

PRIVACY NOTICE FOR COMMERCIAL CLIENTS AND USERS OF REMOTLY SOFTWARE

This Privacy Notice explains how we collect, use, and safeguard the personal data of Users who access and use our Software and Services under a commercial Client Subscription (the "Client"), as defined in the LICENSE AND SERVICE AGREEMENT (the "Agreement").

We act as the data controller for personal data processed for our own purposes, as described below.

The processing of personal data of the Client's End Users ("End User") - where performed on behalf of the Client - and any data transmitted during remote connections established via Remotly Software are governed by the Data Processing Agreement. Personal data processing related to visits to our Website and use of its features is detailed in the [Privacy Policy](#) for www.remotly.com (the "Website").

Unless otherwise defined herein, all capitalized terms have the meanings set forth in the Agreement and, where applicable, in the [Website Terms of Service](#).

1. DATA PROCESSING IN CONNECTION WITH THE CONCLUSION OF THE AGREEMENT AND USE OF THE SOFTWARE

1.1. Data Controller

The controller of your personal data, within the meaning of Regulation (EU) 2016/679 (GDPR), is MIRILLIS CORE spółka z ograniczoną odpowiedzialnością, with its registered office in Zielona Góra, ul. Fabryczna 14B/1 (65-410), Poland, entered into the National Court Register under number KRS: 0001050325, NIP: 9292078550, REGON: 525981046 ("we").

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

1.2. Categories of Personal Data, Purposes, and Legal Bases for Processing

1.2.1. Registration of a Client Account by a Client Account User with Administrator Privileges

To register a Client Account, the following data must be provided:

- Email address
- Password
- Company name
- VAT number with country code
- Country

These data are processed by us in order to conclude and perform the agreement for maintaining the Client Account with the entity on whose behalf you are registering the Account, based on our legitimate interest [Art. 6(1)(f) GDPR].

Since creating a Client Account constitutes the conclusion of an Agreement with the Client (in the "trial" license version), the data are also processed for the purpose of concluding and performing this Agreement, pursuant to Art. 6(1)(f) GDPR, and additionally for the following purposes:

- Communicating with the Client Account User to confirm Account creation, based on our legitimate interest in verifying the accuracy of the data provided and ensuring the security of the Account and the Services offered through it [Art. 6(1)(f) GDPR],

- Performing additional verification during Account login using the “Remotly Login Token,” based on our legitimate interest in maintaining the security of the Account and the Services provided [Art. 6(1)(f) GDPR],
- Conducting onboarding communication with both the Client Account User and the End User regarding the use of the Software and its full functionality, based on our legitimate interest in introducing Users to the full potential of our Software [Art. 6(1)(f) GDPR],
- Sending email communications regarding the Subscription Service, based on our legitimate interest in maintaining contact with the Client in connection with the concluded Agreement [Art. 6(1)(f) GDPR],
- Establishing, exercising, or defending legal claims, based on our legitimate interest [Art. 6(1)(f) GDPR],
- Handling complaints in accordance with applicable legal requirements and fulfilling other legal obligations [Art. 6(1)(c) GDPR].

These data will be retained for the duration of the agreements referenced above, and - where applicable - for the additional period necessary to account for the statute of limitations on any claims that may be brought against us or that we may assert against the Client.

Providing the data described in this section is voluntary; however, it is required to conclude and perform the relevant agreements.

Regardless of the above, if the Client Account User with administrator privileges is also the Licensee, we may process their data as necessary to perform the license agreement set out in the LICENSE AND SERVICE AGREEMENT [Art. 6(1)(b) GDPR].

1.2.2. Switching to a Paid License Plan

To switch to a paid License Plan, the following additional data must be provided:

- First name
- Last name
- Address
- City
- Postal code
- Country

The purposes and legal bases for processing the Client Account User’s personal data, as well as the data retention period, remain the same as those outlined in section 1.2.1 above.

Providing the data specified in this section is voluntary; however, it is necessary to conclude and perform the Agreement with the commercial Client under the paid License Plan. Additionally, the selected country may influence the terms of the Services in accordance with the provisions of the Agreement.

For the paid License Plan, we will also process the Client Account User’s data, where applicable, for the following purposes:

- ensuring proper settlement of the Subscription Service [Art. 6(1)(f) GDPR],
- fulfilling our legal obligations, particularly under tax and accounting regulations, taking into account the data retention periods required by such laws [Art. 6(1)(c) GDPR],
- sending email communications related to the Subscription Service, including reminders about its expiration - based on our legitimate interest in maintaining communication with the Client in connection with the concluded Agreement [Art. 6(1)(f) GDPR].

