Roksnet Privacy Notice for Services (RPN-Services)

Document code: RPN-Services
Version: 1.0
Effective date: 15.06.2026
Last updated: 15.06.2026
Publisher: Roksnet Solutions OÜ

This Privacy Notice explains how Roksnet Solutions OÜ processes personal data in connection with the Roksnet Self-Service Platform (https://app.roksnet.com) and the Roksnet Services activated through it, including the Roksnet Member Directory, Roksnet Support, and related operational components of the Roksnet Framework.

This Privacy Notice does not cover use of the public Roksnet website. Personal data processing related to the public website is described in the Roksnet Privacy Notice for the Website (RPN-Website).

Trust Services are governed by separate Trust Services documentation, which may include its own privacy disclosures.

1. Data controller

Roksnet Solutions OÜ
Business registry code: 12998179
Address: Keevise 10, 11415 Tallinn, Harjumaa, Estonia
Email: support@roksnet.com

2. Scope

This Privacy Notice applies to personal data of:

- representatives of legal entities applying to become Roksnet Members;
- Roksnet Members and their authorized users (administrators, technical contacts);
- natural persons who sign Trust Services applications on a Member's behalf (the Authorized Signatory) and other representatives named in supporting documents;
- individuals communicating with Roksnet Support in connection with Services.

The Customer or Member is a legal entity. Personal data covered by this Notice relates to natural persons acting on behalf of, or designated by, the legal entity.

3. Personal data we process

3.1 Registration and Identification data

When a legal entity applies to become a Roksnet Member, we process:

- organization name, legal name (Latin script), national registration identifier, country, organization type (Member Class), registered address, VAT number (if provided), website (if provided);
- Identification metadata: the Organization Registry Code, Registrar Organization, and Registrar Website (declared by the Customer and not independently verified by Roksnet against any register), and the Verification Method (recorded by Roksnet);
- Verification Invoice Contact details (email and phone) submitted on the registration form, used to deliver the verification invoice and instructions and, by default, recurring invoices for activated Services (the Member may update the billing contact in Account Settings);
- Administrative Contact details submitted in the bank payment description or the qualified-electronically sealed Confirmation Message: the email is used as the login email and is verified through an email confirmation step at account setup; the phone is retained as part of the Member's contact data;
- application metadata (date and time of submission, IP address, browser and device technical information);
- the Roksnet Member Code assigned to the organization at the time of form submission;
- bank transaction data (payer name, account number, payment description content) when Identification is completed via SWIFT/SEPA;
- the sealed Confirmation Message and the qualified eIDAS seal certificate data when Identification is completed via a qualified electronic seal.

3.2 Self-Service authentication and account data

When a Member uses the Self-Service Platform, we process:

- Roksnet Member Code and other assigned identifiers;
- login email (Administrative Contact email);
- password hash;
- TOTP shared secret for two-factor authentication via an authenticator application;
- authentication and session events, including technical metadata required for security and audit;
- account configuration changes and service activation events.

3.3 Member Directory operational data

When a Member uses the Member Directory Service, we process:

- Subsystem identifiers, descriptions, contact details declared by the Member;
- declared Security Server IP addresses;
- certificate metadata (issuer, validity, fingerprint) for AUTH and SIGN certificates;

- Member Directory record changes and request history.

Roksnet does not access or monitor Member-to-Member message content or payload. Processing is limited to metadata and configuration data required for Directory integrity and Service continuity.

3.3A Public Profile data

A Member may, through the Self-Service Platform Profile section, publish information about its organisation that is visible to other Roksnet Members for business inquiry and discovery purposes. This information includes:

- general contact email of the organization;
- general contact phone of the organization;
- legal address of the organization;
- website of the organization;
- organization description;
- organization logo.

The Public Profile is intended for organisational data of the legal entity (for example, a general organisation email or a general organisation phone number). Roksnet Membership is open only to legal entities, not to natural persons or sole proprietors; the legal address is the organisation's registered or contact address, published as organisational data. Submission of personal data of individual employees or other natural persons (for example, a personal email or personal mobile number identifying a specific individual) is prohibited by the Roksnet Acceptable Use Policy (AUP §3). To the extent any personal data is nonetheless present in a field the Member chose to publish, Roksnet processes it as data controller on the basis of Article 6(1)(f) GDPR (legitimate interest in the operation of the Member Directory) and the Member's choice to publish it; data subjects may exercise the rights set out in §10.

