Roksnet Member Directory Service Terms (DST)

Annex B to the Roksnet General Terms and Conditions

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

These Member Directory Service Terms form Annex B to the Roksnet General Terms and Conditions ("RGT") and constitute an integral part of the Agreement between Roksnet Solutions OÜ ("Roksnet") and the Member. In case of conflict, these Terms prevail within their specific scope. Capitalised terms have the meanings set out in the Roksnet Terminology and Definitions (RTD), unless expressly stated otherwise.

1. Purpose and Scope

This Annex governs the Roksnet Member Directory Service — the central registry of the Roksnet Framework. Through the Member Directory Service, Roksnet:

- registers the Member's organization in the Member Directory and makes it discoverable to other Roksnet Framework Members;
- enables registration and listing of the Member's Security Servers;
- enables registration and listing of the Member's Subsystems;
- enables publication and discovery of the Member's APIs and data services;

and thereby allows the Member to participate in secure X-Road based data exchange with other Members.

Personal data processing in connection with the Member Directory Service is described in the Roksnet Privacy Notice for Services (RPN-Services). Acceptable use is governed by the Roksnet Acceptable Use Policy (AUP). Fees are set out in the Roksnet Pricing Policy (RPP — Annex D).

What you are using, and what you buy from Roksnet. Data exchange in the Roksnet Framework runs on X-Road — a mature open-source data-exchange technology managed and developed by NIIS and deployed in national, public-sector, and other organisational ecosystems worldwide. It is used for secure data exchange between organisations, including between government institutions themselves (such as ministries and national registries) and between organisations more broadly. You use this technology yourself to exchange data directly and securely with your own counterparties. What you buy from Roksnet are the services needed to organise that exchange: Membership in the Member Directory (your presence in the central registry); the

listing of your Security Servers and Subsystems in the Member Directory, so that you are recognised in the Framework and other Members can find and connect to you; and, where you choose it, Trust Services. The Security Server software itself — and its installation, configuration, access management, security, and day-to-day operation — you carry out yourself, in accordance with the X-Road licence, the X-Road documentation, and the X-Road technology (the X-Road core software is managed and developed by NIIS and published under the MIT License — see §5.1). The data exchange then takes place directly between your Security Server and your counterparty's, over X-Road; it does not pass through Roksnet (see §5.4).

Roksnet Services and the Member's own systems — responsibility boundary. The Roksnet Service under this Annex is the Member Directory: the central registry that registers and lists the Member, its Security Servers, and its Subsystems, and makes them discoverable. Roksnet may additionally display API and data-service information obtained from Members or through X-Road metadata mechanisms; this display is a separate Roksnet function and is not part of the X-Road central-registry records. The Security Servers, the Subsystems, the Member-to-Member data exchange, and the APIs and data services that a Member publishes or consumes are NOT Roksnet Services: they are installed, configured, operated, controlled, and used by the Member and its counterparties on their own infrastructure. Registering or listing any of them in the Member Directory does not make Roksnet the operator or provider of those systems, or the controller of the Member-to-Member data exchanged through them, and does not transfer responsibility for them to Roksnet. This does not affect Roksnet's controller role for personal data that it processes in operating the Member Directory, as described in the RPN-Services. To the fullest extent permitted by applicable law, Roksnet is not responsible or liable for any loss, damage, or other negative consequence arising from the installation, configuration, operation, use, availability, security, integrity, or content of any Security Server, Subsystem, data exchange, or API or data service — whether or not it is registered in the Member Directory. This does not exclude any liability that cannot be excluded under mandatory applicable law (for example, Roksnet's own intentional or grossly negligent failure), and does not affect Roksnet's responsibility for operating the Member Directory itself (and for Trust Services where Roksnet acts as the Trust Service Provider). See also §5.1 (the X-Road software and technology are NIIS's, not Roksnet's) and §5.4 (peer-to-peer exchange does not pass through Roksnet).

2. Activation and Fees

2.1 Membership status and activation of Membership in the Member Directory

The status of "Member" (the legal entity's contractual status in the Roksnet Framework, attained on successful Identification under RGT §2 and RSST §2.6) is distinct from "Membership in the Member Directory" (the Member's listing in the Member Directory Service governed by this Annex). Becoming a Member does not, by itself, activate Membership in the Member Directory.