The Client Account User with administrator privileges may delete the Account at any time via the Account settings. However, this does not affect our right to retain personal data associated with the Account to ensure proper settlement of the Services [Art. 6(1)(f) GDPR], fulfill legal obligations [Art. 6(1)(c) GDPR], and establish, exercise, or defend legal claims [Art. 6(1)(f) GDPR].

1.2.3. Adding End Users to the Client Account

The Client Account User with administrator privileges may add End Users to the Client Account, allowing them to use the Software under the Client's Subscription Plan.

To do so, the following data must be provided:

- End User name (used internally within the Client Account's admin panel as an alias),
- email address (used for logging into the End User Account; an invitation will be sent to this address).

The Client Account User with administrator privileges may also optionally provide the following additional data:

- first name,
- last name.

These data are processed on behalf of the Client in accordance with the Data Processing Agreement concluded with the Client.

Independently of the above, once the End User downloads the Software, they become a Licensee. As such, we will process their personal data to perform the Agreement (specifically its licensing provisions) [Art. 6(1)(b) GDPR], and, where applicable, for the purposes specified in sections 1.2.10 and 1.2.12–1.2.14 of this document.

1.2.4. Permission Manager - Granting Administrator Privileges to an End User

The Client Account User with administrator privileges may grant any number of End Users the same privileges. Such End Users then assume the rights and responsibilities of an administrator, and sections 1.2.1 and 1.2.2 apply accordingly.

1.2.5. Adding Devices to the Account

Users can add devices to their Account for remote access via our Software. This involves processing the following data:

- Device name
- API key (a unique code used to identify and authorize the device or User)
- Timestamp of device creation in the system
- MAC address
- Fingerprint identifier (a unique identifier generated based on hardware and software characteristics to recognize the device in remote connection systems)
- Device type (e.g., PC, laptop, mobile device)
- System type (e.g., Windows, Android)
- Last IP address

This data is processed to enable the User to utilize the features of our Software under the Agreement (licensing scope) [Art. 6(1)(b) GDPR]. Users may manage and remove devices via their Account settings.

1.2.6. Sending Invitations

From within your Account in the Software, you can create an invitation to allow another User to connect to and control your device. You can also view and manage active invitations, including deleting selected ones.

The invited person must have an active Account to accept the invitation. When sending or receiving an invitation, the invited User's email address is processed to enable the connection between Users' devices in accordance with the Agreement (specifically its licensing provisions), based on Art. 6(1)(b) GDPR.

1.2.7. Conducting Remote Connections

To establish a connection between devices, the state server uses the IP addresses of both devices. The location (country) of the device being connected to is used to select the optimal relay server when a direct peer-to-peer (P2P) connection is not possible due to network constraints.

To identify the device being connected to, the system uses a Connection ID (a unique Remotly session number used for device-to-PC connections) or a Stream ID (a unique identifier for each remote session, enabling tracking and differentiation of multiple simultaneous connections. It ensures that data is correctly assigned to the corresponding transmission).

The state server verifies whether a connection can be established between the parties, which includes checking the status of the Stream ID (e.g., whether it is already in use) and tracking the number of the User's active connections.

These data are processed for the purpose of performing the Agreement with the User (specifically, its licensing provisions), in accordance with Art. 6(1)(b) GDPR.

The IP address and location of the device are stored only while the Application is running. Similarly, the Connection ID and Stream ID exist only during the active session of the Application.

We record the duration of each connection initiated by the User. This information is sent by the Application during the session, in the same request that creates or updates the connection log. The recorded session time is used to:

- update connection logs, as described in section 1.2.9 of this Privacy Notice,
- calculate usage for the purposes of Subscription Service settlement, based on our legitimate interest in ensuring the proper operation and billing of the Subscription Service [Art. 6(1)(f) GDPR].

All Remotly connections are protected with end-to-end encryption (E2EE), meaning that data is encrypted on the sender's device and decrypted only on the recipient's device. Intermediary servers do not have access to the content of the communication. This ensures the confidentiality of transmitted data and prevents unauthorized third-party access. Even if data is intercepted in transit, it remains encrypted and unreadable without the appropriate decryption key. The security of key exchange between parties is ensured by RSA cryptographic algorithms.

Data transmitted between Users during a remote session is processed by us on behalf of the Client under the Data Processing Agreement concluded with the Client.

