Roksnet General Terms and Conditions (RGT)

Document code: RGT
Version: 1.0
Effective date: 15.06.2026
Last updated: 15.06.2026
Publisher: Roksnet Solutions OÜ

1. Introduction and Scope

These Roksnet General Terms and Conditions ("RGT") govern the legal relationship between Roksnet Solutions OÜ ("Roksnet") and any legal entity that applies to use or uses Roksnet Services ("Customer" or "Member"). These RGT apply to all Roksnet Services activated through the Self-Service Platform.

The Roksnet Services are available only to legal entities having separate legal personality. They are not available to natural persons, sole proprietors, or other unincorporated undertakings.

Trust Services are governed by separate Trust Services documentation. The provision and use of Trust Services are subject to that documentation.

Capitalised terms used in these RGT have the meanings set out in the Roksnet Terminology and Definitions (RTD), unless expressly stated otherwise.

2. Acceptance and Conclusion of the Agreement

2.1 Customer's offer and acceptance of terms

A legal entity wishing to use Roksnet Services submits the registration form on the Self-Service Platform (https://app.roksnet.com). By submitting the form, the legal entity:

- becomes a Customer;
- accepts these RGT, the applicable Annexes, and the Roksnet Acceptable Use Policy (AUP), and acknowledges having read the Roksnet Privacy Notice for Services (RPN-Services);
- makes an offer to Roksnet to enter into the Agreement, conditional upon successful Identification.

Upon receipt of the form, Roksnet automatically issues an invoice for the Identification fee or, where the Customer chooses a qualified-electronically sealed Confirmation Message, provides the sealing template and instructions. Issuance of the invoice or template is a procedural step and does not constitute acceptance by Roksnet.

2.2 Roksnet's acceptance via Identification

The Customer completes the Identification procedure (SWIFT/SEPA payment or qualified-electronically sealed Confirmation Message) as set out in the Roksnet Self-Service Terms (Annex A).

Roksnet verifies the Identification (including the consistency of data between the registration form and the Confirmation Message). Successful Identification constitutes Roksnet's acceptance of the Customer's offer, and the Agreement is concluded at this point (subject to §3.3, which governs authority and ratification where the person who registered lacked authority to bind the entity); the Customer becomes a Member, and Membership is activated.

Where Identification fails (for example, due to data mismatch, banking compliance issues, or invalid eIDAS certificate), the Agreement is not concluded. Fees applicable to re-identification are set out in Annex A.

2.3 Acceptance Confirmation at first login

After Identification and successful Account Setup (password creation, email verification, two-factor authentication setup), the Member is presented with an explicit Acceptance Confirmation step in the Self-Service Platform. The Acceptance Confirmation lists the currently applicable versions of these RGT, the Annexes, the RPN-Services, and the AUP, each with a link to the published version. By confirming, the Administrative Contact, acting on the Member's behalf through the authenticated Member Account established at Account Setup, expressly accepts these RGT, the Annexes, and the AUP on behalf of the Member, and acknowledges having read the RPN-Services. Roksnet does not verify the identity of the natural person operating the Account (see §3.3); the confirmation is bound to the authenticated Member Account, not to a verified natural-person identity.

The Acceptance Confirmation event is logged with timestamp, user identifier, Member Code, and document versions. It serves as a strong authenticated account-bound acknowledgement and audit-trail entry. It does not constitute a new contract — the Agreement is concluded at successful Identification per §2.2 and remains in effect from that point; however, where it is given by a person with authority to bind the Member and with knowledge of the registration, it may also operate as ratification under §3.3. Access to the Self-Service Platform Dashboard is granted upon completion of the Acceptance Confirmation.

2.4 Modular activation of Services

Membership alone does not constitute use of any specific Service. Each Service is activated separately by the Member within the Self-Service Platform. A Service is considered active only upon explicit activation by the Member.

Activation of Trust Services is subject to a separate acceptance procedure within the Self-Service Platform. Prior to the first use of Trust Services, the applicable Trust Services documentation is presented to the Member for acceptance, regardless of the integration of the Trust Services interface within the Self-Service Platform.

