Privacy Notice for Non-Commercial User of Remotly Software

This document describes how we collect, use and protect the personal information of the non-commercial Users (hereinafter referred to as "you", "User" or "Client"), in connection with your use of our Software and Services for purposes as described and defined in the LICENSE AND SERVICE AGREEMENT (hereinafter referred to as the "Agreement") in relation to the Home License.

We are the controller of the data, which we process for our own purposes as set out below.

The processing of your personal data in connection with your visit to our Website and your use of the features offered within it is detailed in the Privacy Policy for www.remotly.com.

All capitalized terms used in this document and not otherwise defined herein shall have the meanings ascribed to them in the Agreement and, to the extent applicable, in the Terms of Service.

1. DATA PROCESSING IN CONNECTION WITH ENTERING INTO THE AGREEMENT AND THE USE OF OUR SOFTWARE

1.1. Data controller

The controller of your personal data within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR) is MIRILLIS CORE sp. z o. o. (limited liability company) with its registered office in Zielona Góra, ul. Fabryczna 14B /1 (65-410), Poland registered in the Register of Entrepreneurs kept by the District Court in Zielona Góra, VIII Economic Department of the National Court Register, under the KRS number: 0001050325, with the NIP (Tax Identification Number): 9292078550, REGON: 525981046 (hereinafter referred to as "we").

You can contact us by mail at the above address or via the contact form available on our Website www.remotly.com under "Contact".

1.2. Categories of personal data, purposes and legal basis for the processing

1.2.1. User Account Registration and Free License Plan

For the registration of the Account, it is necessary to indicate:

- email address,
- password.

We process the data in question for the purpose of entering into and executing the Client Account Maintenance agreement [Article 6 (1) (b) of the GDPR].

Since the creation of the Account results in the conclusion of the Agreement (Subscription in the Free Home License Plan), the data in question is processed for the purposes of the conclusion and implementation of the Agreement, in accordance with Article 6 (1) (b) of the GDPR, as well as:

- to communicate with the User in order to confirm the creation of the Account on the basis of our legitimate interest in verifying the correctness of the data entered by the User, as well as ensuring the security of the Account and the Services provided through it [Article 6 (1) (f) GDPR],

- to carry out additional verification when the User logs into the Account using the “Remotly Login Token” — based on our legitimate interest in ensuring the security of the Account and the Services provided through it [Article 6 (1) (f) GDPR],
- to send by email onboarding communications regarding the use of the Software and all of its functionalities — based on our legitimate interest in introducing the User to all of the features of our Software [Article 6 (1) (f) GDPR],
- to send by email information regarding the Subscription — based on our legitimate interest of communicating with the Users on matters related to the concluded Agreement [Article 6 (1) (f) GDPR],
- to establish, protect and pursue claims — on the basis of our legitimate interest [Article 6 (1) (f) GDPR],
- to handle the User’s claims in accordance with our obligations under applicable law and to comply with any other legal obligations that we are subject to [Article 6 (1) (c) of the GDPR].

The data in question will be kept by us for the period of performance of the agreements referred to above with additional consideration, where applicable, of the period of limitation of claims that may be raised against us and that we may have against the User.

The provision of the data referred to in this section is optional but necessary for the conclusion and execution of the above-mentioned agreements.

1.2.2. License Plan upgrade or use of the Additional Service

If you decide to upgrade to a higher License Plan or to use the Additional Service under the Free Home License Plan, it will be necessary to complete the data in your Account with:

- first name,
- last name,
- address,
- city,
- zip code,
- country.

The purposes and legal basis for processing and the retention period will remain as indicated in section 1.2.1 above.

Provision of the data referred to in this section is optional but necessary for the conclusion and execution of the Agreement in the paid License Plan or implementation of the Additional Service.

Subject to the terms of the Agreement, the choice of country may determine the terms of the Subscription and Services.

In the case of the paid License Plan or Additional Service under the Home Free License Plan, we will also process your personal data for the following purposes, where applicable:

- to settle the Service [Article 6 (1) (b) GDPR],
- to comply with our legal obligations, in particular tax and accounting obligations [Article 6 (1) (c) GDPR], taking into account the data retention periods imposed by these laws,

- to send you information about the Subscription Service by email, including information about the expiration date of the Subscription Service — based on our legitimate interest to communicate with you on matters related to the concluded Agreement [Article 6 (1) (f) GDPR].

