

## DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter referred to as the “Agreement”) is incorporated by reference into the “License and Service Agreement” concluded between MIRILLIS CORE limited liability company (hereinafter referred to as the “Service Provider” or “Processor”) and the commercial Client, hereinafter collectively referred to as the “Parties” or individually as a “Party”.

The Parties have concluded the “License and Service Agreement” (hereinafter referred to as the “Main Agreement”), the subject of which is the provision of Services to the commercial Client, as described and defined in the Main Agreement. As a result, the Processor will be entrusted with the processing of personal data to the extent specified in this Agreement.

All terms capitalized in this Agreement and not otherwise defined herein have the meaning assigned to them in the Main Agreement.

### 1. Entrustment of Personal Data Processing

- 1.1. This Agreement is a data processing agreement within the meaning of Article 28(3) of the GDPR.
- 1.2. The provisions of this Agreement also apply in cases where the commercial Client, acting as a processor of personal data on behalf of its principals, further entrusts the processing of such data to the Service Provider. In such cases, the Service Provider shall be deemed a sub-processor.
- 1.3. The provisions of this Agreement do not apply to personal data processed by the Service Provider in its capacity as an independent data controller, in accordance with applicable law. This applies even if such personal data, processed by the Service Provider as a controller, fully or partially overlap with the data entrusted to the Service Provider under this Agreement. Detailed information on how the Service Provider processes personal data of Clients and commercial Users as a controller is provided in the document entitled: „[Privacy Notice for the Client and Commercial User of Remotly Software](#)”.
- 1.4. The provisions of this Agreement do not apply to private Clients.

### 2. Subject of Processing

- 2.1. The subject of processing under this Agreement includes the Personal Data specified below (hereinafter referred to as “Personal Data” or “Data”).

#### Categories of Data Subjects:

- End Users of the commercial Client who have been included in the Client’s License Plan by being added to the Client Account.
- Other individuals whose personal data may be transferred in connection with the establishment of a remote connection, including through features or functionalities associated with such connection.

#### Types of Personal Data entrusted to the Processor for processing:

- End User identification data, such as the End User’s name and email address, as well as any additional data entered into the End User Account by the Client or the User (e.g., first name, surname).
- Data recorded in remote connection logs, as described in section 1.2.9 of the “Privacy Notice for the Client and Commercial User of Remotly Software.” This includes:
  - i. Email address of the User who initiated the connection (internally replaced by a unique User ID),

- ii. Name of the machine connected to (if available) or connection ID,
  - iii. Timestamp of connection start and connection duration.
- Notably, the Processor replaces the User's email address with a unique Client-associated User identifier in the connection logs stored on its servers. When an administrator-level Client Account User retrieves the list of logs, the Client ID is re-mapped to the corresponding email address on the Client's side. As a result, the Processor does not store the actual email addresses in its connection logs.
- Any other personal data transferred in the course of establishing or maintaining a remote connection, including data processed through features such as file transfer, voice chat, video chat, or session recording.

**Scope of Processing of Personal Data (operations performed on Personal Data processed on behalf of the commercial Client):**

- collection,
- recording,
- organization,
- structuring,
- storage, adaptation or alteration,
- retrieval,
- consultation,
- use,
- disclosure by transmission,
- dissemination or otherwise making available,
- alignment or combination,
- erasure or destruction.

**Scope of services under which the Processor is entrusted with the processing of Personal Data (purpose and nature of processing):**

- The Processor is entrusted with personal data for the purpose of performing the subject matter of the Main Agreement, specifically in the scope of:
  - i. Establishing and maintaining remote connections, including the use of additional functionalities such as voice chat, video chat, file transfer, and session recording;
  - ii. Managing and maintaining End User Accounts of the commercial Client.
- Personal data is processed in the Processor's IT systems in an automated manner.
- The nature of the processing is continuous and lasts for the duration of the Main Agreement.

### **3. Method of Data Processing**

- 3.1. To the extent this Agreement applies, the Processor shall process Personal Data solely on the basis of documented instructions from the commercial Client, unless processing is required under Union or Member State law to which the Processor is subject. The Main Agreement shall be deemed to constitute such a documented instruction, including any task assigned to the Processor by the commercial Client under the Main Agreement, whether issued in written or electronic form (each referred to as an "Instruction").
- 3.2. Any Instructions from the commercial Client that go beyond the scope of the Main Agreement require the prior written or electronic consent of the Service Provider, including agreement on any additional fees that may be payable by the Client for implementing such Instructions. Should

the Service Provider refuse to carry out such additional or amended Instructions, the commercial Client shall have the right to terminate this Agreement and the Main Agreement.