The Member may update or remove, at any time through Account Settings, the Public Profile fields it provided and that Roksnet does not validate: legal address, general contact email, general contact phone, organisation description, organisation logo, and website. Other directory fields originate from the Identification process or the X-Road central server (Member Name, Member Code, Member Class, Country, Trust Service Provider, and other verification data) and are not editable by the Member; the fields that cannot be hidden from the directory are set out in DST §3.3.

3.3B Visibility tiers and recipients

Member Directory data is published at two levels:

- Mandatory registry data (Tier 1) - Member Name, Member Code, and Member Class - is published in the X-Road central registry and is visible to all X-Road participants (other Members) via their Security Servers. It is required for X-Road communication and cannot be hidden while the Member is active. Registered Subsystems become visible through the central-registry configuration; API and data-service information may be discoverable

separately (X-Road metadata mechanisms or Roksnet's separate display function). These identifiers relate to the legal entity, not to a natural person.

- Public Member profile (Tier 2) - visible to other Roksnet Members - comprises the identity data above together with Country, Member Since, status, and environment, the verification data (Organization Registry Code, Registrar Organization, Registrar Website, Verification Method, Trust Service Provider), and the Member-provided contact data (general contact email, general contact phone, legal address, website, organization description, organization logo). The Member may hide from search the parts of its profile other than the fields that cannot be hidden - Member Name, Member Code, Member Class, Country, and Trust Service Provider (see DST §3.3).

The recipients of this published data are other Roksnet Members and X-Road participants. Roksnet does not otherwise disclose Member Directory data except as set out in §6 (Recipients and service providers).

3.4 Support data

When a Member interacts with Roksnet Support, we process:

- the content of email enquiries, attachments, and Roksnet replies;
- the content of AI Support (GPT Assistant) chat sessions, including questions submitted by the user and responses produced by the AI provider;
- contact details associated with the support interaction;
- communication metadata (date, time, channel).

Members are advised not to submit unnecessary personal data, credentials, cryptographic keys, or third-party confidential data through support channels.

3.5 Operational security logs

We process technical and security logs generated by the Self-Service Platform and the Member Directory, including:

- IP addresses, timestamps, request metadata;
- security events, anomaly detection signals, rate-limiting records;
- error and diagnostic logs.

3.6 Trust Services application data

When a Member applies for Roksnet Trust Services through the Self-Service Platform, we process the personal data of the Authorised Signatory — the natural person who signs the Trust Services Application on the Member's behalf (who may be a different person from the Administrative Contact):

- full name;
- position or title;
- email address;
- phone number;
- signature (digital or handwritten) and signing metadata (date and place);

- the signed application document and the Organization Registration Document submitted in support of the application.

This data is processed to handle the Trust Services application and to maintain the acceptance and audit record required for the provision of Trust Services. It is internal application and audit data and is not published in the Member Directory. Personal data processing related specifically to issued certificates and ongoing Trust Services operation may be described in further detail in the Trust Services documentation.

4. Purposes and legal bases

We process personal data for the following purposes and legal bases under the GDPR:

- Handling Membership applications, completing Identification, and entering into the service relationship:

Legal basis: Article 6(1)(b) (performance of a contract or steps prior to entering a contract).

- Providing the Self-Service Platform and activated Services (Member Directory, Support):

Legal basis: Article 6(1)(b) (performance of a contract).

- Handling Roksnet Trust Services applications:
- Authorized Signatory personal data (a natural person signing on the Member's behalf): Legal basis Article 6(1)(f) (legitimate interests — reviewing the submitted evidence of the signatory's authority and assessing apparent authority to bind the Member, maintaining the acceptance and audit record, and establishing, exercising, or defending legal claims). The contract is with the Member (a legal entity); the signatory is not a party to it, so Article 6(1)(b) is not relied upon for the signatory's personal data.
- Supporting documents (the Organization Registration Document and the signed application), to the extent they contain personal data of the Member's representatives: Legal basis Article 6(1)(f) (legitimate interests — validating the Member, maintaining the application and audit record, and establishing, exercising, or defending legal claims). Article 6(1)(c) (legal obligation) applies in addition only where a specific legal provision requires retention.
- Authentication, account security, and abuse prevention:

Legal basis: Article 6(1)(f) (legitimate interests).

- AI Support (GPT Assistant) processing of user-submitted content:

Legal basis: Article 6(1)(b) (performance of a contract) or Article 6(1)(f) (legitimate interests), depending on context. Where the AI Support channel is offered as an optional alternative to human support, an additional confirmation may be collected from the user before the channel is activated.

- Operational security, integrity, and incident response:

Legal basis: Article 6(1)(f) (legitimate interests).

