Data Processing Addendum (“DPA”)

Last updated: 1 October 2025

This Data Processing Addendum (hereinafter DPA’) supplements the Terms of use (hereinafter ‘Terms’), the agreement between you (hereinafter ‘User’ ‘Customer’, ‘you’, ‘your’) and RO App (meaning the legal entity with which Customer has a contractual relationship according to the Terms, hereinafter ‘Company’,‘we’, ‘us’ or ‘our’) which is governing the processing of personal data that you upload or otherwise provide RO App in connection with the Software or of any personal data that RO App obtains in connection with the performance of the Software, hereinafter referred to individually as a ‘Party’ or together as the ‘Parties’.

Unless otherwise defined in this DPA, all capitalized Terms used in this DPA will have the meanings set forth in Terms. This DPA shall remain in force until the termination of the Terms between you and us governing your use of the Software.

1. Background

1.1 The Client has agreed to the Terms, according to which RO App has agreed to provide certain services to Client (“Services”).

1.2 When providing the Services, RO App may collect, gain access to, or otherwise Process Personal Data of individuals (Data Subjects) on behalf of Client. Unless otherwise agreed to between the Parties, Client will be the Data Controller, and RO App will be the Data Processor of such Personal Data.

1.3 This DPA specifies the data protection obligations of the Parties under the Terms. It applies to all activities performed by RO App in connection with the Terms in which RO App, its staff, or a third party acting on behalf of Ro App comes into contact with Personal Data as a Data Processor on behalf of the Client.

1.4 The DPA is based on the provision of Article 28 of the GDPR and the definitions contained in the GDPR.

1.5 If there is a conflict between the terms of the Terms and those of this DPA, the provisions of this DPA will prevail.

2. Definitions

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, the United Kingdom, Brazil, applicable to the processing of personal data under the Terms as amended from time to time, such as GDPR, UK Data Protection Laws, or other applicable laws and regulations.

“General Data Protection Regulation (GDPR)” means 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.

“UK Data Protection Laws” means the Data Protection Act 2018 and the UK GDPR (retained version of the EU GDPR).

“EU Standard Contractual Clauses (EU SCCs)” means Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

“UK Addendum” means International Data Transfer Addendum to the EU Standard Contractual Clauses that has been issued by the Information Commissioner for Parties making Restricted Transfers in the meaning of the UK Data Protection Laws, as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

“controller”, “processor”, “data subject”, “personal data”, and “processing” have the meanings given in Data Protection Laws and Regulations.

“Customer Data” means personal data that you upload or otherwise provide Company in connection with the Software or of any personal data that the Company obtains in connection with the performance of the Software.

“Sub-processor” means any entity that provides processing Software to the Company in furtherance of Company processing on behalf of the Customer.

“Public Authority” means a government agency or law enforcement authority, including judicial authorities.

“Supervisory Authority” means an independent public authority to be responsible for monitoring the application of the data protection legislation.

3. Details of Processing

3.1 Purpose of Processing. Subject to Section 5.1 below, RO App will Process Personal Data in connection with the Terms only for the purpose of providing and maintaining the Services. RO App will carry out the Processing operations in accordance with the Terms, as well as any reasonable Instructions received from Client that do not conflict with the provisions of this DPA, the Terms, or Data Protection Laws. Copies or duplicates of any Personal Data made available hereunder may only be compiled as may be technically required for the provision of the Services, or required for lawful data retention.

3.2 Nature of Processing. RO App is a cloud-based, self-service, SaaS (software as a service) CRM (customer relationship management) tool. Personal Data will be Processed in accordance with the Terms and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide and maintain the Services;

- Disclosure in accordance with the Terms and/or as compelled by applicable laws.

3.3 Controller Instructions. The Parties agree that the Terms together with the Client's use of the Services constitute the Client's complete and final Instructions to RO App in relation to the Processing of Personal Data, and any additional Instructions outside the scope of the Instructions shall require prior written agreement between the Parties.

