For Instances created before March 13, 2024, this Data Processing Agreement will apply until April 2, 2024, when the Data Processing Agreement below will come into effect.

All previous versions of the Data Processing Agreements can be found HERE.

PERSONAL DATA PROCESSING AGREEMENT

ANNEX 2 TO THE RAYNET CRM TERMS OF SERVICE

(hereinafter the “**Data Processing Agreement**”) concluded by and between:

A. **you,** the entity who has chosen to use the RAYNET service;
(hereinafter the “**Controller**” or “**you**”)

and

B. **RAYNET s.r.o.**, ID No.: 26843820, with the registered office at Hlavní třída 6078/13, Poruba, 708 00 Ostrava, Czech Republic, represented by Ing. Aleš Seifert and Ing. Jaroslav Bazala, registered in the Commercial Register maintained by the Regional Court in Ostrava under File No. C 28180,

(hereinafter the “**Processor**”, “**RAYNET**” or “**we**”)

(the Controller and Processor collectively as the “**Parties**” and individually as a “**Party**”).

If you use the RAYNET CRM service (“**Service**” or “**CRM**”), RAYNET will be the processor of the Personal Data you provide to us, in particular, that uploaded to the CRM Software. The Service is provided under the RAYNET CRM Terms of Service (“**Terms of Service**”). By concluding the Agreement, you hereby confirm that you have read and agree with the Data Processing Agreement. This Data Processing Agreement applies to all users who access or use the Service and is legally binding.

Therefore, please read this Data Processing Agreement carefully; it sets forth the terms and conditions of processing Personal Data under which the Service is provided. Should you have any inquiries regarding processing Personal Data, you can contact us at dpo@raynetcrm.com.

The Parties process the Personal Data pursuant to the Agreement and applicable legal regulations.

1. DEFINITIONS

For the purposes of this Data Processing Agreement, we use terms not defined in the Terms of Service. For the sake of clarity, we, therefore, set out what each term means unless otherwise defined in the Data Processing Agreement.

GDPR	Regulation (EU) 2016/679 of the EU Parliament and of the Council;
CCPA	California Consumer Protection Act of 2018;
PDPA	Personal Data Protection Act of 2012 in force and effect in Singapore;
EEA	European Economic Area;
Personal Data	any information about the User that can directly or indirectly identify them;
Controller	you, as our customer and user of the Service in relation to the Personal Data you provide to us, in particular, the Personal Data of your clients you upload to the Application;
Processor	we, RAYNET, as we process Personal Data you provide to us as part of providing the Service;

Subprocessor entities, subproviders, that RAYNET commissions to process data within the framework of providing the Services in relation to the Personal Data you provide to us.

Personal Data Processing in simple terms, this means any handling of Personal Data – whether storing, disclosing, deleting or changing it;

The above definitions are consistent with the terms and definitions under GDPR.

If you reside in Singapore, the terms used in this Data Processing Agreement such as “Data Subject”, “Controller” and “Processor” correspond to the terms “Individual”, “Organization” and “Data Intermediary” used under the PDPA.

If you are located in the state of California, the terms “Personal Data”, “Data Subject”, “Controller” and “Processor” used in this Data Processing Agreement correspond to the terms “Personal Information”, “Consumer”, “Business” and “Service Provider” under the CCPA. In connection with the CCPA, we also state that we do not sell, rent or otherwise disclose your Personal Information for financial or other consideration under any circumstances. Should we disclose your Personal Information to a third party in any way, we do so in order to provide our Services or to comply with our legal obligations.

2. INTRODUCTION AND BRIEF SUMMARY OF THE AGREEMENT

2.1. **The subject and purpose of the Data Processing Agreement.** By concluding this Data Processing Agreement, you, as the Controller, authorize the Processor to process Personal Data on your behalf in connection with providing the Service. The purpose is to ensure the Personal Data security to the extent required by law. The scope of the processed Personal Data can be found in **Annex A** to this Data Processing Agreement.

2.2. **The Service.** The RAYNET Service consists of providing CRM software. RAYNET provides setup, control and management tools and other functionalities via the desktop application, mobile application or API (including other features offered) and other related services, such as Customer Support.

2.3. **The role of the Processor and the Controller.** When using the Service, you provide us with Personal Data of which you are the Controller. We then process this Personal Data upon your instruction and to the extent you set out. When processing Personal Data, you are in the position of the Personal Data Controller.

