

DATA PROTECTION AGREEMENT FOR ORDER DATA PROCESSING PURSUANT TO ART. 28 OF THE EU GENERAL DATA PROTECTION REGULATION

This Agreement is entered into between
Recrea Systems SLU and 55 Degrees AB on Monday, 14 November 2022

PARTIES

1. 55 Degrees AB, incorporated and registered in Sweden with company registration number 559201-6843 and having its registered office at Nordenskiöldsgatan 24 211 19 Malmö, hereafter “Data Controller”,
2. Recrea Systems, SLU, incorporated and registered in Spain with company registration number B35635648 and having its registered office at Bravo Murillo, 34, Las Palmas de Gran Canaria, hereafter “Data Processor”,

The Data Controller and the Data Processor may be referred to individually as a “Party” and collectively as the “Parties”.

WHEREAS

- (A) The Data Controller wishes to subcontract certain Services (as defined below), which imply the processing of personal data, to the Data Processor.
- (B) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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 (General Data Protection Regulation).
- (C) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS

1. Definitions and Interpretation

- 1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
 - 1.1.1. “Agreement” means this Data Processing Agreement and all Schedules, if any.
 - 1.1.2. “Confidential Information” means all information disclosed by a Party to the other Party pursuant to this Agreement which is either designated as proprietary and/or confidential, or by its nature or the nature of the circumstances surrounding disclosure, should reasonably be understood to be confidential, including (but not limited to), information on products, customer lists, price lists and financial information.
 - 1.1.3. “Schedule” means a schedule to the Data Processing Agreement and which forms an integral part of the Agreement.
 - 1.1.4. “Service” means the software as a service (SaaS) offered by Quaderno and having a variety of resources including but not limited to tax calculations, receipts generation, emailing to customers and other functionalities as developed and introduced by Quaderno from time to time.
- 1.2. The clause headings in this Agreement are for reference purposes only and shall not be used in the interpretation thereof.

2. Object of this Agreement

- 2.1. The Data Processor shall perform the Services in accordance with the provisions of the Agreement.

3. Relationship between the Parties

- 3.1. None of the provisions of this Agreement can be interpreted as indicating the intent of the Parties to form a company, association or joint venture.

4. Duration and Termination

- 4.1. The duration of this Agreement is as long as the Data Controller uses the services of the Data Processor.
- 4.2. Either Party shall have the right to terminate the Agreement, partially or entirely, forthwith by sending a written notice of termination to the other Party, if any of the following events occur:

- 4.2.1. the other Party materially breaches any of its obligations under this Agreement
 - 4.2.2. the other Party breaches any of its obligations under this Agreement and, notwithstanding a written request from the non-breaching Party to remedy such a breach, fails to comply with such a request within a period of thirty (30) days following such notice;
 - 4.2.3. an event of force majeure prevails for a period exceeding three (3) months; or
 - 4.2.4. the other Party becomes insolvent or enters liquidation, a petition in bankruptcy is filed for it or a receiver is appointed.
- 4.3. Upon the termination or expiry of this Agreement, any rights and obligations of the Parties, accrued prior to the termination or expiry thereof shall continue to exist.
- 4.4. Upon termination or expiry of the Agreement, or at any earlier moment if the personal data are no longer relevant for the delivery of the Services, at the choice of the Data Controller, the Data Processor shall return all the personal data to the Data Controller, and securely delete existing copies unless a law or regulation requires the storage of the personal data.
- 4.5. The provision of articles 5, 6, and 7 of this Agreement shall survive the termination of this Agreement.

5. Data Protection

- 5.1. As the performance of the Agreement and the delivery of the Services implies the processing of personal data, the Data Controller and the Data Processor shall comply with the applicable data protection legislation and regulations.
- 5.2. The Data Processor shall ensure that in relation to personal data disclosed to it by, or otherwise obtained from the Data Controller, it shall act as the Data Controller's data processor in relation to such personal data and shall, therefore:
- 5.2.1. from 25 May 2018, create and maintain a record of its processing activities in relation to this Agreement; the Data Processor shall make the record available to the Data Controller, any auditor appointed by it, and/or the supervisory authority on the first request;
 - 5.2.2. not process the personal data for any purpose other than to deliver the Services and to perform its obligations under the Agreement in accordance with the documented instructions of the Data Controller; if it cannot provide such compliance, for whatever reasons, it agrees to promptly inform the Data Controller of its inability to comply;
 - 5.2.3. inform the Data Controller immediately if it believes that any instruction from the Data Controller infringes applicable data protection legislation and regulations;