1.2.8. Using the QuickSupport or QuickHost Module under the Client's License Plan

When using these modules under the Client's License Plan, the Software processes the following data:

- Location (country)
- IP address of the device
- Application version

- Preferred relay server port (used to select the nearest relay server)

These data are processed to perform the Agreement with the User (specifically the licensing provisions related to the use of the Software), pursuant to Art. 6(1)(b) GDPR - this applies in particular to the QuickSupport Module. In cases where the QuickHost functionality is used to connect to a workstation assigned to a specific individual within a commercial Client's organization, the data are processed as necessary to pursue our legitimate interest in providing remote connection services to the commercial Client [Art. 6(1)(f) GDPR].

These data are retained only while the Software is running.

1.2.9. Remote Connection Logs

When using the Software, basic technical data regarding remote device connections are logged, including:

- Email address of the User who established the connection
- Name of the connected machine (if available) or connection ID
- Timestamp of connection start
- Duration of the connection

To enhance privacy, email addresses are replaced with unique User identifiers in the logs. The logs store the Client ID associated with each User. When logs are accessed by a Client Account User with administrator privileges, these IDs are mapped back to the corresponding email addresses on the Client side. As a result, our server does not store actual email addresses in connection logs.

Connection logs are available to Client administrators for the following durations:

- 60 days under the trial license
- 120 days under the Premium License Plan
- 210 days under the Ultimate and Enterprise License Plans

These data are processed on behalf of the Client in accordance with the Data Processing Agreement. The Client may configure shorter retention periods at their discretion.

1.2.10. Technical Support and Software Improvement

To provide technical support and improve our Software, we may process the following data, where applicable:

- Server logs (state server and Website)
- Client ID
- Email address
- Device ID
- Device location (country)

This processing is based on our legitimate interest in supporting Users and continuously enhancing our services [Art. 6(1)(f) GDPR]. Location data is processed only during active sessions. Device data remains in the system for as long as the device exists within the Software.

1.2.11. Mobile App Analytics and Crashes

When using our Mobile Application, the app store provider collects and shares with us anonymized information about Application crashes. This data may include the type of mobile device, model, manufacturer details, and the specific location in the Application code that triggered the crash.

Additionally, in connection with Users' use of the Mobile Application, we receive aggregated statistics such as error reports, the number of app launches, and the date and time of the last use.

The information described above does not contain any personal data.

For details on how your app store provider processes your personal data, please refer to the privacy documentation provided by them.

1.2.12. Ensuring Security

To enhance security, we implement mechanisms designed to prevent automated password guessing attempts. After four consecutive failed login attempts to an Account, access is temporarily blocked for 30 minutes. These security measures do not involve the processing of personal data.

Our Software also uses an externally provided IP scoring service to analyze and assess the risk level associated with a User's IP address, thereby strengthening the overall security of our Services. For this purpose, the User's IP address is transmitted to a provider based in the United States.

This transfer is carried out on the basis of appropriate safeguards that legitimize the transfer of personal data outside the European Economic Area (EEA), including the European Commission's adequacy decision of July 10, 2023, which recognizes an adequate level of personal data protection through MaxMind, LLC's participation in the EU-U.S. Data Privacy Framework. Where applicable, the transfer is also governed by [Standard Contractual Clauses](#) concluded with our provider.

The activities described in this section are carried out based on our legitimate interest in ensuring the security and integrity of our Services, our Software, and the protection of our Users [Art. 6(1)(f) GDPR].

1.2.13. User Support

If you need assistance with using the Software, we encourage you to use the [Remotly Community forum](#). In this context, the provisions of our Privacy Policy for www.remotly.com apply. Additional details about the User support process are outlined in the Agreement.

1.2.14. Processing User Data for Legal Obligations and Protection of Interests

We may process your personal data where necessary to comply with legal obligations, including responding to requests from law enforcement or regulatory authorities [Art. 6(1)(c) GDPR].

We may also process personal data to establish, exercise, or defend legal claims, based on our legitimate interest [Art. 6(1)(f) GDPR].

1.2.15. Servers

The use of our Software and Services would not be possible without the use of servers. For the processing of data covered by this document, we rely on infrastructure provided by the following suppliers:

- **OVH sp. z o.o.** - for the operation of the state server. In this case, we use the option to store data exclusively within the European Union.
- **Amazon Web Services EMEA SARL** - for hosting our Website (through which Users create Accounts) and for using the Amazon CloudFront (CDN) service to distribute content. Consequently, personal data entered by Users into Website forms may be transmitted through Amazon's global CDN server network. Amazon CloudFront accelerates content delivery, including dynamic requests (e.g., form submissions), via edge servers located worldwide. These data transfers are carried out on the basis of appropriate safeguards legalizing transfers outside the European Economic Area (EEA), including the European Commission's adequacy decision of July

10, 2023, recognizing an adequate level of personal data protection through **Amazon Web Services, Inc.'s** participation in the *EU-U.S. Data Privacy Framework*, as well as [Standard Contractual Clauses](#) adopted by the European Commission and concluded with our hosting provider.