3.4 Categories of Data Subjects. RO App will not have any knowledge or control over the categories of Data Subjects whose Personal Data the Client may elect to record or upload into the Services, except as provided in the Terms. Personal Data to which RO App may receive access usually concerns, in particular, the following categories of Data Subjects:

- Client's directors, officers, employees, interns, trainees, agents, contractors, job applicants, customers, suppliers, subcontractors, business contacts; and
- Any other individuals for which Client enters Personal Data or information into the Services.

3.5 Categories and Nature of Personal Data. RO App will not have any knowledge or control over the categories or nature of the Personal Data that Client may elect to record or upload into the Services, except as provided in the Terms. The Processing activities will generally include the following categories of Personal Data:

- Name, title, street address, email address, phone number, other contact information;
- Customer history;
- IP addresses;
- Free-text notes, such as references and meeting notes, as entered by Client; and
- Other data collected by Client and entered or uploaded into the Services, the nature of which is determined solely by Client.

In accordance with the restrictions of Section 7.3 of the Terms, the Parties do not anticipate the Processing of Sensitive Information.

4. Your obligations

Within the scope of the DPA and Terms and your use of the Software, including our integrations, you will be solely responsible for complying with all requirements that apply to you under the Data Protection Laws and Regulations. You represent and warrant that you will be solely responsible for:

- (i) the accuracy, quality, integrity, confidentiality and security of collected Customer Data;
- (ii) complying with all necessary transparency, lawfulness, fairness and other requirements under Data Protection Laws and Regulations for the collection and use of personal data by: establishing and maintaining the procedure for the exercise of the rights of the data subjects whose personal data are processed on behalf of Customer; providing us only with data that has been lawfully and validly obtained and ensuring that

such data will be relevant and proportionate to the respective uses; ensuring compliance with the provisions of this DPA and Terms by your personnel or by any third-party accessing or using Customer Data on your behalf; and

- (iii) ensuring that your Instructions to us regarding the processing of Customer Data comply with the Data Protection Laws and Regulations, including complying with principles of data minimisation, purpose and storage limitation.

5. Our obligations

5.1. General Obligations

With regard to the processing of Customer Data we shall:

- (i) process Customer Data using appropriate technical and organisational security measures, and in compliance with the Instructions received from the Customer subject to Section 3 of this DPA;
- (ii) inform Customer if, in our opinion, a Customer's Instructions may be in violation of the provisions of the Data Protection Laws and Regulations;
- (iii) follow Customer's instructions regarding the collection of Customer Data, in case we are obtaining Customer Data from data subjects on behalf of Customer under Terms;
- (iv) take reasonable steps to ensure that any employee/contractor to whom we authorize access to Customer Data on our behalf comply with respective provisions of the Terms and this DPA.

5.2. Notices to Customer

Upon becoming aware, we shall inform you of any legally binding request for disclosure of Customer Data by a Public Authority, unless we are otherwise forbidden by law to inform the Customer, for instance, to preserve the confidentiality of investigation by a Public Authority. We will inform the Customer if it becomes aware of any notice, inquiry, or investigation by a Supervisory Authority with respect to the processing of Customer Data under this DPA conducted between you and us.

5.3. Security measures

We shall implement and maintain appropriate technical and organizational measures to protect Customer Data from personal data breaches (hereinafter 'Security Incidents'), in accordance with our security standards set out in Annex 1 of this DPA. You acknowledge that security measures are subject to technical progress so that we may modify or update Annex 1 of this DPA at our sole discretion provided that such modification or update does not result in a material degradation in the security measures offered by Annex 1 of this DPA.

5.4. Security Incident

Upon becoming aware of a Security Incident, we shall:

- (i) notify you without undue delay after we become aware of the Security Incident;

- (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by you; and
- (iii) promptly take reasonable steps to contain and investigate any Security Incident so that you can notify competent authorities and/or affected Data Subjects of the Security Incident. Our notification of or response to a Security Incident shall not be construed as an acknowledgment by us of any fault or liability regarding the Security Incident.

5.5. Confidentiality

We will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Software, or as necessary to comply with contractual and legal obligations or binding order of a public body (such as a subpoena or court order). We shall ensure that any employee/contractor whom we authorize to access Customer Data on our behalf is subject to appropriate confidentiality contractual or statutory duty obligations with respect to Customer Data.

