

## Miro Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into between RealtimeBoard, Inc. dba Miro ("**Miro**" or "**data importer**") and the entity identified as the Customer ("**Customer**" or "**data exporter**") and is appended to either (i) the Miro Cloud Agreement or Terms of Service (as applicable); or (ii) other electronic or written agreement in incorporating this DPA, governing the Customer's access and use of the Miro platform and related services (the "**Agreement**"). The parties agree that this DPA shall be incorporated into and form part of the Agreement and subject to the provisions therein, including limitations of liability.

**This DPA sets forth the terms and conditions under which Miro may receive and process Customer Personal Data from Customer and incorporates the Standard Contractual Clauses. If Customer makes any deletions or revisions to this DPA, those deletions or revisions are hereby rejected and invalid, unless agreed by Miro. Customer's signatory represents and warrants that he or she has the authority to bind the Customer to this DPA. This DPA will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this DPA.**

### Data Processing Terms

#### 1. Definitions

"**Applicable Privacy Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU/UK Data Protection Law.

"**Customer Personal Data**" means any Customer Content that is Personal Data and protected by Applicable Privacy Law(s).

"**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the Swiss Federal Data Protection Act ("**Swiss DPA**"), and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) (iii) or (iv); in each case as may be amended or superseded from time to time;

"**Miro Subsidiary**" means any entity that is directly or indirectly controlled by, controlling or under common control with Miro.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject based to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data

from Switzerland to any other country which is not determined to provide adequate protection for Personal Data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

**"Standard Contractual Clauses"** means: (i) where the EU GDPR or the Swiss DPA applies, the contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (specifically, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses) ("**UK SCCs**"), as applicable in accordance with Section 8 (Data Transfers).

**"Security Incident"** means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Customer Personal Data. A "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

**"Subprocessor"** means any third party (including any Miro Subsidiary) engaged by Miro to process any Customer Personal Data (excluding Miro employees or consultants).

The terms "**Controller**", "**data subject**", "**Personal Data**", "**Processor**," and "**processing**," have the meanings given to them in Applicable Privacy Law(s). If and to the extent that Applicable Privacy Law(s) do not define such terms, then the definitions given in EU/UK Data Protection Law will apply.

## **2. Role and Scope of Processing**

- 2.1 The parties acknowledge that with regard to the processing of Customer Personal Data, Customer shall be the Controller and Miro shall process Customer Personal Data as a Processor on behalf of Customer.
- 2.2 Miro will process Customer Personal Data only in accordance with Customer's documented instructions and will not process Customer Personal Data for its own purposes, except as set out in this DPA or where required by applicable law(s). The Agreement, including this DPA, along with Customer's configuration of any settings or options in the Services (as Customer may be able to modify from time to time), constitute Customer's complete and final instructions to Miro regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses. Additional instructions outside the scope of such Processing instructions (if any) require prior written agreement between the parties.
- 2.3 Each party shall comply with its obligations under Applicable Privacy Law(s) in respect of any Customer Personal Data it Processes under or in connection with the Services or this DPA. Without prejudice to the foregoing, Customer is responsible for determining whether the Services are appropriate for the storage and processing of Customer Personal Data under Applicable Privacy Law(s) and for the accuracy, quality and legality

of the Customer Personal Data and the means by which it acquired Customer Personal Data. Customer further agrees that it has provided notice and obtained all consents, permissions and rights necessary for Miro and its Sub-processors to lawfully process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA).

2.4 Miro shall promptly notify Customer if it makes a determination that Customer's instructions infringe Applicable Privacy Law(s) (but without obligation to actively monitor Customer's compliance with Applicable Privacy Law(s)) and in such event, Miro shall not be obligated to undertake such Processing until such time as the Customer has updated its processing instructions and Miro has determined that the incidence of non-compliance has been resolved.

2.5 Details of Data Processing:

- (a) **Subject matter:** The subject matter of the data processing under this DPA is the Customer Personal Data.
- (b) **Duration:** As between Customer and Miro, the duration of the processing is the term of the Agreement plus any period after the termination or expiry of the Agreement during which Miro will process Customer Personal Data in accordance with the Agreement.
- (c) **Purpose:** Miro will process Customer Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.
- (d) **Nature of the processing:** The provision of the Services as described in the Agreement and initiated by the Customer from time to time.
- (e) **Types of Customer Personal Data.** Customer Personal Data uploaded to the Services under Customer's Miro account.
- (f) **Categories of data subjects:** The data subjects could include Customer's employees, consultants, agents and third parties authorized to use the Services as "Users" under Customer's Miro account and any other data subjects whose personal data is submitted to Miro by Customer through the Services.

### 3. Subprocessing

3.1 Customer grants Miro a general authorization to subcontract the processing of Customer Personal Data to a Subprocessor, including those Subprocessors listed at <https://miro.com/static/legal/Miro-Current-Subprocessors-List.pdf> (or such other successor URL) ("**Subprocessor List**").