- **DigitalOcean, LLC (USA)** - for hosting the **Remotly Community** forum. As a result, User data may be transferred outside the EEA based on safeguards including the European Commission's adequacy decision of July 10, 2023, based on **DigitalOcean, LLC's** participation in the *EU-U.S. Data Privacy Framework*, and, where applicable, [Standard Contractual Clauses](#) concluded with the provider.

In addition, to enable Users to use the Software, we rely on **relay servers**, which ensure the establishment and maintenance of stable, secure connections. The current list of intermediary servers is available [HERE](#). Users may also configure their own relay servers in the Account settings.

As described in section 1.2.7 of this Privacy Notice, all Remotly connections are protected by **end-to-end encryption (E2EE)**. This means data is encrypted on the sender's device and decrypted only on the recipient's device - intermediary servers have no access to the content of the data.

However, because even end-to-end encrypted data qualifies as personal data under the GDPR, we emphasize that if a remote connection involves servers located outside the EEA, or if the provider of such servers is based outside the EEA, such transfers are made with appropriate safeguards. These include the European Commission's adequacy decision of July 10, 2023 (e.g., for providers participating in the *EU-U.S. Data Privacy Framework*), and, where required, Standard Contractual Clauses concluded with the relevant hosting provider. These agreements are entered into in the **Processor-to-Processor** module, as data transmitted during User connections is processed by us on behalf of the Client.

2. RECIPIENTS OF YOUR PERSONAL DATA

Where applicable, personal data may be transferred to the following categories of recipients:

- **Authorized individuals** – including our employees and associates who require access to the data in order to perform their job responsibilities,
- **Processors** – i.e., entities to whom we outsource specific tasks related to personal data processing, such as companies managing our IT systems, providers of IT tools and server infrastructure, consulting service providers, tool suppliers, our legal and business advisors, and accounting offices - only to the extent that they process data on our behalf,
- **Independent data controllers** – such as Payment Operators, who process personal data on their own behalf and under their own responsibility,
- **Public authorities** – where disclosure is required under applicable law.

3. DATA RETENTION PERIOD

Retention periods for specific data categories are described in relevant sections above. Generally:

- **Consent-based processing:** Data is retained until consent is withdrawn or the purpose is fulfilled, whichever occurs first
- **Legitimate interest:** Data is retained until the data subject objects (unless we demonstrate overriding legitimate grounds), or until the purpose is fulfilled
- **Legal obligations:** Data is retained for the period required under the applicable legal provisions
- **Processing on behalf of the Client:** Retention is managed by the Client, who acts as the data controller. The Client may, for example, delete End User Accounts directly through the Client Account

4. VOLUNTARY PROVISION OF PERSONAL DATA

Providing personal data is voluntary. However, it is necessary to the extent required for concluding the Agreement and using our Services, including access to the Software.

5. YOUR RIGHTS

In connection with the processing of your personal data, you have the following rights, within the limits set by law and where applicable:

- 5.1. The right to access your data, and to request its rectification, erasure, or restriction of processing, as well as the right to data portability.
- 5.2. Where your data is processed based on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to its withdrawal.
- 5.3. The right to object at any time to the processing of your personal data based on our legitimate interests, on grounds relating to your particular situation.
- 5.4. The right to object at any time to the processing of your personal data for direct marketing purposes.
- 5.5. The right to lodge a complaint with a data protection supervisory authority in another country - particularly in the EU Member State of your habitual residence, place of work, or the place of the alleged infringement - if you believe that your personal data is being processed in violation of the GDPR. A list of competent supervisory authorities is available [HERE](#).

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

We are committed to handling your request promptly and to addressing any questions you may have regarding the processing of your personal data. We will respond no later than 30 days from the date of receiving your request. If an extension of this deadline is required due to the complexity of the request or the number of requests received, we will inform you accordingly and explain the reasons for the delay.

In cases of reasonable doubt as to the identity of the individual submitting a request, we may ask for additional information necessary to confirm your identity. Providing this information is voluntary; however, failure to do so may result in our inability to fulfill the request.

We retain records of received requests to demonstrate compliance with our obligations under the GDPR’s accountability principle and for the purposes of establishing, exercising, or defending legal claims.

6. CHANGES TO THE PRIVACY NOTICE

Our goal is to provide the highest level of protection for your personal data. As technology and our Services continue to evolve, the information contained in this document may be subject to change. The most up-to-date version of the Privacy Notice for Users is always available on our Website.