- 3.3. Taking into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing, as well as the risk to the rights and freedoms of natural persons - of varying likelihood and severity - the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. A current list of security measures applied by the Processor to Personal Data entrusted under this Agreement is available at [insert link]. The Processor may adopt alternative but equally effective security measures as technology evolves, provided that such changes do not reduce the overall level of protection.
- 3.4. The Processor may demonstrate compliance with the obligations referred to in Section 3.3, in particular, through adherence to an approved code of conduct as set forth in Article 40 of the GDPR, or through certification under an approved certification mechanism in accordance with Article 42 of the GDPR.
- 3.5. If the Processor has any doubts regarding the lawfulness of an Instruction - particularly its compliance with data protection laws - it shall promptly inform the commercial Client, who will assess the validity and legality of the Instruction.
- 3.6. The Processor shall ensure that only persons who are duly authorized and bound by confidentiality obligations are permitted to process Personal Data on its behalf.
- 3.7. The Processor undertakes to maintain the confidentiality of all information and Personal Data accessed in connection with the performance of the Main Agreement, except where disclosure is required by applicable law. In such cases, the Processor shall promptly notify the commercial Client, unless prohibited from doing so by law.
- 3.8. Taking into account the nature of the processing, the Processor shall assist the commercial Client, to the extent possible and through appropriate technical and organizational measures, in fulfilling its obligation to respond to requests from data subjects in the exercise of their rights under Chapter III of the GDPR.

#### **4. Reporting of Personal Data Breaches**

- 4.1. The Processor shall promptly notify the commercial Client of any Personal Data breach without undue delay after becoming aware of it. Where possible, the Processor shall also take all reasonable measures to mitigate any potential adverse effects resulting from the breach.
- 4.2. The notification referred to in Section 4.1 shall be delivered to the email address designated by the commercial Client in its Client Account.

#### **5. Consent for Subprocessing**

- 5.1. The commercial Client grants the Processor a general authorization to engage subprocessors for the further processing of Personal Data, to the extent and for the purpose necessary to perform the subject matter of the Main Agreement.
- 5.2. A current list of subprocessors engaged by the Processor is available on the Processor's website at <https://remotly.com/legal>.

- 5.3. The Processor shall inform the commercial Client in advance of any intended addition or replacement of subprocessors. This notification must occur before the new subprocessor begins processing Personal Data, allowing the commercial Client a period of 14 days from the date of notification to raise any objections.
- 5.4. If no objection is submitted within the 14-day period, the change shall be deemed accepted. Should the commercial Client object, it must provide a written (including electronic) justification for the objection. The justification must specify which technical and organizational measures applied by the proposed subprocessor are deemed insufficient, and on what basis this conclusion was reached - such as the results of an audit, a known data breach, or a sanction imposed by a supervisory authority as defined under the GDPR.
- 5.5. In the case of a justified objection submitted in accordance with the above requirements, the commercial Client shall have the right to withdraw from the services provided under the Main Agreement.
- 5.6. Notification of any intended changes to subprocessors will be provided either:
- i. by updating the list of subprocessors on the Processor's website, or
  - ii. via email to the address provided in the Client Account, provided the commercial Client has opted in to receive such notifications by selecting the appropriate option in the Client Account settings.
- 5.7. The Processor shall enter into a written agreement with each subprocessor that imposes the same data protection obligations as those set out in this Agreement, including the obligation to implement appropriate technical and organizational measures to ensure compliance with applicable data protection laws.
- 5.8. If a subprocessor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the commercial Client for the performance of the subprocessor's obligations.

## **6. Cooperation Regarding Obligations under Articles 32–36 of the GDPR**

- 6.1. Taking into account the nature of the processing of the entrusted Personal Data and the information available to the Processor, the Processor shall assist the commercial Client, in its capacity as data controller, in fulfilling its obligations under Articles 32 to 36 of the GDPR. If, in the Processor's reasonable opinion, the requested assistance exceeds standard support, the Processor may charge an additional fee for such services. The Processor shall inform the commercial Client in advance of the applicable fees and estimated completion time. The provision of such additional assistance shall commence only upon the commercial Client's acceptance of the terms.

## **7. Cooperation Regarding Data Subject Rights**

- 7.1. In cases where data subjects exercise their rights under data protection legislation by submitting requests to the commercial Client via the Processor, the commercial Client shall remain solely responsible for responding to such requests.