The Member activates Membership in the Member Directory by explicitly confirming activation within the Self-Service Platform (the "Activate Membership" action). Before activation, the Self-Service Platform informs the Member that activation:

- registers the organization in the Member Directory with its Member Name, Member Code, and Member Class, and makes it discoverable to other Members;
- enrolls the Member in both the Development (DEV) and Production (PROD) environments, so the Member can build and test in DEV and run live data exchange in PROD, without a separate activation step for each environment;
- starts a recurring Membership fee after a 14-day free period (see §6.3), billed to the billing contact (by default the Verification Invoice Contact; see RSST §2.1), with per-Security-Server-pair, per-Subsystem-pair, and other usage fees billed separately as the Member adds resources;
- unlocks the registration of Security Servers and Subsystems, the publication of APIs, and the consumption of services from other Members.

There is no obligation to activate Membership in the Member Directory (RGT §4.2). An account that remains entirely unused may, however, be treated as dormant under the account-dormancy provision in RGT §12 (suspension only after prior notice).

2.2 Paid Services Commitment

Activation of Membership in the Member Directory is a paid Service activation. By confirming activation, the Member:

- accepts the fees applicable to the Member Directory Service as set out in the RPP at the time of activation;
- authorizes Roksnet to issue invoices for those fees in accordance with the RPP;
- causes the operational provisions of this Annex to take effect.

Billing of Membership follows the general billing rules in §6, including the trial period (Membership receives the trial once).

Activation of Membership in the Member Directory does not, by itself, activate any other Roksnet Service (for example, Trust Services), each of which is activated and billed separately.

2.3 Environments

The DEV and PROD environments are separate Central Server instances (for example, "roksnet-dev" and "roksnet-prod"). Both are enrolled together on activation of Membership in the Member Directory. The environments are means of operating within the Framework; the recurring Membership fee covers the Member's listing across both environments. Per-Security-Server-pair and per-Subsystem-pair fees apply as set out in the RPP.

3. Member Directory Data and Visibility

3.1 Data visible to all X-Road participants (mandatory registry data)

The following data is published in the X-Road central registry and is visible to other Members via their Security Servers, to enable discovery and the establishment of connections:

- Member Name;
- Member Code;
- Member Class (one of COM, GOV, or NGO).

This data is required for X-Road communication and cannot be hidden while the Member is active in the Member Directory. Registered Subsystems become visible through the central-registry configuration. API and data-service information may be discoverable separately through X-Road metadata mechanisms or Roksnet's separate display function (see §1).

The Member Class is declared by the Member as part of registration (RSST §2.1) and is recorded at Identification. It cannot be changed by the Member afterwards (it forms part of the non-editable registry data; see §3.3); a correction of a genuine error is made by Roksnet on request. The Member Class is one of: COM (a private-law for-profit legal entity), GOV (a public-law body or other entity designated as a public-sector entity), or NGO (a private-law non-profit legal entity). It is determined by the entity's legal form and purpose; a body governed by public law or designated as public-sector is GOV, a private-law entity is COM if for-profit and NGO if non-profit (so a state-owned company operating as a private-law for-profit entity is COM). Where the correct class is unclear, the Member selects the closest class. Roksnet does not independently verify the Member Class against governmental or other official registers (it has no official verification channel for this) and does not guarantee its accuracy; the Member is responsible for the accuracy of the Member Class it declares, and Roksnet is not liable for an incorrect classification. Roksnet may correct a manifestly incorrect class.

3.2 Public Member profile (visible to other Roksnet Members)

A public Member profile is visible to other Roksnet Members and contains the Member's organisational information, including:

- identity data (Member Name, Member Code, Member Class, Country, Member Since, status, environment);
- verification data (Organization Registry Code, Registrar Organization, Registrar Website, Verification Method, Trust Service Provider);
- contact information (general organization email, general organization phone, legal address, website);
- description and organization logo;
- registered Subsystems and published APIs.

The business-register information (Organisation Registry Code, Registrar Organisation, Registrar Website) is declared by the Member and is not independently verified by Roksnet

against any register (see §4); it is shown as Member-declared information, not as Roksnet-verified.