- Compliance with legal and regulatory obligations:

Legal basis: Article 6(1)(c) (legal obligation).

- Establishment, exercise, or defense of legal claims:

Legal basis: Article 6(1)(f) (legitimate interests), and Article 9(2)(f) where applicable.

5. Legitimate interests pursued

Where processing is based on Article 6(1)(f), our legitimate interests include:

- maintaining the integrity, security, and continuity of the Self-Service Platform and Services;
- operating the Member Directory, including registering and publishing Members' organizational data to enable discovery and the establishment of connections between Members;
- reviewing the submitted evidence of an Authorized Signatory's authority and assessing apparent authority to bind the Member, reviewing Trust Services applications and their supporting documents, and maintaining the related acceptance and audit record;
- preventing fraud, abuse, and unauthorized access;
- providing efficient support to Members;
- protecting Roksnet's legal rights and managing claims.

6. Recipients and service providers

We may share personal data with:

- hosting, infrastructure, and IT service providers operating Roksnet platforms;
- the AI Support provider (currently OpenAI), under the AI provider's applicable data processing terms, for the processing of AI Support chat sessions when that channel is used;
- cybersecurity, anti-abuse, and technical support providers;
- payment infrastructure providers in connection with Identification and billing;
- professional advisers (legal, audit, compliance) where necessary;
- public authorities where required by law.

Service providers act under contractual instructions and appropriate confidentiality and security obligations.

7. International data transfers

Personal data is processed primarily within the EEA. Where personal data is transferred outside the EEA, we apply lawful transfer mechanisms under GDPR Chapter V, including:

- adequacy decisions where applicable; or
- Standard Contractual Clauses under Article 46 with supplementary safeguards as required.

In particular, where the AI Support channel is used, the AI provider may process data outside the EEA, including in the United States, depending on the provider's configuration. Where such a transfer occurs, it is made under an appropriate safeguard (for example, Standard Contractual

Clauses) or an adequacy decision, complemented by Roksnet's data-minimisation guidance and the user notice provided before the channel is activated.

8. AI Support channel - additional information

Roksnet may offer an AI Support channel (GPT Assistant) within the Self-Service Platform. The AI Support channel is an AI system within the meaning of Article 3 of Regulation (EU) 2024/1689 (EU AI Act) and is subject to the transparency obligations of Article 50 of that Regulation. By using the AI Support channel, the user acknowledges interaction with an automated system.

The AI Support channel:

- does not make legally or similarly significantly affecting decisions;
- does not perform biometric identification;
- does not operate in a high-risk domain as defined under the EU AI Act.

Before the AI Support channel can be used, the user is informed that:

- queries may be processed by the AI provider (OpenAI) outside the EEA, depending on the provider's configuration;
- any transfer outside the EEA is made under an appropriate safeguard (for example, Standard Contractual Clauses) or an adequacy decision;
- the user should not submit unnecessary personal data, credentials, cryptographic keys, or third-party confidential data;
- human Support remains available as an alternative channel.

Use of the AI Support channel may be discontinued by the user at any time by switching to human Support.

9. Retention

We retain personal data only for as long as necessary for the relevant purpose:

- accounting-relevant records within the application and Identification data (payment and transaction records and the data needed to evidence the transaction): retained for seven years from the end of the relevant financial year, as required by the Estonian Accounting Act §12 and tax law (Article 6(1)(c)); invoices fall under the "invoices and accounting records" item below;
- Identification evidence (the data establishing who entered into the Agreement and on what basis): retained for the duration of the Membership and thereafter for the period necessary to establish, exercise, or defend legal claims (Article 6(1)(f)), and no longer than required for that purpose;
- other registration and application data not needed for the purposes above: retained for the duration of the Membership and deleted when no longer necessary; it is not retained on accounting grounds;