3. Contracting Parties

3.1 Parties

- Roksnet Solutions OÜ - the operator and provider of Roksnet Services.
- Customer - a legal entity that has submitted a registration form, has been assigned a Roksnet Member Code, and has not yet completed Identification.
- Member - a legal entity that has completed Identification, at which point Membership is activated.

The Roksnet Member Code is assigned upon submission of the registration form and serves as the organisation's public identifier within the Roksnet Framework. Assignment of the Member Code does not, by itself, activate Membership.

3.2 Privacy and Acceptable Use

Personal data processing in connection with the Self-Service Platform and Roksnet Services is described in the Roksnet Privacy Notice for Services (RPN-Services). The RPN-Services applies in parallel with these RGT and the Annexes.

Rules for acceptable use of the Self-Service Platform and Roksnet Services are set out in the Roksnet Acceptable Use Policy (AUP), which applies in parallel with these RGT and the Annexes.

Personal data processing related to the public Roksnet website is described separately in the Roksnet Privacy Notice for the Website (RPN-Website) and is not covered by the RPN-Services.

3.3 Authority and Corporate Action

The Member acts through its legal representative or persons duly authorised by the legal representative. Subject to the provisions on conclusion of the Agreement and on fraud set out below, any action performed after conclusion of the Agreement via the Roksnet Self-Service Platform or any Roksnet Service using the Member's registered credentials, contacts, or other access means is attributed to the Member and is binding on the Member, subject to mandatory applicable law.

The Member is solely responsible for:

- ensuring that only persons authorized by its legal representative have access to the Self-Service Platform and the Member's credentials;
- managing internal allocation of authority, roles, and access among its personnel;
- the consequences of actions performed by such persons in connection with Roksnet Services.

Roksnet does not verify the identity of individual natural persons operating on the Member's behalf and relies on the Member's internal authority arrangements.

Declaration of authority. By submitting the registration form, completing Identification, and using the Roksnet Services, the Member declares and warrants that the decision to enter into the Agreement, and all statements, seals, payments, and other acts performed in connection with registration and Identification, were made by a person duly authorised to act for and bind the Member. Roksnet does not require the Member to identify that person and does not request that information.

No verification of authority. Roksnet does not verify the authority of any person against any public register or by any other means, and does not undertake to do so. A Customer or Member that requires such verification should not use the Roksnet Services.

Ratification. Where registration or Identification was carried out without authority, the Agreement may be ratified by the entity - by its legal representative, or a person with actual authority to bind it, acting on the entity's behalf and with knowledge of the material circumstances of the earlier act. Ratification may be express or result from conduct that unequivocally treats the Agreement as the entity's own (for example, authorised use of the Services or payment of invoices by such a person). Continued use of the disputed credentials by the same unauthorised person does not, by itself, constitute ratification.

Conclusion of the Agreement (who is bound). The Agreement is concluded with the Member only where the person who registered and completed Identification had actual or apparent authority to bind the entity, or where the entity subsequently and validly ratifies it (see "Ratification" below). Where the person had no such authority and the entity does not ratify, no Agreement binds that entity. Roksnet does not verify authority and relies in good faith on the registration, the Identification, any qualified electronic seal, and the payment; to the fullest extent permitted by applicable law it is not liable for having so relied.

Post-conclusion account activity and security. Once the Agreement is concluded, actions performed through the Member's credentials, contacts, account, or access means are attributed to the Member, whether or not internally authorised; and where misuse was made possible by the Member's failure to meet its security obligations (§8) (for example, credentials, contacts, bank account, or access means that the Member did not adequately protect and that were then misused), the resulting acts and the associated risk are the Member's.

Fraudulent registrant acting for itself. Where the registrant is a real party acting for itself but engages in fraud, misrepresentation, or deceptive conduct (for example, an entity established or used in order to deceive other Members), the Agreement binds that registrant, which alone is responsible for its conduct; Roksnet does not warrant the honesty, legitimacy, or suitability of any Member, is not liable to any deceived Member or third party, and may suspend or terminate under §12 and the AUP.