The Member is responsible for ensuring that all information it submits, declares, or publishes in the Member Directory or the Self-Service Platform is accurate, complete, current, and not misleading. Roksnet does not independently verify this information against official registers, but may refuse registration, decline publication, correct, hide, unlist, suspend, or remove the affected record or Service where the information appears inconsistent, false, misleading, unlawful, or materially inconsistent with the registration form, bank-payment data, qualified electronic seal Confirmation Message, or other data submitted by the Member. This does not create any obligation for Roksnet to verify Member data against official registers.

The public Member profile is intended exclusively for organisational data of the legal entity. Submission of personal data of individual employees or other natural persons through the public profile is prohibited under the AUP (AUP §3); the privacy treatment of this data is set out in RPN-Services §3.3A.

3.3 Member's control of the profile

The Member can preview its own public profile exactly as other Members see it.

The Member may edit, through Account Settings, only the fields that the Member itself provided and which Roksnet does not validate — the legal address, general contact email, general contact phone, organisation description, organisation logo, and website.

The Member may not edit data that originates from the Identification process (data received through the bank payment or the qualified-electronically sealed Confirmation Message) or data held in the X-Road central server. This includes, without limitation, the Member Name, Member Code, Member Class, Country, and Trust Service Provider, together with the other verification data.

The following data cannot be hidden from the Member Directory while the Member is active: Member Name, Country, Trust Service Provider, Member Code, and Member Class. The Member may hide the remainder of its profile from search ("Hide from search").

3.4 Discovery of other Members

A Member discovers another Member by entering that Member's Member Code, which is obtained directly from the counterparty. The Member Code uniquely identifies each Roksnet Framework Member.

4. Member identity and counterparty verification

Through the Member Directory Service, Roksnet provides identification data that Members submit and that Roksnet validates only to the level of the Identification procedure (RSST §2.2–§2.6). The bank transaction and any qualified electronic seal are inputs to Identification; they are not KYC/AML or registry verification performed by Roksnet, and they do not confirm the

Member's registry data or the authority of any person to bind it. Roksnet does not independently verify Member attributes against governmental registers and does not guarantee that any Member is a suitable or correct counterparty for another Member's data exchange.

The decision to exchange data with another Member, and the verification of that Member's identity and suitability for that purpose, rests with each Member individually. Before exchanging data, a Member should confirm that the Roksnet Member Code corresponds to the organisation it intends to connect with.

Roksnet does not warrant the identity, authenticity, or authority of any Member to any other Member, and is not liable for loss arising from another person's fraud, forgery, impersonation, or lack of authority. The allocation of risk for registration, authority, fraud, impersonation, and forgery is set out in RGT §3.3.

Nothing in this section excludes or limits Roksnet's liability for its own intentional or grossly negligent failure to perform its obligations, or any other liability that cannot be excluded or limited under mandatory applicable law (see RGT §10).

5. Security Servers

5.1 What a Security Server is and who operates it

A Security Server is a physical or virtual server, running supported operating systems (for example Ubuntu or RHEL) together with the X-Road Security Server software, that the Member installs and operates on its own infrastructure. It is the Member's gateway between the Member's information systems (its Subsystems) and the rest of the Roksnet Framework, handling authentication, signing (eSealing), encryption, and timestamping of each X-Road request.

X-Road software and technology — third-party, not within Roksnet's responsibility. The X-Road Security Server software, and the underlying X-Road technology, are open-source software managed and developed by the Nordic Institute for Interoperability Solutions (NIIS) and published under the MIT License. They are not Roksnet's software or technology, and Roksnet is not their author, owner, licensor, or distributor. The Member obtains and installs the X-Road Security Server software directly from NIIS's official distribution source (its package repository and the source code published on GitHub) and uses it under the applicable NIIS open-source licence (the MIT License). Where Roksnet provides a link to that source, or references to it in guides, for the Member's convenience, the link or reference does not make Roksnet the supplier, licensor, or distributor of the software and does not transfer any responsibility for it to Roksnet.

To the fullest extent permitted by applicable law, Roksnet is not responsible or liable for the X-Road software or the X-Road technology itself, including their availability, functioning, defects, security vulnerabilities, updates, or fitness for any purpose. Roksnet is responsible only for its own Services as set out in the RGT and the applicable Annexes. Nothing in this section

excludes or limits any liability that cannot be excluded or limited under mandatory applicable law (see RGT §10).