- application data of Customers whose application is cancelled (Identification not completed within the deadline): deleted promptly after cancellation, except where retention is required by law. The Member Code is archived and is not reassigned to a different organization for at least six months;
- Self-Service authentication and account data: for the duration of the Membership; authentication event logs up to 12 months unless longer retention is required for security investigation or legal compliance;
- Member Directory public record (public profile, listing): removed from the Member Directory on cancellation or termination; not retained as a public record thereafter. A Member Code that has identified an active Member is permanently retired and is not reassigned (it remains referenced in audit and message logs, certificates, and other Members' records); the six-month reuse rule applies only to Member Codes from applications that were never activated;
- Member Directory operational and configuration data (Security Server, Subsystem, and API registrations and change history): for the duration of the relevant record and for a limited period after deactivation (up to 12 months) for audit and continuity purposes;
- invoices and accounting records: for seven years from the end of the financial year, as required by the Estonian Accounting Act §12 and tax law;
- evidence of acceptance and of the contractual relationship (for example, acceptance logs): for the period necessary to establish, exercise, or defend legal claims, and in any event no longer than required for that purpose;
- on cancellation or termination, and on deletion of the Self-Service account, Roksnet does not retain the Member's data in full: it retains only the categories listed in this §9, each for its stated period and purpose;
- the signed Trust Services Application (acceptance evidence): retained for the period necessary to establish, exercise, or defend legal claims and to maintain the acceptance and audit record (Article 6(1)(f)), and no longer than required for that purpose; any accounting-relevant document follows the accounting-records item above;
- Authorized Signatory contact data (name, position, email, phone): retained for the duration of the Trust Services relationship and a limited period thereafter; where the same data also forms part of the signed acceptance evidence, that copy follows the acceptance-evidence retention above;
- the Organization Registration Document: retained for the duration of the Trust Services relationship and for the statutory recordkeeping period where applicable;
- Email Support communications: up to 90 days after the interaction, unless retention is required for active disputes, investigations, or legal compliance;
- AI Support chat content: retained by the AI provider only for as long as necessary and in accordance with the AI provider's applicable data processing terms and Roksnet's configuration; anonymized excerpts may be retained by Roksnet for up to 6 months for service improvement; no profiling or automated decision-making is conducted based on chat content;
- Operational security logs: up to 12 months, unless longer retention is required to investigate or document a security incident or to comply with law.

10. Your rights

Subject to GDPR and applicable law, the data subject has the right to:

- request access to personal data;
- request rectification of inaccurate data;
- request erasure of data, subject to retention obligations;
- request restriction of processing;
- object to processing based on legitimate interests;
- request data portability where applicable;
- withdraw any optional confirmation given for the AI Support channel at any time, without affecting prior processing.

Requests may be submitted to support@roksnet.com. Roksnet may request additional information to verify the identity of the requester and the legitimacy of the request.

The data subject has the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon): https://www.aki.ee/en.

11. Whether providing data is mandatory

Provision of registration and Identification data is required to enter into the service relationship and to provide the Services. Without this data, Roksnet cannot establish Membership or provide access to the Self-Service Platform or activated Services.

Provision of support content is voluntary; without it, Roksnet cannot respond to the request.

12. Automated decision-making

Roksnet does not use personal data covered by this Privacy Notice for automated decision-making producing legal or similarly significant effects within the meaning of GDPR Article 22.

13. Security

Roksnet applies reasonable technical and organisational measures to protect personal data, including:

- role-based access controls;
- encryption in transit;
- authentication and session security;
- logging and internal access control measures;
- limited retention periods;
- contractual safeguards with service providers.

14. Relationship with other Roksnet documents

This Privacy Notice applies in parallel with the Roksnet General Terms and Conditions (RGT), the applicable Annexes (RSST, DST, RPP), and the Roksnet Acceptable Use Policy (AUP). Capitalised terms used in this Privacy Notice have the meanings set out in the Roksnet Terminology and Definitions (RTD), unless expressly stated otherwise.

Member's responsibility under local law. Roksnet processes personal data as set out in this Privacy Notice on the basis of Estonian and European Union law. The Member is responsible for compliance with the data-protection and other laws applicable to it (see RGT §14.3) in respect of the personal data it publishes in the Member Directory and the data it exchanges with other Members through the Roksnet Framework. For Member-to-Member data exchange, Roksnet is not in the data path and does not access its content or payload (§3.3); the Member determines the purposes and means of that exchange and acts as the controller for it; where the Member instead processes personal data on behalf of and on the documented instructions of another controller, it acts as a processor for that controller (and not as the entity determining the purposes and means). Where a law applicable to the Member prohibits, restricts, or imposes additional or stricter requirements on such processing, the Member must comply with that law and, where required, cease the affected use (RGT §14.4).

Personal data processing related to the public Roksnet website is described in the Roksnet Privacy Notice for the Website (RPN-Website).

15. Changes to this Privacy Notice

Roksnet may update this Privacy Notice from time to time. Material adverse changes will be communicated to Members at least 30 days before they take effect. Other changes take effect upon publication. The latest version is published on the Self-Service Platform and on the Roksnet website.

Contact:
Roksnet Solutions OÜ
Email: support@roksnet.com