You may delete your Account at any time from within your Account Settings. Please note that this will not affect our right to store your personal data for the proper settlement of the Agreement [Article 6 (1) (b) GDPR] and, where applicable, for compliance with our legal obligations [Article 6 (1) (c) GDPR] as well as for the establishment, protection and assertion of claims based on our legitimate interest [Article 6 (1) (f) GDPR].

1.2.3. Account registration and login via external authentication services (Facebook, Google, Apple) **[AVAILABLE SOON].**

A User who is also a user of at least one of the services that enables logging into the User Account, such as Facebook, Google or Apple, has the option of creating the Client Account and logging in using the account data held on one of these services. By registering with one of the external services, the User allows our Website to access the User's personal data included in the User's profile existing within the framework of a given service, to the extent necessary to create the Account.

If you're logging in with a Google account, we'll have your email address, first and last name, preferred language, and profile picture. Please note that sharing your profile picture with us is based on information published by Google, but we do not receive your picture when you log in or store it in our infrastructure. If you sign in with a Facebook account, the information we receive is your email address and information from your default public profile.

When logging in with an Apple account, Apple provides us with:

- your first and last name (you can choose whether to share real name or enter other data),
- your email address (Apple allows you to hide your real e-mail address by generating a unique proxy address (in the domain "@privaterelay.appleid.com"), which will forward messages to your real address. This proxy address is unique for each application or website),
- an authorization token — a token that an application or site receives from Apple to confirm that you have been properly authenticated. The token contains information about your session, such as your User ID (unique for each application) and confirmation of session validity.

You can check or change the information you have made available to applications and websites via the "Sign in with" function:

- in settings of your Google account,
- in the settings of your Facebook account in the section "Applications and Sites",
- in the settings of your Apple ID account (for more information, see HERE).

Your login information will be stored by us for the duration of your Subscription.

The purposes and legal bases for processing set out in Sections 1.2.1 and 1.2.2 of this document apply to the extent applicable.

1.2.4. Contact form in the User Account

From your Account level, you can use the contact form to make statements related to the Agreement or to send us notifications. We'll process this data when it's relevant:

- to fulfill our obligations under the Agreement [Article 6 (1) (b) GDPR],
- to pursue our legitimate interests, which include enabling users to reach out to us and address their questions [Article 6 (1) (f) GDPR].

We will retain the data for the duration of the correspondence relating to the matter with which you have contacted us, taking into account, where applicable, the duration of the Agreement and the statute of limitations on any claims that you may have against us and that we may have against you.

1.2.5. Adding devices to your Account

Within your Account, you can add devices that you can connect to remotely via our Software.

Adding a device involves processing the following data:

- device name,
- API key for device identification (this is a unique code used to identify and authorize a device or User in our Software),
- information about when the device was created in our Software as an instance of an object,
- MAC address,
- fingerprint identifier (this is a unique identifier assigned to a device that is used to recognize it in remote connection systems. It is generated based on specific characteristics of the device's hardware and software, such as hardware configuration, system settings or Software versions, and acts like a digital fingerprint, allowing the remote system to uniquely identify the device in question),
- type of device (whether it is a mobile device, PC or laptop),
- system type (Windows, Android),
- last IP address.

The data in question is processed in order to enable you to use certain features of our Software in connection with the concluded Agreement on the basis of Article 6 (1) (b) GDPR.

From your Account, you can manage the list of devices, including deleting them.

1.2.6. Sending invitations

From your Account level, you can create an invitation, to enable connection and control of your device. You can use the list of active invitations to view and remove selected invitations. The User you want to invite must have an active Account. When an invitation is sent, as well as when such invitation is received, the email address of the invited User is processed in order to enable the connection between the Users' devices in accordance with the concluded Agreement pursuant to Article 6 (1) (b) GDPR.

1.2.7. Remote connections

To establish a connection between devices, the status server uses the IP addresses of both devices. The location (country) of the connected device is used to find the optimal relay server (connection server), which is used when a direct P2P connection between devices is not possible due to network infrastructure.

The connection ID (the unique session number of a remotely connected device used to link a PC) or Stream ID (a unique session identifier used to manage individual remote connections, with each remote session assigned a different Stream ID, which allows the Software to monitor and differentiate between various connections within the system. This allows for the identification of which data belongs to which transmission, particularly in instances of multiple simultaneous connections) is used to identify the device to which the connection is made. The status server verifies the ability of both parties to establish a connection. This is done by checking the Stream ID status (to determine if a connection has already been established) and counting the number of active connections for a given User.

The data in question is processed in connection with the performance of the Agreement concluded with the User on the basis of Article 6 (1) (b) GDPR.

Device IP and location are stored only for the duration of the Application runtime. Connection ID and Stream ID exist only for the duration of the Application runtime.