3.2 If Miro engages a new or replacement Subprocessor, Miro will:

- (a) update the Subprocessor List;

- (b) impose substantially the same data protection terms on any Subprocessor it engages as contained in this DPA (including data transfer provisions, where applicable); and
  - (c) remain liable to Customer for any breach of this DPA caused by an act, error or omission of such Subprocessor.
- 3.3 If Customer elects to be notified in writing 10 days prior to Miro engaging a new or replacement Subprocessor, Customer must subscribe to such notifications via the [customer notification portal](#);
- 3.4 Customer may object to Miro's appointment of any new or replacement Subprocessor promptly in writing within thirty (30) days after receipt of notice in accordance with (3.2 (a)) and on reasonable grounds related to Subprocessor's ability to comply with Applicable Privacy Law(s). In such case, the parties shall discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution. If the parties cannot reach such resolution, Miro shall have the right, at its sole discretion, to either not appoint the disputed Subprocessor, or permit Customer to suspend or terminate the applicable Order and/or the Agreement. These procedures are Customer's exclusive remedy and Miro's entire liability for resolving Customer's objections to Miro's appointment of Subprocessor's under this DPA.

#### 4. **Cooperation**

- 4.1 Miro shall reasonably cooperate with Customer to enable Customer to respond to any requests, complaints or other communications from data subjects and regulatory or judicial bodies relating to the processing of Customer Personal Data, including requests from data subjects seeking to exercise their rights under Applicable Privacy Law(s). In the event that any such request, complaint or communication is made directly to Miro, Miro shall, once it has identified the request is from or related to a data subject for whom the Customer is responsible, pass this onto Customer and shall not respond to such communication without Customer's express authorization (unless required to do so in order to comply with applicable law(s)).
- 4.2 To the extent Miro is required under Applicable Privacy Law(s), Miro will assist Customer to conduct a data protection impact assessment and, where legally required, consult with applicable data protection authorities in respect of any proposed processing activity that presents a high risk to data subjects.
- 4.3 Taking into account the nature of the processing, Customer agrees that it is unlikely that Miro would become aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Miro becomes aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Miro will reasonably cooperate with Customer to erase or rectify inaccurate or outdated Customer Personal Data transferred under the Standard Contractual Clauses.

#### 5. **Data Access & Security Measures**

- 5.1 Miro will ensure that any personnel tasked with the processing of Customer Personal Data are subject to an appropriate duty of confidentiality (whether a contractual or statutory duty) and that they process Customer Personal Data only for the purpose of delivering the Services.
- 5.2 Miro will implement and maintain reasonable and appropriate technical and organizational security measures with the aim of protecting Customer Personal Data from Security Incidents in accordance with the measures listed in Schedule 2 ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Miro may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish overall security of the Services.

## 6. **Security Incidents**

In the event of a Security Incident, Miro shall inform Customer without undue delay and will provide written details of the Security Incident to Customer, including the type of data affected and the identity of affected person(s), once such information becomes known or available to Miro. Miro shall, to the extent possible, provide timely information and cooperation to Customer to allow Customer to fulfil its data breach reporting obligations under Applicable Privacy Law(s) and shall take reasonable steps to remedy or mitigate the effects of the Security Incident. The obligations herein shall not apply to Security Incidents that are caused by the Customer or its users.

## 7. **Security Reports & Inspections**

- 7.1 Upon request, Miro shall provide copies of any certifications, audit report summaries and/or other relevant documentation it holds, where reasonably required by Customer to verify Miro's compliance with this DPA.
- 7.2 While it is the parties' intention ordinarily to rely on Miro's obligations set forth in Section 7.1 to verify Miro's compliance with this DPA, following a confirmed Security Incident or where a data protection authority requires it, Customer may provide Miro with thirty (30) days' prior written notice requesting that a third-party conduct an audit of Miro's operations and facilities ("**Audit**"); provided that (i) any Audit shall be conducted at Customer's expense; (ii) the parties shall mutually agree upon the scope, timing and duration of the Audit; (iii) the Audit shall not unreasonably impact Miro's regular operations.
- 7.3 Any written responses or Audit described in this Section 7 shall be subject to the confidentiality provisions of the Agreement. The parties agree that the audits described in Clause 8.9 of EU SCCs shall be carried out in accordance with this Section 7 (Security Reports & Instructions).

## 8. **Data Transfers**

- 8.1 Customer Personal Data that Miro processes under the Agreement may be processed in any country in which Miro, its Miro Subsidiaries and Sub-processors maintain facilities to

perform the Services, as further detailed in the Subprocessor List. Miro shall not process or transfer Customer Personal Data (nor permit such data to be processed or transferred) outside of EEA, Switzerland or UK, unless it first takes such measures as are necessary to ensure the transfer is in compliance with this EU/UK Data Protection Law.