The Member is responsible for the installation, configuration, hardening, patching, monitoring, and operation of the Security Server (see RGT §8). Installation and configuration take place outside the Self-Service Platform; the Self-Service Platform provides the steps, guides, references, and the required artefacts (configuration anchor, CSR upload, certificate download).

5.2 Setup and registration

Setting up a Security Server involves, at a high level: preparing a host and installing the software; performing the initial configuration and generating certificate signing requests (CSRs); ordering AUTH and SIGN certificates from Trust Services and downloading them; and uploading the certificates, configuring timestamping, and registering the Security Server. AUTH and SIGN certificates are ordered as part of the Security Server setup, not before. Registration of a Security Server in the Member Directory (Central Server) is processed automatically; once registered, the Security Server becomes visible to other Members in the Member Directory. Automatic processing does not waive the requirement to activate a corresponding pair in the Self-Service Platform first (see §5.8).

5.3 Message logging and legal evidence

When enabled, the Security Server logs every message it processes and produces tamper-evident records (hash-linked logs with timestamps) capable of evidencing what was exchanged, when, and between which parties. Message logging, and the associated timestamping, is a feature of the X-Road Security Server software that the Member controls and that can be disabled; the Member is responsible for ensuring that message logging and timestamping are enabled and correctly configured where it requires evidence of its data exchange. Because the Security Server is installed and operated by the Member, these records are held and controlled by the Member, and the Member is responsible for retaining and archiving them for as long as it requires them. Roksnet does not hold these message logs. The records are intended to support the Member's evidence of data exchange, including for non-repudiation; Roksnet does not guarantee any particular evidential weight or how any court or authority will assess them.

5.4 Peer-to-peer exchange

Data exchange takes place directly between Members' Security Servers (peer-to-peer). It does not pass through Roksnet's central server, and Roksnet does not access or monitor the content or payload of Member-to-Member exchange (see RPN-Services §3.3).

5.5 Listing and fees

The Security Server listing is the registration of the Member's Security Server in the Member Directory (the central registry) and the maintenance of that registration, so that the Security Server is recognised in the Framework and can participate in data exchange, subject to all other technical and certificate prerequisites (registration alone does not by itself make the Security Server ready for exchange). This listing is the Roksnet service the Member pays for; obtaining,

installing, configuring, and operating the Security Server itself is the Member's own responsibility (§1, §5.1).

The Security Server listing is a separately-priced component of the Member Directory Service, charged as pairs. A Security Server pair comprises one Production (PROD) Security Server slot and one Development (DEV) Security Server slot. The Member activates a Security Server pair in the Self-Service Platform; activation starts the recurring per-pair fee, and the Member may then register up to one PROD and up to one DEV Security Server within the pair, in any order. The DEV Security Server is not charged separately — it is included in the pair. By activating a Security Server pair, the Member accepts the applicable per-pair fee set out in the RPP in effect at the time of activation, and authorises Roksnet to issue invoices for it (consistent with RGT §4.2).

The Member may activate additional Security Server pairs as needed (for example, additional PROD servers for redundancy or scale). Each pair is a separate billable unit; the total fee is the number of active pairs multiplied by the per-pair fee. The Security Server fee is separate from, and additional to, the recurring Membership fee (§2). Billing of Security Server pairs follows the general billing rules in §6, including the trial period (the trial applies only to the first Security Server pair; additional pairs are billed without a trial). Fees are set out in the RPP.

5.6 Security obligations

Security obligations relating to Security Servers, AUTH and SIGN certificates, and related cryptographic material are set out in RGT §8 and the applicable Trust Services documentation.

5.7 Subsystems

The Subsystem listing is the registration of the Member's Subsystem in the Member Directory and the maintenance of that registration, so that the Subsystem is recognised and can provide or consume services in the Framework, subject to all other technical and certificate prerequisites. The Subsystem (the Member's information system) and its operation remain the Member's own responsibility (§1).

The Subsystem listing is a separately-priced component of the Member Directory Service, charged as pairs in the same way as Security Servers (§5.5). A Subsystem pair comprises one Production (PROD) Subsystem slot and one Development (DEV) Subsystem slot. The Member activates a Subsystem pair in the Self-Service Platform; activation starts the recurring per-pair fee, and the Member may then register up to one PROD and up to one DEV Subsystem within the pair, in any order. The DEV Subsystem is not charged separately. By activating a Subsystem pair, the Member accepts the applicable per-pair fee set out in the RPP in effect at the time of activation, and authorises Roksnet to issue invoices for it (consistent with RGT §4.2). The Member may activate additional Subsystem pairs as needed; each pair is a separate billable unit. Registered Subsystems are listed in the Member Directory; API and data-service information may be displayed separately (see §1). Billing of Subsystem pairs follows the general billing rules in §6, including the trial period (the trial applies only to the first Subsystem pair; additional pairs are billed without a trial). Fees are set out in the RPP.