No genuine party - external fraud, impersonation, or forgery. Where registration or Identification was carried out by a person with no connection to the Member and not enabled by any failure of the Member to meet its security obligations (genuine external fraud), where a person impersonates another existing entity, or where seals or documents are forged, no Agreement

binds the purported or impersonated entity unless and until the act is validly ratified by a person duly authorised to act for that entity. Roksnet acts in good-faith reliance on the registration, the Identification (including any qualified electronic seal), and the payment, and to the fullest extent permitted by applicable law is not liable for having so relied. A qualified electronic seal benefits from the presumption of the integrity of the data and of the correctness of the origin of that data under eIDAS Article 35(2). The seal, by itself, does not prove the internal corporate authority of any person to bind the entity.

Common provisions. Roksnet does not verify internal corporate authorisation and does not warrant to any person the identity, authenticity, authority, honesty, or suitability of any Member; each Member is responsible for verifying its counterparty before exchanging data with it (see Annex B / DST §4). As between Roksnet and the Member, the Member releases and waives any claim of its own, and shall indemnify and hold Roksnet harmless against any claim by a third party (including another Member), arising from any lack or excess of authority, fraud, forgery, impersonation, misrepresentation, or any other form of deception in connection with the Member or its registration, Identification, account, or use of the Services. Roksnet gives no warranty or assurance to, and assumes no responsibility or duty of care towards, any person (whether a Member or not) who relies on a registration, an Identification, a qualified electronic seal, or a Member Directory listing; any such reliance is at that person's own risk. To the fullest extent permitted by applicable law, Roksnet is not liable to any party for loss arising from such matters. Nothing in this section excludes or limits any liability that cannot be excluded or limited under mandatory applicable law (for example, Roksnet's own intentional or grossly negligent failure).

4. Annexes and Integration

4.1 Annexes

The following documents form Annexes to these RGT and constitute an integral part of the Agreement between Roksnet and the Member:

- Annex A - Roksnet Self-Service Terms (RSST)
- Annex B - Roksnet Member Directory Service Terms (DST)
- Annex D - Roksnet Pricing Policy (RPP)

4.2 Effect of Annexes

The Annexes apply together with these RGT. By accepting these RGT and the applicable Annexes at registration, the Member commits to the terms of all Annexes as the contractual framework. The operational provisions of an Annex governing a specific Service take effect only upon activation of that Service. Acceptance at registration does not create an obligation to activate any specific Service.

Where a Service covered by the RPP is activated by the Member within the Self-Service Platform and that Service carries fees, the Member's confirmation of activation constitutes

acceptance of the fees applicable to that Service as set out in the Roksnet Pricing Policy (RPP — Annex D) at the time of activation, and authorises Roksnet to issue invoices for those fees. Fees for Trust Services are governed by the separate Trust Services documentation, not by the RPP. Each Service is activated and billed separately.

5. General Principles

Roksnet Services must be used solely for lawful purposes and in accordance with these RGT, the applicable Annexes, published policies, and operational instructions. Members are responsible for the secure management of credentials and for the lawful use of Services by their authorised users.

6. Communication and Notification

6.1 Communication channels

Official communication from Roksnet is sent through the Self-Service Platform or to the contact email designated by the Member. Members must maintain accurate contact details and monitor the designated channels. Notices sent to the last known address are deemed delivered.

6.2 Language

These RGT and all Roksnet service documents are issued in English.

6.3 Character set

All statements, forms, and certificate fields processed through Roksnet must use the Latin alphabet (A-Z, 0-9, standard punctuation). Non-Latin characters (diacritics, accents, Cyrillic, and similar) are not accepted in legal identifiers or certificate fields.

7. Confidentiality

Customers and Members must treat all non-public information obtained through Roksnet Services as confidential and must comply with applicable confidentiality and data-protection obligations.

Roksnet, in turn, treats non-public information it receives from a Customer or Member - through applications, the Self-Service Platform, and Support - as confidential, and uses it only to provide and administer the Roksnet Services and as described in the RPN-Services, subject to disclosures required by law or made to professional advisers and service providers bound by confidentiality obligations. This mutual obligation does not apply to information that is or becomes public other than through a breach of this section, that the receiving party already lawfully held, or that it independently develops. The obligations in this section survive termination of the Agreement for three years, and for any trade secret for as long as it remains a trade secret.