2.4. **Written form.** The Parties hereby set out the rules for processing Personal Data in writing.

2.5. **“In layman’s terms” notes.** We have tried to draw up the Data Processing Agreement so it is as clear as possible. This is also what the “in layman’s terms” notes in blue are for, to summarize the relevant parts of the Data Processing Agreement. However, these notes are not a binding part of the Data Processing Agreement and are only included to facilitate the understanding of its individual provisions.

2.6. **Definitions.** The terms and definitions listed in the Terms of Service will be adopted with the same meaning in the Data Processing Agreement.

2.7. **Term of the Terms of Service.** This Data Processing Agreement is concluded for the duration of the Agreement pursuant to the Terms of Service.

2.8. **The moment of conclusion and termination of the Data Processing Agreement.** The Data Processing Agreement is concluded at the moment of finishing the sign-up process for the purpose of using the Service (concluding the Agreement). The Data Processing Agreement may be terminated at the same time and on the same terms as termination of the Service under the Terms of Service.

2.9. **Effects of termination.** The termination of the Terms of Service causes the termination of this Data Processing Agreement. However, the termination of this Data Processing Agreement does not affect the obligations of the Processor to transfer (return) Personal Data to the Controller or dispose of it and to respect the confidentiality of the information.

In layman's terms: *You upload your clients' personal data to the CRM system. We then process it for you. The law requires us to put this processing relationship in writing. There is no need to worry. We have very limited access to the data you upload to the application. It will be mainly data needed for diagnostics or statistics.*

3. JOINT OBLIGATIONS OF THE CONTROLLER AND PROCESSOR

3.1. **Lawfulness of processing.** The Controller and the Processor undertake to comply with the applicable regulations governing the protection of Personal Data.

3.2. **Cooperation.** The Controller and the Processor undertake to cooperate with each other to the extent necessary and reasonable in the performance of their obligations while processing the Personal Data arising from the concluded agreements and legal regulations, in particular, in connection with responses to the exercise of data subjects' rights, security incidents as well as the preparation of impact assessments and dealings with authorities. The Parties undertake to provide the necessary documentation for the processing of requests concerning the processing of Personal Data pursuant to the Terms of Service. A Party will provide these documents without undue delay, but no later than within ten business days of receiving the request for cooperation from the other Party.

In layman's terms: *Both you and we are committed to complying with the regulations governing the protection of the Personal Data. At the same time, if there is an audit or a data leak, we must mutually cooperate and send each other the necessary documents.*

3.3. **Incident.** A Party will notify the other Party when it becomes aware of a security breach within 48 hours thereof. A breach means any security breach of Personal Data that may potentially lead to the accidental or unlawful destruction, change or unauthorized disclosure of or access to Personal Data processed under the Agreement as amended by the Terms of Service.

In layman's terms: *Should a personal data breach occur on either our side or your side, we must inform each other of that incident as soon as possible. Here, the law dictates a 48-hour limit.*

4. RIGHTS AND OBLIGATIONS OF THE PROCESSOR

4.1. **Access Restriction.** The Processor will ensure that access to Personal Data is limited to (a) employees who process Personal Data as part of their job description and (b) persons who cooperate with the Processor and may process Personal Data on behalf of the Processor as part of such cooperation in accordance with the terms and conditions of this Data Processing Agreement and for the purpose of providing the Services under the Agreement as amended by the Terms of Service. If these persons are not subject to a legal confidentiality obligation, the Processor must ensure their contractual confidentiality.

In layman's terms: *We will have minimum contact with the Personal Data you upload to the application. Despite that, we undertake to ensure that all persons who have or may have access to the data to comply with the rules of data protection and the confidentiality obligation.*

4.2. **Processor's obligation regarding the measures taken.** The Processor has adopted and undertakes to maintain appropriate technical and organizational measures for the term of the Data Processing Agreement in accordance with the GDPR applicable to the Processor. The overview of measures taken can be found in **Annex B** hereto.