5.6. Return or deletion of Customer Data

Upon request or expiration of the Terms (25 months) concluded between you and us, we shall delete all Customer Data in our possession or control; except that this requirement shall not apply to the extent, we are required by applicable law or respective contractual obligations to retain some or all of the Customer Data.

5.7. Reasonable Assistance

We agree to provide reasonable assistance to the Customer regarding:

- (i) any request from a data subject in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Data that we process on behalf of Customer. In the event that a data subject sends such a request directly to us, Section 7 of this DPA shall apply;
- (ii) the investigation of Security Incidents and communication of necessary notifications regarding such Security Incidents subject to Section 6.4 of this DPA;
- (iii) preparation of data protection impact assessments and, where necessary, consultation of Customer with the Supervisory Authority under Articles 35 and 36 of the GDPR.

5.8. Audit and Certification

If a Supervisory Authority requires an audit of the data processing facilities from which we process Customer Data to ascertain or monitor Customer's compliance with Data Protection Laws and Regulations, we will cooperate with such audit. The Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time we expend for any such audit, in addition to the rates for Software performed by us.

Customer may, prior to the commencement of processing, and at regular intervals, thereafter, audit the technical and organizational measures taken by us. If Customer is the controller with

respect to the personal data processed by us on its behalf, upon reasonable and timely advance agreement, during regular business hours and without interruption to our business operations, we may provide Customer with all information necessary to demonstrate compliance with its obligations laid down in the Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer with respect to such processing.

We shall, upon Customer's written request and within a reasonable period, provide Customer with all information necessary for such audit, to the extent that such information is within our control and we are not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

6. Data Subject Request

In the event that a data subject contacts us with regard to the exercise of their rights under Data Protection Laws and Regulations (in particular, requests for access to, rectification or deletion of Customer Data), we will use all reasonable efforts to forward such requests to you. If we are legally required to respond to such a request, we shall immediately notify you and provide you with a copy of the request unless we are legally prohibited from doing so.

7. Sub-processors

You agree that we may engage Sub-processors to assist in fulfilling our obligations with respect to the provision of the Software under the Terms. The agreed list of Sub-processors is set out in Annex 2 of this DPA.

8. Transfers of Customer Data

8.1. General

Parties agree that when the processing of Customer Data on behalf of Customer in connection with Software constitutes a transfer under Data Protection Laws and Regulations and appropriate safeguards are required, such processing will be subject to the Standard Contractual Clauses and/or UK Addendum which are deemed to incorporated into and form part of this DPA as further described in subsections 9.2 and 9.3 of this DPA. If and to the extent the EU SCCs and/or UK Addendum, as applicable, conflict with any provision of the DPA, the EU SCCs and UK Addendum shall prevail to the extent of such conflict

8.2. Transfers under GDPR

When the processing of Customer Data on behalf of the Customer in connection with Software constitutes a "transfer" under GDPR, Standard Contractual Clauses shall apply. When you are a controller and we are a processor, Module Two of the EU SCCs shall apply, and when you are a processor and we are a sub-processor, Module Three of the EU SCCs shall apply.

For the purpose of the EU SCCs, we are a "data importer" and you are a "data exporter". The relevant provisions contained in the EU SCCs are incorporated by reference and are an integral part of this DPA. Clauses and annexes of the EU SCCs deemed to be completed as follows:

8.3. Transfers under UK Data Protection Laws

When the processing of Customer Data on behalf of Customer in connection with Software constitutes a “restricted transfer” under UK Data Protection Laws, UK Addendum shall apply. When you are a controller and we are a processor, Module Two of the EU SCCs shall apply, and when you are a processor and we are a sub-processor, Module Three of the EU SCCs shall apply, as completed in subsection 9.2 of this DPA.