8. Security Obligations

8.1 General principle

The Member is responsible for ensuring the highest reasonably achievable level of security for all systems, accounts, credentials, devices, and infrastructure used to access or operate Roksnet Services. The Member must apply industry-standard security controls, including access management, encryption, patching, monitoring, and incident response.

8.2 Scope of Member's security obligations

The obligation set out in §8.1 extends to, without limitation:

- the Administrative Contact email account and any other email used in connection with Roksnet Services;
- authentication credentials and any tools or devices used to manage them;
- end-user devices (workstations, mobile devices, browsers) used to access the Self-Service Platform or Roksnet Services;
- network and remote-access infrastructure used to reach Roksnet Services;
- Security Servers operated by the Member in connection with the Member Directory Service (detailed obligations are set out in Annex B);
- AUTH and SIGN certificates and their associated cryptographic keys, hardware security modules, and key-protection mechanisms (detailed obligations are set out in the applicable Trust Services documentation);
- any other system or asset whose compromise could affect the Member's use of Roksnet Services or the security of other Members.

8.3 Operational duties

The Member must:

- limit access to the assets listed in §8.2 to specifically authorized persons under the principles of least privilege and need-to-know;
- promptly revoke access upon personnel changes or upon suspected compromise;
- maintain organizational procedures for managing security incidents;
- promptly notify Roksnet of any actual or suspected compromise that may affect Roksnet Services or related credentials.

Detailed operational rules for credentials and the Self-Service Platform are set out in the Roksnet Acceptable Use Policy (AUP §4) and in Annex A (RSST §3). Service-specific security rules are set out in the corresponding Annexes.

8.4 Roksnet's position

Roksnet maintains its own security systems for the Self-Service Platform and Roksnet Services. Roksnet is not liable for breaches, losses, or unauthorised actions resulting from the Member's failure to meet the obligations set out in this §8 or from vulnerabilities within the Member's environment.

9. Prohibited Use

It is prohibited to:

- use Roksnet Services for unlawful purposes;
- attempt to gain unauthorized access to systems, accounts, or data;
- provide false or misleading information;
- interfere with the availability, integrity, or security of Roksnet Services;
- use automation, bots, or scraping against Roksnet Services without explicit permission.

10. Limitation of Liability

To the fullest extent permitted by applicable law, Roksnet is not liable for damages, losses, costs, or claims arising from the use of or inability to use Roksnet Services, including any indirect, special, incidental, punitive, or consequential damages such as loss of business, profits, data, reputation, or opportunity.

Nothing in these RGT excludes or limits any liability that cannot be excluded or limited under mandatory applicable law.

11. Amendments

Roksnet may amend these RGT and the Annexes. Material adverse changes will be communicated to Members at least 30 days before they take effect. Other changes take effect upon publication.

Continued use of Roksnet Services after changes take effect constitutes acceptance of the amended documents. A Member that does not wish to accept a material adverse change may terminate the affected Service or the Agreement before the change takes effect (see §12).

12. Suspension and Termination

Roksnet may suspend or terminate access to the Self-Service Platform or any Service in cases of:

- material breach of these RGT, an Annex, or applicable law;
- security concerns;
- non-payment, in accordance with the procedures set out in the relevant Annex;
- account dormancy, as set out below;
- a prohibition, restriction, or additional or conflicting legal requirement under a jurisdiction applicable to the Member or to the provision of the Services to it, as set out in §14.5;
- termination of the Membership for other reasons set out in the Annexes or applicable law.

Account dormancy: an account that has no activated Service and shows no operational activity for 90 days following Identification may be treated as dormant. Roksnet may suspend a dormant account, and subsequently close it, only after giving the Member prior notice and a reasonable

opportunity to keep the account active. This does not oblige the Member to activate any specific Service (see §4.2); it addresses accounts that remain entirely unused.

