) with the business they messaged, or by writing to info@root-ling.com with their WhatsApp number and the name of the business; we will act on it together with that business. Step-by-step deletion instructions are published at **https://www.root-ling.com/data-deletion**. Data that WhatsApp itself stores (for example the chat on your phone) is controlled by Meta and can be managed in WhatsApp.

*© 2026 UAB Root-ling. Section 17 was added to describe the WhatsApp Business Messaging Services. Questions about this Policy: info@root-ling.com.*