## **8. Transfer of Personal Data to Third Countries**

- 8.1. The Service Provider may engage subprocessors located outside the European Economic Area (EEA) for the processing of Personal Data in connection with the performance of the Main Agreement, provided that the requirements set forth in Articles 45 or 46 of the GDPR are met.
- 8.2. Where the provision of services under the Main Agreement requires the transfer of Personal Data to a third country – particularly in connection with the provision of services based on the operation of servers located worldwide – the Service Provider shall ensure that such transfers are carried out in compliance with Articles 45 or 46 of the GDPR, and that appropriate safeguards, as defined therein, are implemented. Such transfers shall be deemed to constitute documented Instructions from the commercial Client under the Main Agreement.
- 8.3. In the situations referred to in Sections 8.1 and 8.2, the Service Provider shall, upon each documented request by the commercial Client, provide information concerning the transfer of Personal Data to third countries, and, where applicable, the safeguards applied in accordance with Article 46 of the GDPR.
- 8.4. Sections 8.1 to 8.3 shall not apply where the commercial Client or its Users independently initiate or configure data transfers through the Software, such as by requesting a connection to an endpoint located outside the EEA or by configuring a custom connection server. In such cases, the commercial Client is solely responsible for ensuring that any resulting data transfer complies with applicable data protection laws.

## **9. Audit**

- 9.1. The Processor shall make available to the commercial Client all information necessary to demonstrate compliance with its obligations under this Agreement and shall allow for and cooperate with audits or inspections conducted by the commercial Client or auditors authorized by the commercial Client, including by supporting verification and remediation efforts.
- 9.2. Audits as referred to in Section 9.1 may be conducted no more than once every 12 months, unless a Personal Data breach has occurred at the Processor, as confirmed by a supervisory authority within the meaning of the GDPR.
- 9.3. The commercial Client shall notify the Processor of a planned audit or inspection at least 30 days in advance, specifying the persons authorized to conduct the audit, in order to jointly agree on the date and scope of the audit.
- 9.4. The commencement of the audit shall be conditional upon the Parties entering into appropriate confidentiality agreements.
- 9.5. The audit may be conducted on business days during the Processor's regular working hours by individuals specifically designated by the commercial Client. These individuals shall be entitled to request information from the Processor concerning the processing of Personal Data.
- 9.6. Individuals designated by the commercial Client to conduct the audit must not engage in any competitive activity against the Processor and must not be employed (under an employment or civil law contract) by any entity engaged in such activity.
- 9.7. All audits or inspections carried out by or on behalf of the commercial Client shall be conducted at the Client's expense. However, the Processor shall provide reasonable assistance necessary for the audit without charging additional fees.

- 9.8. For audit time exceeding two (2) working hours, the Processor shall be entitled to charge a fee. The amount of this fee shall be communicated to the commercial Client prior to the commencement of the audit and shall be calculated based on an hourly rate that reflects the Processor's costs associated with the involvement of its personnel.

## **10. Processor's Liability for Non-Compliance**

- 10.1. The Processor's liability to the commercial Client for any claims, damages, liabilities, losses, or costs arising from a breach of this Agreement or from unlawful processing of Personal Data by the Processor shall be limited to the total amount of fees paid by the commercial Client to the Processor for data processing services during the twelve (12) months preceding the event giving rise to the claim.

## **11. Duration of Personal Data Processing**

- 11.1. This Agreement shall remain in force for the duration of the Main Agreement.
- 11.2. Upon termination or expiry of the Main Agreement, the Processor shall, at the choice of the commercial Client, either delete or return all entrusted Personal Data and delete all existing copies thereof, unless Union or Member State law requires the continued storage of such Personal Data.
- 11.3. The provisions of this Agreement shall continue to apply beyond the termination of the Main Agreement and remain in effect until all Personal Data entrusted by the commercial Client has been permanently deleted or returned.

## **12. Final Provisions**

- 12.1. This Agreement enters into force on the date of execution of the Main Agreement.
- 12.2. In the event of any conflict between the provisions of this Agreement and the provisions of the Main Agreement, the provisions of this Agreement shall prevail.
- 12.3. This Agreement supersedes any prior agreements or arrangements between the Parties concerning the processing and protection of Personal Data in connection with the performance of the Main Agreement.
- 12.4. Any amendments or additions to this Agreement shall be made in the same manner as amendments to the Main Agreement, as set out therein.
- 12.5. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall remain valid and enforceable to the fullest extent permitted by law.
- 12.6. All matters not expressly regulated by this Agreement shall be governed by applicable law, in particular the provisions of the GDPR and other relevant data protection legislation.
- 12.7. Any disputes arising between the Parties in connection with this Agreement shall be subject to the jurisdiction of the court having competence over the Processor's registered office.