For the purpose of the UK Addendum, we are an “Importer” and you are a “Exporter”. The relevant provisions contained in the UK Addendum are incorporated by reference and are an integral part of this DPA. Tables in the UK Addendum deemed to be completed as follows:

ANNEX 1 - TECHNICAL AND ORGANIZATIONAL MEASURES

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

- The data importer is committed to preserving the confidentiality, integrity, availability and resilience of all the personal data in question throughout the data importer processing activities and ensuring that personal data are protected against loss and destruction by implementing appropriate internal information security policies and procedures.
- The data importer has adopted anonymisation and pseudonymisation policies that are designed to protect the privacy of data subjects by ensuring the security of personal data processing.
- The data importer has implemented measures designed to ensure that personal data, in the event of a physical or technical incident, may be restored in a timely manner.
- The data importer maintains a regular schedule of operating system and software updates to its equipment and other devices. Also, all servers of the data importer are protected by firewalls that are maintained and supplied with updates and patches.
- The data importer has implemented measures designed to deny unauthorized persons access to processing equipment used for processing of personal data and prevent the use of automated processing systems by unauthorized persons. All data importer's staff members have a randomly generated password in accordance with the data importer's password policy. The personal data is subject to a strictly need-to-know principle of access and can be displayed to authorized users only.
- The data importer has implemented measures designed to ensure that the confidentiality and integrity of personal data are protected during transfers of personal data.
- The data importer has implemented measures designed to prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data.
- The data importer has implemented the following measures for ensuring the physical security of locations at which personal data are processed:
    - **all staff members must work only using the data importer's equipment;**
    - equipment is accounted for and has an identified owner;

    - anytime when staff member stops performing their work, they must block access to their equipment;
    - the data importer has a security alarm system;
    - access to the data importer's facilities is strictly regulated;
- The data importer has implemented measures designed to ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input.
- The data importer's staff shall comply with the data importer's internal information security policies, procedures, and other applicable documents. It is required to read the current version of such documents to any staff member before undertaking any of their responsibilities regarding personal data processing. All staff members shall receive appropriate security training or instructions concerning the processing of personal data.
- The data importer always checks whether its hosting providers are SOC 2 certified in order to ensure the hosting provider securely manages personal data. In addition, the data importer engages an independent security code auditor who conducts source code review to discover if there are any potential security weaknesses, bugs, exploits or violations of programming standards.
- The data importer has adopted information security policies, procedures and other documents for ensuring the fulfillment of data minimization, data quality, limited data retention and accountability principles and ensuring system configuration.
- The data importer has implemented a user data detection policy that ensures that data subjects can enjoy their rights under the GDPR, including the right to erasure for deletion of their accounts and related personal data.

ANNEX 2 - SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Sub-processor 1

Name: Scaleway SAS
Entity country: France
Description of processing: All Customer Data stored by the Customer

Sub-processor 2

Name: Cloudflare Germany GmbH
Entity country: Germany
Description of processing: End-User or Agent IP address

Sub-processor 3

Name: IP Telecom Bulgaria LTD
Entity country: Bulgaria
Description of processing: Call recordings, phone numbers and call metadata

Sub-processor 4

Name: Intercom R&D Unlimited Company
Entity country: Ireland
Description of processing: Conversations (and any data Customer would share) between the Customer and our Support team

Sub-processor 5

Name: AMAZON WEB SERVICES EMEA SOCIÉTÉ À RESPONSABILITÉ LIMITÉE
Entity country: Luxemburg
Description of processing: All Customer Data stored by the Customer

Sub-processor 6

Name: Pipedrive OU
Entity country: Estonia
Description of processing: Customer Data

Sub-processor 7

Name: RETENTION YES SP. Z.O.O.
Entity country: Poland
Description of processing: Customer Email addresses

Sub-processor 8

Name: Autoiso Sp. z o.o.
Entity country: Poland
Description of processing: Clients' WIN numbers

Sub-processor 9

Name: PPG DIGITAL Sp. z o.o.
Entity country: Poland
Description of processing: Customer Payment Data

Sub-processor 10

Name: MessageBird B.V. (SparkPost.com)
Entity country: Netherlands
Description of processing: Customer Transaction Data, Customer Data, Client Data

Sub-processor 11

Name: KNK Building Services Ltd (IMEIDB.XYZ)
Entity country: UK
Description of processing: Clients' IMEI numbers

Sub-processor 12

Name: OpenAI Ireland Ltd
Entity country: Ireland
Description of processing: Provides large language model processing via APIs for customers using Intercom's AI Products

Sub-processor 13

Name: Google Cloud EMEA Limited.
Entity country: Netherlands
Description of processing: All Customer Data stored by the Customer