- 5.2.4. not disclose the personal data to any person other than to its personnel as necessary to perform its obligations under the Agreement and ensure that such personnel is subject to statutory or contractual confidentiality obligations;
 - 5.2.5. take appropriate technical and organizational measures against any unauthorized or unlawful processing, and evaluate at regular intervals the adequacy of such security measures, amending these measures where necessary.
 - 5.2.6. ensure that access, inspection, processing, and provision of the personal data shall take place only in accordance with the need-to-know principle, i.e. information shall be provided only to those persons who require the personal data for their work in relation to the performance of the Services;
 - 5.2.7. promptly notify the Data Controller about (i) any legally binding request for disclosure of the personal data by a data subject, a judicial or regulatory authority unless otherwise prohibited, such as the obligation under criminal law to preserve the confidentiality of a judicial inquiry, and to assist the Data Controller therewith (ii) any accidental or unauthorized access, and more in general, any unlawful processing and to assist the Data Controller therewith;
 - 5.2.8. deal promptly and properly with all reasonable inquiries from the Data Controller relating to its processing of the personal data or in connection with the Agreement;
 - 5.2.9. make available to the Data Controller all information necessary to demonstrate compliance with the applicable data protection legislation and regulations;
 - 5.2.10. at the request and costs of the Data Controller, submit its data processing facilities for audit or control of the processing activities;
 - 5.2.11. refrain from engaging another data processor without the prior consent of the Data Controller; the list of other data processors engaged by the main data processor is found under Schedule 1
 - 5.2.12. assist the Data Controller, subject to reasonable additional compensation, with the Data Controller's obligation under applicable data protection laws and regulations.;
- 5.3. Personal data processed in the context of this Agreement may not be transferred to a country outside the European Economic Area without the prior consent of the Data Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved standard contractual clauses for the transfer of personal data.

6. Confidentiality

- 6.1. Each Party acknowledges that during this Agreement, a Party (the “receiving Party”) may become privy to Confidential Information which is disclosed by the other Party (the “disclosing Party”).
- 6.2. The receiving Party shall keep all Confidential Information confidential. The receiving Party shall not disclose Confidential Information to any third party, and shall not use Confidential Information for any purposes other than for the purposes of this Agreement. The receiving Party shall safeguard the Confidential Information to the same extent that it safeguards its own confidential and proprietary information and in any event with no less than a reasonable degree of protection.
- 6.3. Each Party agrees that before any of its subcontractors and/or agents may be given access to Confidential Information, each such subcontractor and/or agent shall agree to be bound by a confidentiality undertaking comparable to the terms of this Agreement. Notwithstanding the return of any Confidential Information, each Party and its subcontractors and/or agents will continue to hold in confidence all Confidential Information, which obligation shall survive any termination of this Agreement.
- 6.4. In the event the receiving Party is requested or required to disclose, by court order or regulatory decision, any of the disclosing Party’s Confidential Information, the receiving Party shall provide, to the extent permitted, the disclosing Party with prompt written notice so that the disclosing Party may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. The receiving Party shall furnish only that portion of the Confidential Information which is legally required.
- 6.5. Within ten (10) business days following (i) the termination or expiry of this Agreement or (ii) the disclosing Party’s reasonable earlier request at any time, the receiving Party shall destroy or return to the disclosing Party (at its option) any and all of the disclosing Party’s Confidential Information, and shall purge all copies and traces of the same from any storage location and/or media.
- 6.6. The confidentiality undertaking under this Article 6 shall not be applicable if the Confidential Information:
 - 6.6.1. has become publicly known prior to being divulged or thereafter, but without any breach of confidentiality undertaking; or
 - 6.6.2. had been legitimately obtained from a third party neither tied by an obligation of confidentiality nor professional secrecy; or
 - 6.6.3. was independently created by the receiving Party without the use of any Confidential Information of the disclosing Party; or
 - 6.6.4. was already known or developed by the Receiving Party, as can be demonstrated by documentary evidence.

7. Miscellaneous Provisions

- 7.1. This Agreement contains the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes and replaces all prior agreements or understandings, whether written or oral, with respect to the same subject matter that is still in force between the Parties.
- 7.2. Any amendments to this Agreement, as well as any additions or deletions, must be agreed upon in writing by both the Parties.
- 7.3. Whenever possible, the provisions of this Agreement shall be interpreted in such a manner as to be valid and enforceable under the applicable law. However, if one or more provisions of this Agreement are found to be invalid, illegal, or unenforceable, in whole or in part, the remainder of that provision and of this Agreement shall remain in full force and effect as if such invalid, illegal or unenforceable provision had never been contained herein. Moreover, in such an event, the Parties shall amend the invalid, illegal or unenforceable provision(s) or any part thereof and/or agree on a new provision in such a way as to reflect insofar as possible the purpose of the invalid, illegal or unenforceable provision(s).
- 7.4. Any failure or delay by a party in exercising any right under this Agreement, any single or partial exercise of any right under this Agreement, or any partial reaction or absence of reaction by a party in the event of a violation by the other party of one or more provisions of this Agreement, shall not operate or be interpreted as a waiver (either express or implied, in whole or in part) of that party's rights under this Agreement or under the said provision(s), nor shall it preclude any further exercise of any such rights. Any waiver of a right must be expressed and in writing. If there has been an express written waiver of a right following a specific failure by a party, this waiver cannot be invoked by the other party in favor of a new failure, similar to the prior one, or in favor of any other kind of failure.