Member-initiated termination: The Member may terminate the Agreement at any time by closing its Member Account - through the Self-Service Platform or by written request to support@roksnet.com. Separate deactivation of individual Services beforehand is not required; closing the Member Account terminates the Agreement and cancels all Services together. Roksnet first verifies that the request genuinely comes from the Member (as for cancellation under the applicable Annex). Where the request is verified and processed, termination takes legal effect on the date of processing - the Agreement, the Member's general status in the Roksnet Framework, account access, and all Services end then; until then they remain in effect. Under the whole-calendar-month billing rule (applicable Annex), the calendar month in which the closure request is made is the last month charged, regardless of the processing date, and no pro-rata refund applies. Where the request is withdrawn by the Member, or its authenticity cannot be verified, no termination takes effect and no billing cut-off applies. This Agreement-level termination is distinct from cancelling an individual Service (for example, Member Directory cancellation under Annex B §7.1), which ends only that Service and leaves the Member Account and other Services in place; the Service-specific unwinding procedures in the relevant Annexes continue to apply.

Termination on amendment: Where Roksnet notifies a material adverse change under §11, the Member may, instead of accepting it, terminate the affected Service or the Agreement by notice given before the change takes effect. In that case the existing terms continue to apply until termination takes effect, and the Member is not charged beyond the whole-calendar-month billing rule.

Specific suspension and termination procedures applicable to individual Services are set out in the relevant Annexes.

13. Hierarchy and Interpretation

13.1 Conflict resolution within the service package

In case of conflict between documents in the service package, the following order applies:

(a) mandatory applicable law;

(b) the applicable Annex - for matters within its specific scope;

(c) these RGT - for matters not covered by an Annex or where the Annex defers to these RGT;

(d) operational policies and technical instructions.

13.2 Trust Services

The Trust Services documentation prevails over these RGT and any Annex only in relation to the provision and use of Trust Services. It does not affect any Service that the Member has not activated.

13.3 Website documents

The Roksnet Site Terms, the Roksnet Privacy Notice for the Website, and the Roksnet Cookie Notice apply only to use of the public Roksnet website and do not govern Services.

14. Governing Law, Jurisdiction, and Cross-Border Use

14.1 Governing law and jurisdiction

These RGT are governed by the laws of the Republic of Estonia. Disputes arising from or in connection with these RGT are subject to the exclusive jurisdiction of Harju County Court (Harju Maakohus), unless mandatory law provides otherwise.

14.2 Place of provision

Roksnet provides the Roksnet Services from Estonia and on the basis of Estonian and European Union law. The Services are designed and operated to comply with that legal framework. Regardless of the country in which the Customer or Member is established, resident, or carries on business, the Agreement remains governed by Estonian law, and Roksnet does not adapt the Services to, or assess them against, the law of any other jurisdiction.

14.3 Member's responsibility for local law

The Customer or Member is solely responsible for ensuring that its access to and use of the Roksnet Services is lawful under every law applicable to it, including the law of any jurisdiction in which it is established, resident, or carries on business. This includes, without limitation, local data-protection and data-localisation requirements, confidentiality and professional-secrecy rules, export-control and sanctions regimes, and any sector-specific or licensing requirements. Roksnet does not monitor, advise on, or warrant compliance with the law of any jurisdiction other than Estonia and the European Union.

14.4 Duty to cease use

If any law applicable to the Customer or Member prohibits or restricts its use of the Roksnet Services, or prohibits or restricts Roksnet's provision of the Services to it, the Customer or Member must cease using the affected Services. The Customer or Member must notify Roksnet promptly upon becoming aware of any such prohibition or restriction.

14.5 Roksnet's right to suspend or terminate

Where Roksnet becomes aware that a law applicable to the Customer or Member, or to the provision of the Services to it, (a) prohibits or restricts the Services, or (b) imposes on Roksnet additional, stricter, or conflicting requirements beyond those of Estonian and European Union

law, this constitutes grounds for Roksnet to suspend or terminate the affected Services or the Agreement immediately and unilaterally. To the fullest extent permitted by applicable law, Roksnet incurs no liability to the Customer or Member for exercising this right. Roksnet will notify the Member of such suspension or termination. This right is in addition to the suspension and termination rights in §12.

14.6 No assumption of foreign-law obligations

Nothing in the Agreement constitutes Roksnet submitting to the jurisdiction of, or assuming obligations under, the law of any country other than Estonia (together with European Union law as applicable in Estonia). To the fullest extent permitted by applicable law, Roksnet is not liable for any loss, penalty, fine, or claim arising from the Customer's or Member's use of the Services being unlawful or restricted under any law applicable to the Customer or Member.

Contact:

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