4.3. **Processor's obligations.** The Processor undertakes to:

4.3.1. comply with all obligations arising for the Personal Data Processor from the applicable legal regulations when processing Personal Data;

4.3.2. process the Personal Data only on the basis of instructions from the Controller made under the Data Processing Agreement, including the area of transferring the Personal Data to a third country or international organization;

4.3.3. notify the Controller without undue delay of cases where an inspection or other proceedings are initiated by a supervisory authority regarding the Personal Data processing by the Processor and provide the Controller with all information on the course and results of such inspection or proceedings;

4.3.4. cooperate with the Controller in ensuring compliance with the Controller's obligations regarding the security of Personal Data, taking into account the nature of the processing to be carried out by the Processor;

4.3.5. allow the Controller to conduct internal audits, including inspections, performed by the Controller or another auditor commissioned by the Controller (hereinafter the "**Audit**"). The Processor must be notified of the Audit at least one month in advance. The Processor may object to any auditor commissioned by the Controller if such auditor is not independent or in a competitive or similar position to the Processor. Based on the Processor's objection, the Controller is obligated to commission another auditor;

4.3.6. notify the Controller of any Personal Data security breach of which the Processor becomes aware without undue delay and no later than 48 hours after becoming aware thereof;

4.3.7. keep records of all Personal Data security breaches and the corrective measures taken to ensure adequate processing security. The Processor is obligated to provide the Controller with all necessary cooperation related to the investigation into the security breaches and performance of the Controller's obligations;

4.3.8. cooperate with the Controller in documenting processes and documents demonstrating the Controller's compliance with the applicable personal data security legislation rules.

In layman's terms: *We undertake to comply with everything required by law and to be helpful in the event of any issues.*

4.4. **Compensation for costs.** The Parties agree that the Processor is entitled to reimbursement from the Controller for reasonable costs associated with providing cooperation.

4.5. **Confidentiality of the Processor.** The Processor undertakes to comply with the confidentiality obligation regarding all Personal Data transmitted by the Controller and to maintain its confidentiality, not to disclose it to any third party, neither in whole nor in part, unless it is to be transmitted on the basis of the Controller's instructions or legal regulation.

4.6. **Trade secrets.** All information and documents disclosed by the Processor to the Controller in connection with an Audit or inspection are subject to the Processor's trade secrets and, unless otherwise specified, will be subject to the confidentiality obligation hereunder. Such information and documents may only be disclosed to an authorized supervisory authority.

4.7. **Lawfulness of processing.** The Processor's obligations regarding the protection of Personal Data shall be fulfilled by the Processor for the entire term of the Agreement unless the provisions hereof, of the Agreement or applicable legal regulations state they should continue even after the termination thereof.

4.8. **Involvement of processors and new processors.** The Controller grants the Processor consent to the involvement of other processors. The Processor has involved **Amazon Web Services, Inc.** (**AWS**), **Digital Solutions, s.r.o.** (**Digisign**), and **Microsoft** (**Azure OpenAI Service**)in the processing of Personal Data. If the Processor is to involve other processors, it must inform the Controller thereof before such change via email or directly through the user interface. In the event that the Controller does not agree to the involvement of the new processor, it may withdraw its consent and file an objection no later than five days after receiving the Processor's notification. Filing an objection, and thus not involving a new (sub)processor, may result in the inability to use the Service.

In layman's terms: *We cannot do everything by ourselves, and we need to use the services of other entities (we need, a place to store data, for example). We will let you know in advance if we plan to start a new cooperation that will involve the processing of your data.*

4.9. **Processor's obligation in case of termination of the cooperation.** The Processor undertakes to delete all Personal Data in the event of termination of the provision of the Services and to return it, including any copies, at the request of the Controller in accordance with the provisions herein, unless the EU or Czech law requires their storage.

4.10. **Data return.** Before terminating the cooperation, the Controller may export their data from the Processor's system. Alternatively, the Controller may request the Processor to send the backed-up data according to the Terms of Service no later than 80 days after cancelling an Instance. After this period expires, the Controller's data will be irretrievably deleted.

In layman's terms: *If you decide you no longer want to use our services, you can download the data yourself or contact us with a request to provide you with a data backup. After 80 days of canceling the Instance, we will delete your data, so you do not have to worry about your data being stored forever.*

5. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

5.1. **Lawfulness.** The Controller is responsible for ensuring that all processing activities are lawful and that Personal Data is processed for a specific purpose based on a lawful title.

5.2. **Controller's measures.** The Controller is liable for the following:

5.2.1. compliance with the legal regulations relating to the Personal Data security,

5.2.2. assessing whether the technical and organizational measures meet the requirements for the Personal Data security,

5.2.3. taking technical and organizational measures to ensure Personal Data security.