8. Applicable Law and Jurisdiction

- 8.1. The laws of Spain shall apply to this Agreement.
- 8.2. The Courts of Las Palmas de Gran Canaria (Spain) shall have exclusive jurisdiction with respect to all disputes arising out of or in connection with this Agreement. Attempts to solve disputes informally shall not prevent the Parties from submitting such disputes to the Courts.

AS WITNESS the hands of the duly authorized representatives of the Parties the day month and year first above written:


SIGNED on behalf of
The Data Controller

DocuSigned by:

032E3A17812D403...
.....
(Signature)

Name: Julia Wester
Title: CEO

SIGNED on behalf of
The Data Processor

DocuSigned by:

B478FB0EB57B4C9...
.....
(Signature)

Name: Carlos Hernández Medina
Title: CEO

Annex 1: Data Processing Activities

1. Description of the data processing carried out on behalf of the Data Controller

In addition to the information provided elsewhere in the Agreement, the Parties wish to document the following information in relation to the data processing activities.

The data processing performed by the Data Processor on behalf of the Data Controller relates to **receipts and tax calculations**. **The data processing activity consists of** storing the data included in receipts.

The categories of personal data involved are:

- Personal identification data: full name, billing address, telephone number, and email.
- Device's IP address
- Financial identification data: bank account number, invoices, and credit notes.

The data subjects are **clients of the Data Controller**.

The duration of the data processing activities is **aligned with the contract duration**.

2. Existing Subprocessors

At the time this Agreement is entered into, the Data Processor has appointed the following Subprocessors:

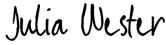
- Amazon Web Services, Inc.
- DigitalOcean, LLC.
- GoCardless, Ltd.
- PayPal (Europe) S.à r.l. et Cie, S.C.A.
- Rollbar, Inc.
- Wildbit, LLC.
- Stripe, Inc.
- Zapier, Inc.

3. Outsourcing to new or replacement of existing Subprocessors

The Data Processor will inform without delay of any intended change in respect of new sub-processors or the replacement of previous sub-processors. The Data Controller will be able to object to such changes.


In the event that the Data Processor uses Subprocessors that are not domiciled in the EU/EEA or whose parent companies are not domiciled in the EU/EEA, the Data Processor will ensure that a data protection agreement pursuant to data protection legislation in effect has been entered into with the subcontractor to ensure an appropriate level of data protection.

SIGNED on behalf of
The Data Controller

DocuSigned by:

032E3A17812D403...
.....
(Signature)

Name: Julia Wester
Title: CEO

SIGNED on behalf of
The Data Processor

DocuSigned by:

B478FB0EB57B4C9...
.....
(Signature)

Name: Carlos Hernández Medina
Title: CEO

Annex 2: Technical and Organizational Security Measures

1. Introduction

We maintain internal policies and procedures or procure that our Subprocessors do so, which are designed to:

- (a) secure any User Personal Data Processed by us against accidental or unlawful loss, access, or disclosure;
- (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the User Personal Data Processed by us;
- (c) minimize security risks, including through risk assessment and regular testing.

We will conduct periodic reviews of the security of our network and the adequacy of our information security program as measured against industry security standards and our policies and procedures, and will use reasonable efforts to procure that our Subprocessors do so as well.

We will periodically evaluate the security of our network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews, and will use reasonable efforts to procure that our Subprocessors do so as well.

2. Access controls

We limit access to personal data by implementing appropriate access controls.

3. Availability and backup of User Personal Data

We regularly back-up User Personal Data. Back-ups are stored separately.

4. Disposal of IT equipment

We have in place processes to securely remove all personal data before disposing of IT systems (for example, by using appropriate technology to purge equipment of data and/or destroying hard disks).

5. Encryption

We use encryption technology where appropriate to protect User Personal Data held electronically.

6. Transmission or transport of User Personal Data

We will implement appropriate controls to secure User Personal Data during transmission or transit.

7. Device hardening

We will remove unused software and services from devices used to process User Personal Data. Default passwords that are provided by hardware and software producers will not be used.

8. Physical security

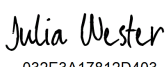
We implement appropriate physical security measures to safeguard User Personal Data.

9. Staff training and awareness

We carry out staff training on data security and privacy issues relevant to their job role and ensure that new starters receive appropriate training before they start their role.

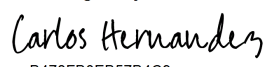
Staff is subject to disciplinary measures for breaches of our policies and procedures relating to data privacy and security.

SIGNED on behalf of
The Data Controller

DocuSigned by:

032E3A17812D403...
.....
(Signature)

Name: Julia Wester
Title: CEO

SIGNED on behalf of
The Data Processor

DocuSigned by:

B478FB0EB57B4C9...
.....
(Signature)

Name: Carlos Hernández Medina
Title: CEO