All Remotly connections are secured with end-to-end encryption (E2EE), which ensures that data is encrypted on the sender's device and decrypted only on the recipient's device. The intermediary servers along the way do not have access to the transmitted data. This guarantees privacy protection and provides guarantees against access by third parties. Even if the data is intercepted during transmission, it will be encrypted and unreadable without the encryption key. The security of key exchange between parties is ensured by using RSA algorithms.

1.2.8. Technical support and improvement of our Software

For this purpose, we may process the following data where appropriate:

- logs (status server, Website logs),
- Client ID,
- User's email address,
- device ID,
- device location (country).

The processing in this case is based on our legitimate interest in providing support to our Users and improving our Software [Article 6 (1) (f) GDPR].

Device location information is processed only for the duration of the active session (when the device is logged into the system). The device identification data exists in the system as long as the device exists in our Software.

1.2.9. Mobile Application Crash analysis and repair and Mobile Application usage statistics

When you use our Mobile Application, the app store provider collects and provides us with anonymous information about Application crashes. The data set includes information on the type of mobile device, model, manufacturer and the location in the app code where the crash occurred.

In connection with Users' use of our Mobile Application, we also receive aggregated statistics, including information on application errors, number of launches and date and time of last use.

The information referred to above is not considered to be personal data.

For more information on how your app store processes your personal data, please refer to the privacy documentation it provides.

1.2.10. Ensuring security

To guarantee the security of our Services, we utilize automated mechanisms to prevent unauthorized attempts to guess passwords. After four unsuccessful attempts to log into the User's Account, access is blocked for 30 minutes. This type of action does not involve the processing of personal data.

Our Software employs an externally provided IP scoring service, which analyzes and verifies IP addresses. This process enables to assess potential risks associated with a given IP address, thereby enhancing the security level of our Services. To this end, we may transfer a User's IP address to a service provider based in the United States. The transfer in question is made in compliance with the applicable measures legalizing the transfer of personal data outside the European Economic Area (EEA). This includes the European Commission's decision of July 10, 2023, on the adequacy of data protection level with relation to MaxMind, LLC's participation in the "EU-U.S. Data Privacy Framework" program and, where applicable, Standard Contractual Clauses included in the contract with our service provider.

We take the actions referred to in this section on the basis of our legitimate interest in ensuring the security and integrity of our Services, our Software and the safety of our Users [Article 6 (1) (f) GDPR].

1.2.11. User support

If you wish to contact us regarding the use of our Software, you are welcome to use our Remotly Community forums. In this instance, our Privacy Policy for the www.remotly.com Website will apply. For more information on User support, please refer to the Agreement.

1.2.12. Processing of your data within the scope of our legal obligations and protection of our interests

In certain circumstances, we may process your personal data in order to comply with our legal obligations. This may include responding to inquiries from law enforcement or government agencies under Article 6 (1) (c) of the GDPR.

We may also process your personal data for the purpose of establishing, protecting and pursuing claims — based on our legitimate interest under Article 6 (1) (f) GDPR.

1.2.13. Servers

Our Software and Services rely on the functionality of servers to operate. We utilize servers provided by:

- OVH sp. z o.o. — state server. In this case we use the option of storing data only in the European Union.
- Amazon Web Services EMEA SARL — hosting for our Website, where the User creates an Account, together with Amazon CloudFront (CDN) service for content distribution. Accordingly, personal information that Users enter in forms available on our Website may be transmitted through the CDN server network. Amazon CloudFront works by accelerating the delivery of content, including dynamic queries such as form data, through edge servers located around the world. The data transfers in question will take place on the basis of applicable measures legalizing transfers of personal data outside the EEA including the European Commission's decision of July 10, 2023, on the

adequacy of data protection level with relation to the participation of Amazon Web Services, Inc. in the "EU-US Data Privacy Framework" program and the applicable Standard Contractual Clauses developed by the European Commission and concluded between us and the hosting provider.

- DigitalOcean, LLC, based in the United States — Remotly Community forum hosting. Accordingly, Users' data may be transferred outside the EEA pursuant to applicable measures legalizing transfers of personal data outside the EEA covering the European Commission's decision of July 10, 2023, on the adequacy of data protection level with relation to the participation of DigitalOcean, LLC in the "EU-U.S. Data Privacy Framework" program and, where applicable, Standard Contractual Clauses included in the contract with the hosting provider.

Furthermore, in order to enable Users to use the Software, we utilize relay servers, which are connection servers that facilitate the setup and maintenance of stable and secure connections.