In layman's terms: *How you handle the data is your responsibility. We recommend that you take sufficient precautions when using the service to prevent data leaks.*

5.3. **Instructions.** We process data exclusively based on the Controller's instructions which are in accordance with the Terms of Service. Should the Controller's instructions go beyond the scope of the Terms of Service, the Processor will only carry out the relevant processing activity by written agreement with the Controller.

In layman's terms: *We process your personal data only to the extent set out in the Terms of Service. If you require us to do anything extra, we need to agree on it first.*

6. TRANSFER OF PERSONAL DATA ABROAD

6.1. **Standard contractual clauses.** In connection with the provision of the Services, we use Subprocessors who may be based outside the EEA. In this case, we will enter into a standard contractual clause with each Subprocessor to ensure adequate security of Personal Data in accordance with the GDPR.

7. CALIFORNIA CONSUMER PRIVACY ACT

7.1. **Applicability.** This section applies if we process Personal Data on your behalf under the CCPA (you are subject to the CCPA).

7.2. **Processor's obligations.** The Processor undertakes to process Personal Data in accordance with the CCPA, in particular, to perform the following:

7.2.1. not to sell Personal Data,

7.2.2. not to retain, use or disclose the Personal Data for any purpose other than providing the Services,

7.2.3. not to retain, use or disclose the Personal Data outside the processing relationship between the Controller and the Processor.

7.3. **Personal Data processing.** The Processor processes Personal Data for the Controller pursuant to the conclusion of the Agreement and acceptance of the Terms of Service.

7.4. **Controller's obligations.** The Controller undertakes to ensure that it has properly informed its customers that their data is being used or shared in accordance with the applicable provisions of the CCPA. The Controller is responsible for compliance with the provisions of the CCPA.

8. FINAL PROVISIONS

8.1. **Applicable law.** Matters not specifically covered in this Data Processing Agreement are governed by the generally binding, applicable legal regulations. This Data Processing Agreement is governed by and construed in accordance with Czech law, in particular, Act No. 89/2012 Sb., the Civil Code, as amended. The Parties agree that business practices do not take precedence over any provisions of the law, including those that do not have a coercive effect.

8.2. **Jurisdiction.** In the event that a dispute arises between the Controller and the Processor hereunder, the competent court to resolve such a dispute is the district court in Ostrava, Czech Republic.

8.3. **Force Majeure.** The Processor is not liable for situations in which it was unable to fulfil its obligations hereunder due to an event referred to as an instance of force majeure (war, riots, terrorism, civil unrest, strikes, fire, epidemics or natural disasters).

8.4. **Communication between the Parties.** The Parties agree that their communication regarding the Data Processing Agreement will be made via email at the following addresses:

8.4.1. Controller: the email address that the Controller has used to sign up for the Service or has set as their primary email address for the purpose of the Service;

8.4.2. Processor: support@raynetcrm.com, DPO (notifying one another of security incidents): dpo@raynetcrm.com;

8.5. **No assignment**. Neither Party may assign or transfer its rights and obligations under or related to this Data Processing Agreement without the prior written consent of the other Party.

8.6. **Amendments and changes.** The Processor reserves the right to modify or amend this Data Processing Agreement. If we make any changes or amend the rights and obligations hereunder, you will be notified thereof in a timely manner via email. If you continue using the Service, you thereby agree to the updated Data Processing Agreement. If you disagree with the changes, please stop using the Service.

8.7. **Effect.** This Data Processing Agreement will be effective in this wording as of April 2, 2024.

8.8. **Annexes.** The following annexes form integral parts of the Data Processing Agreement:

- **Annex A:** Nature, Scope, Period and Purpose of Personal Data Processing,
- **Annex B:** Technical and Organizational Measures.

ANNEX A

TO THE PERSONAL DATA PROCESSING AGREEMENT

NATURE, SCOPE, PERIOD AND PURPOSE OF PERSONAL DATA PROCESSING

Nature of processing. Personal Data is processed automatically through the Processor's systems used to provide the Service.

Purpose. The purpose of the processing is to enable the Controller to use the Service (performance of the Agreement).

Legal basis for processing. The legal basis for Personal Data processing within the provision of the Service is the performance of the Agreement (as amended by the Terms of Service).

Scope of processing: Depending on how the Controller uses the Service, the following Personal Data may be processed in connection with the provision of that Service:

- ➔ **Contact details:** First name, last name, email, phone number, address, ID No., registered office, bank account no.;
- ➔ **Any additional personal data** are processed exclusively upon the Controller's instructions.