5.8 Activation in the Self-Service required before registration; enforcement

The Member must activate the corresponding capacity in the Self-Service Platform (§5.5, §5.7) before it registers or connects a Security Server or a Subsystem. Registering a Security Server or Subsystem in the Member Directory does not, by itself, constitute activation or payment and does not relieve the Member of this obligation. In each environment, the number of registered Security Servers and Subsystems must not exceed the respective slots included in the Member's active pairs.

Where a Security Server or Subsystem is registered without corresponding activated capacity, Roksnet may immediately and without prior notice unlist and de-register the uncovered resource and keep it unlisted until the required capacity is activated. Roksnet will notify the Member promptly of the action, its reason, and the steps required to restore the listing. This resource-level corrective action does not by itself suspend or terminate the Member Account or the Agreement.

If, after receiving such notice, the Member repeats the conduct, Roksnet may suspend the Member Account in accordance with RGT §12, RSST §7, and AUP §6. Roksnet may terminate the Agreement only where the repeated conduct constitutes a material breach or otherwise provides grounds for termination under RGT §12 and applicable law. The applicable prior-notice rules remain in effect unless immediate action is required because of an active security incident, a serious violation, or a legal or regulatory requirement.

Nothing in this section limits any liability that cannot be excluded under mandatory applicable law.

6. Fees and Billing

6.1 Fees

Fees for the Member Directory Service — the recurring Membership fee, per-Security-Server-pair fees, and per-Subsystem-pair fees — are set out in the RPP (Annex D), which is the sole source of pricing. The price applied to an activated Service is the price in effect at the time of activation, which is recorded in the activation log. Fees are billed to the billing contact (by default the Verification Invoice Contact; the Member may update the billing contact in Account Settings — see RSST §2.1). Prices are exclusive of VAT, which is added where applicable.

6.2 Whole calendar month billing

Fees are charged in whole calendar months. Any calendar month during which a Service is active for any part of the month is charged as a full month; no pro-rata applies. (For example, a Service activated on 29 May is charged for the whole of May.) This applies to all paid components of the Member Directory Service.

6.3 Trial period

The Self-Service Platform presents a 14-day trial. The following rule applies and always provides at least 14 free days:

- where the Service is activated on the 1st to the 14th day of a calendar month (inclusive), the month of activation is free, and whole-month billing begins on the 1st day of the following month;
- where the Service is activated on the 15th day to the last day of a calendar month, the month of activation is free and the following month is charged at 50%, and whole-month billing begins from the month after that.

The trial applies to: Membership (once); the first Security Server pair; and the first Subsystem pair. All additional pairs (Security Server or Subsystem) are billed without a trial, i.e. whole-month billing applies from activation (§6.2). The trial is granted once per service type and is not renewed by cancelling and re-activating (this prevents repeated free periods).

7. Suspension, Cancellation, and Termination

7.1 Member-initiated cancellation

The Member may request cancellation of its Membership in the Member Directory at any time through the Self-Service Platform. Cancellation does not take effect instantly: because Membership underlies the Member's entire presence in the Roksnet Framework, Roksnet first verifies that the request genuinely reflects the Member's intent, to protect the Member against compromised credentials, social-engineering, and accidental cancellation.

The review is limited to verifying the authenticity of the request (that it genuinely came from the Member's organisation). It is not a discretionary decision on whether the Member may leave; the Member's right to cancel is not subject to Roksnet's discretion.