The current list of relay servers is available HERE. You can set up your own connection servers in your Account settings.

As we point out in section 1.2.7. of this document, all Remotly connections are secured with end-to-end encryption (E2EE), which ensures that data is encrypted on the sender's device and decrypted only on the receiver's device. Intermediary servers along the way cannot access the data. Please note that even end-to-end encrypted data is subject to the provisions of the GDPR. Therefore, in the event that the remote connection uses servers located outside the EEA, or if the provider of such servers is a non-EEA entity, the relevant measures legalizing transfers of personal data outside the EEA will be taken into account. This includes the European Commission's decision of July 10, 2023, on the adequacy of data protection level with relation to the participation of the hosting provider in the "EU-US Data Privacy Framework" program and, where applicable, the applicable Standard Contractual Clauses developed by the European Commission and concluded between us and the hosting provider. Should you require a copy of the relevant clauses, please let us know via the contact form available on our Website www.remotly.com under "Contact".

2. RECIPIENTS OF YOUR PERSONAL DATA

In certain instances, we may disclose your data to:

- Persons authorized by us, our employees and associates who require access to the data in order to perform their duties.
- Processors to whom we outsource certain tasks related to the processing of personal data, such as companies that support our ICT systems or provide us with ICT tools or servers, consulting companies, accounting companies, suppliers of the tools we use and our advisors.
- Other entities that will process personal data as an independent data controller, e.g., Payment Operators.
- It may also include disclosure to public entities when required by law.

3. DATA RETENTION

The above sections of this document outline the retention periods for personal data, or, where applicable, the criteria for determining them. The retention periods are closely related to the specific purpose of processing and the related legal basis for such processing.

For general information on the principles for establishing data retention periods, please see below.

We are entitled to process personal data that we process based on your consent until you revoke your consent or until the processing of your personal data is no longer necessary to achieve the purpose for which the data was collected, or when the relevant purpose of the processing has been achieved and completed, whichever event occurs first.

We will process certain data on the basis of our legitimate interests until you raise any objection (unless we demonstrate that our interests are overridden by your interests or fundamental rights and freedoms, or grounds for establishing, pursuing or defending claims), or until the processing of your personal data is no longer necessary to achieve the purpose for which the data was collected, or when the relevant purpose of the processing has been achieved and completed, whichever event occurs first.

Where we process data to comply with our legal obligations, we will retain the data for as long as required by applicable law.

Notwithstanding the foregoing, inactive User Accounts, shall be deleted 1 year from the last successful login, unless the Account is covered by an active paid Subscription.

4. PROVISION OF PERSONAL DATA AS STATUTORY OR CONTRACTUAL REQUIREMENT

Provision of data is voluntary, but to the extent applicable, necessary for the execution of the Agreement and the use of our Services, including the use of the Software.

5. YOUR RIGHTS

In relation to the processing of your personal data, you have the following rights within the limits of the law and where applicable:

5.1. to request access to, rectification, and erasure of personal data or restriction of processing and to data portability,

5.2. in situations where we process your personal data on the basis of your consent, you have the right to withdraw your consent at any time, but this will not affect the lawfulness of the processing carried out on the basis of your consent prior to its withdrawal,

5.3. to object at any time to the processing of personal data on the grounds of our legitimate interest for reasons relating to your particular situation,

5.4. where your personal data is processed for direct marketing purposes, you have the right to object to the processing of your personal data for such marketing at any time,

5.5. if you believe that the processing of your personal data is not in accordance with the applicable European data protection law, you may lodge a complaint with the data protection supervisory authority in the country where you have your habitual residence, place of work or where the alleged breach occurred. A list of the competent authorities in each Member State can be found here.

You can exercise your rights by contacting us via the contact form available on our Website www.remotly.com under “Contact”.

We will endeavor to deal with your request promptly and to answer any questions you may have regarding the processing of your personal data. We will respond within 30 days of receiving your request. If this period is extended due to the complexity of the request or the number of requests we receive, we will inform you of the extension and the reasons for it.

If we have reasonable doubt as to the identity of the person making the request, we may request additional information necessary to confirm the identity of the person making the request. It is not compulsory to provide this information, but failure to do so will result in the request being refused.

We keep information about the requests we receive to demonstrate compliance in line with the principle of accountability referred to in the GDPR and to establish, protect and pursue claims.

6. CHANGES TO THE PRIVACY NOTICE

It is our goal to ensure that your personal data is as secure as possible. The information provided herein is subject to change as technology and our Services evolve. The latest Privacy Notice is always available on our Website.