Special Categories of Personal Data. The Controller undertakes not to disclose to the Processor any Personal Data that falls within a special category of Personal Data within the meaning of Article 9 of the GDPR. The special categories of Personal Data may only be processed with the express prior agreement with the Processor. **What are the special categories of Personal Data?** This is Personal Data that reveal a person's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union memberships, health condition, sex life or sexual orientation. Genetic and biometric data is also considered a special category of personal data if it is processed for the purpose of uniquely identifying a private individual.

Data subjects. As a rule, this includes the Personal Data of the Controller's customers or clients, its employees and other cooperating persons, including its suppliers, users of the Controller's website, business partners or their employees or representatives.

Period of processing. Personal Data is processed for the period of time corresponding to the period during which the Parties are bound by the Agreement as amended by the Terms of Service unless the Parties' agreement or a legal regulation provides for a longer period.

ANNEX B

TO THE PERSONAL DATA PROCESSING AGREEMENT

TECHNICAL AND ORGANIZATIONAL MEASURES

Technical and organizational Measures. Security is of the utmost importance to us, and we put continuous effort into keeping your Personal Data safe. We take into account the scope of processing, the associated risks and the state of our equipment when selecting the appropriate measures.

Technical measures. We have adopted and are committed to complying with the following measures:

- **HTTPS.** We use a secure https protocol. The data on our servers is encrypted. We encrypt data using SSL/TLS ("Secure Sockets Layer/Transport Layer Security") in all cases of data transfers.
- **Backup.** We perform a complete backup of all data and files every day.
- **Data center.** RAYNET Cloud CRM uses one of the largest and most modern IT infrastructures in the world: Amazon Web Services (AWS). AWS data centers are the world leader in physical and software security, they are able to withstand emergencies such as natural disasters, massive hacker attacks or power failures. Of course, regular stress and penetration tests are carried out as well.
- **Data insurance.** In terms of data protection, we go one step further than is common for the largest ICT service providers. All data stored in the Service is insured against damage, theft or disclosure.
- **Monitoring and minimization.** Access passwords to information systems (where Personal Data will be processed) and access to Personal Data are controlled at the individual level. All access to data is monitored.
- **Secure access.** Wherever possible, access to the systems is safeguarded using two-factor authentication (2FA). Access to the Service's infrastructure is allowed only via a private network (VPN) and by using a hardware security key, which is uniquely paired with dedicated devices.
- **Updates.** We regularly perform infrastructure updates.
- **Security at the application level.** Access to the application is protected by a unique username and password. The strength of the password and the frequency of its changes can be configured in the system administration. Optionally, a two-factor authentication mode can be enabled. Due to the nature of the application, it is easy to define permissions to access data.
- **Other measures.** We take other internal hardware, software and procedural measures to increase data security.

Organizational measures. We, as a Processor of your data, have adopted and are committed to complying with the following measures:

- **Confidentiality.** Our employees are bound by the confidentiality obligation.
- **Staff training.** Our employees are duly trained and undergo further training on a regular basis regarding the protection of Personal Data, and are familiar with safety rules for working with work devices.
- **Personal Data Processing Logging.** We use systems that allow us to uniquely identify which persons have accessed individual Personal Data, when and how individual Personal Data has been changed or when and by whom it has been deleted, even retroactively for the period of 30 days.
- **Controlling access to Personal Data.** We undertake to take such measures to ensure that only authorized users can access Personal Data and that such users can only access the Personal Data within the scope of their competence, insofar as this is possible given the nature of the Personal Data Processing.
- **Safe store.** We store passwords in the operating environment at a separate location (Safe store) with recorded logs so that we can monitor employee access to individual Personal Data of the Users.
- **Strong passwords.** All of our passwords are of sufficient length and format to prevent password cracking as much as possible. These passwords are not entered manually but via Safe store.
- **Pseudonymization of Personal Data.** We undertake to process Personal Data in such a way that it can no longer be attributed to a specific Data Subject without using additional information, provided that such information is kept separately.
- **Control of the transfer of Personal Data**. We have taken measures to ensure that Personal Data cannot be read, copied, altered or deleted during their transfer, transmission or storage.

- **Internal audit.** We regularly evaluate how we can minimize Personal Data Processing and what the appropriate measures to take are.