On a cancellation request:

- the request is sent to Roksnet for authenticity verification;
- the Membership in the Member Directory remains active, and billing continues in the normal way, during the review;
- where the cancellation is verified and processed, the last month charged is the calendar month in which the cancellation request was made; this cut-off is applied retroactively to the month of the request, so Roksnet's processing time does not add a further charged month even if the review concludes in a later calendar month;
- the Member may withdraw the request at any time before it is processed;
- Roksnet completes the review within 14 days of the request;
- if Roksnet cannot verify that the request genuinely came from the Member's organization, it does not process the cancellation: it notifies the Member and either rejects or holds the request pending verification. A cancellation is never processed on the basis of an unverified request (this protects the Member against compromised credentials and social-engineering);

- where the request is withdrawn by the Member, or is not processed because its authenticity could not be verified, no cut-off applies and billing continues in the normal way; the cut-off above takes effect only when a valid cancellation is verified and processed.

This section governs cancellation of the Member Directory Service only; it does not, by itself, close the Member's Account, end the Member's general status in the Roksnet Framework, or cancel other Services (see §7.4). Termination of the Agreement as a whole is governed by RGT §12. When the cancellation is verified and processed, it takes legal effect on that date - Membership in the Member Directory and access to the Member Directory Service end then, that Membership having remained active until then - and:

- the Membership in the Member Directory is cancelled and the organization is removed from the Member Directory;
- all of the Member's Security Servers, Subsystems, and APIs and data services are unlisted from the Member Directory;
- all ongoing data exchange with other Members through the Member Directory stops.

Re-joining after cancellation requires completing the setup again.

7.2 Deactivation of Security Server and Subsystem pairs

Independently of cancelling the Membership in the Member Directory, the Member may deactivate an individual Security Server pair or Subsystem pair in the Self-Service Platform. Deactivation of a pair is the means of stopping the recurring fee for that pair; it does not cancel the Membership in the Member Directory and does not affect the Member's other active pairs.

The following apply to pair deactivation:

- the billable unit is the pair, not the individual PROD or DEV slot. Releasing, unregistering, or leaving empty a PROD or DEV slot within a pair does not, by itself, stop the per-pair fee; the Member must deactivate the pair to stop the fee;
- under the whole-calendar-month billing rule (§6.2), the calendar month in which the pair is deactivated is the last month charged for that pair; no fee is charged for that pair for any month after the month of deactivation;
- on deactivation, the Security Servers or Subsystems registered within the pair are unlisted from the Member Directory, and any APIs and data services published through them are unlisted; ongoing data exchange through them stops;
- pair deactivation is an authenticated action attributed to the Member under RGT §3.3 and does not require the authenticity review that applies to Member Directory Membership cancellation under §7.1.

7.3 Urgent situations

If the Member suspects a security incident, abuse of the account, or any other urgent issue requiring immediate action, the Member should not wait for the cancellation review and should contact Roksnet immediately at support@roksnet.com.

7.4 Services not affected

Cancellation of the Member Directory Service does not cancel other Roksnet Services, each of which has its own cancellation procedure, including Roksnet Trust Services and any separately activated Support, Monitoring, Portal, or professional-service arrangement.

7.5 Roksnet-initiated suspension and termination

Roksnet may suspend or terminate the Member Directory Service in accordance with RGT §12 (including for material breach, security concerns, or non-payment). Non-payment treatment is set out in the RPP.

8. Data retention

On cancellation or termination, the Member's public record is removed from the Member Directory. A Member Code that has identified an active Member is permanently retired and is not reassigned to another organisation, because it remains referenced in audit logs, message logs, certificates, and other Members' records and must stay unambiguous for historical and counterparty-identification purposes. (The six-month reuse rule in RSST §2.9 applies only to Member Codes from applications that were never activated.) Roksnet does not retain the Member's data in full after cancellation. Roksnet retains only specific categories, each for its own period and purpose:

- invoices and accounting records — for the statutory accounting-retention period;
- evidence of acceptance and of the contractual relationship (for example, acceptance logs) — for the period necessary to establish, exercise, or defend legal claims;
- operational and configuration history, and security and audit logs — for a limited period after deactivation.

Deletion of the Member Account (available in Account Settings or by written request to support@roksnet.com) terminates the Agreement and all Services (RGT §12); it is distinct from cancelling the Member Directory Service alone (§7.1). After account deletion, Roksnet retains only the categories above, for their stated periods; it does not retain the Member's data in full. The detailed retention periods for personal data are set out in RPN-Services §9.

9. Relationship with other documents

This Annex applies together with the RGT and alongside the other Annexes, the RPN-Services, and the AUP. Amendment, liability, governing law, jurisdiction, communication, and general provisions are set out in the RGT.

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