- 8.2 The parties agree that, when the transfer of Customer Personal Data from Customer to Miro is a Restricted Transfer, it shall be governed by
- (a) for transfers of Customer Personal Data subject to GDPR or the Swiss DPA, the EU SCCs, which the parties hereby enter into and incorporate into this DPA, or
  - (b) for transfers of Customer Personal Data subject to UK GDPR, the UK SCCs, which the parties hereby enter into and incorporate into this DPA.
- 8.3 For the purposes of the Standard Contractual Clauses, the relevant annexes, appendices or tables shall be deemed populated with the relevant information set out in Annex I. In the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 8.4 If Miro adopts an alternative lawful data export mechanism for the transfer of personal data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with EU/UK Data Protection Law and extends to the territories to which the relevant Customer Personal Data is transferred).

## 9. Deletion & Return

- 9.1 Upon Customer's request, or upon termination or expiry of this DPA, Miro shall destroy or return to Customer all Customer Personal Data in its possession in accordance with Miro's then-current data deletion timelines and policies, which may be requested by Customer at any time. This requirement shall not apply to the extent that Miro is required by any applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data archived on back-up systems, which data Miro shall isolate and protect from any further processing except to the extent required by such law. The parties agree that the certification of deletion of Personal Data described in Clause 8.5 and 16.(d) of EU SCCs shall be provided by Miro to Customer only upon Customer's written request.

## 10. California Consumer Privacy Act (CCPA)

- 10.1 To the extent that Customer has users of the Services who are residents of the state of California in the United States and the CCPA applies, the terms set forth in this Section 10 shall apply to this DPA.
- 10.2 The following amendments shall be made to the definitions set forth in Section 1 of this DPA:

- (a) “CCPA” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq..
  - (b) “Business” has the meaning given to it in the CCPA.
  - (c) “Service Provider” has the meaning given to in the CCPA.
- 10.3 For purposes of Customer Personal Data constituting “personal information” under the CCPA, Customer is a Business and Miro is a Service Provider. Customer’s transfer of Customer Personal Data to Miro is not a sale, and Miro provides no monetary or other valuable consideration to Customer in exchange for Personal Data.
- 10.4 Miro agrees to comply with all applicable requirements of the CCPA, and if and to the extent agreed between Customer and Miro in writing as set forth in this DPA.
- 10.5 As applicable to the Services, Miro shall reasonably assist Customer in responding (at Customer’s expense) to any request from a data subject (including “verifiable consumer requests”, as such term is defined in the CCPA), relating to the processing of Customer Personal Data under the Agreement.

## **11. General**

- 11.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA controls and takes precedence. With effect from the effective date, this DPA is part of, and incorporated into the Agreement.
- 11.2 In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.
- 11.3 Any claim or remedy Customer may have against Miro, its employees, agents and Subprocessors, arising under or in connection with this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence) or under any other theory of liability, shall to the maximum extent permitted by law be subject to the limitations and exclusions of liability in the Agreement. Accordingly, any reference in the Agreement to the liability of a party means the aggregate liability of that party under and in connection with the Agreement and this DPA together.
- 11.4 This DPA may not be modified except by a subsequent written instrument signed by both parties.
- 11.5 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Privacy Law(s) or the Standard Contractual Clauses.
- 11.6 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

## ANNEX I

### A. LIST OF PARTIES

#### MODULE TWO: Transfer controller to processor

##### Data exporter(s):

Name: The entity identified as the "Customer" in this DPA.

Address: The address for the Customer associated with its Miro account or otherwise specified in the DPA or the Agreement.

Contact person's name, position and contact details: The contact details associated with the Customer's account, or otherwise specified in this DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Annex 1(B) below.

Role (controller/processor): Controller

##### Data importer(s):

Name: RealtimeBoard, Inc. dba Miro ("Miro")

Address: 201 Spear Street, Suite 1100, San Francisco, CA 94105

Contact person's name, position and contact details: Darryl Anthony, [privacy@miro.com](mailto:privacy@miro.com) (Data Protection Officer)

Activities relevant to the data transferred under these Clauses: The activities specified in Annex 1(B) below.

Role (controller/processor): Processor

### B. DESCRIPTION OF TRANSFER

#### MODULE TWO: Transfer controller to processor

*Categories of data subjects whose personal data is transferred:*

Customer employees, consultants, agents and authorized third parties to use the Services as "users" under Customer's Miro account and any other data subjects whose personal data is submitted to Miro by Customer through the Services.

*Categories of personal data transferred:*

Name, email address and any other personal data submitted by Customer through the Services, including as Customer Content

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict*



*purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:*

None; not permitted under the Miro prohibited use policy.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):*

Customer Personal Data may be transferred on a continuous or one-off basis depending on the Customer's use of the Services and the Customer's processing instructions.

*Purpose(s) of the data transfer and further processing:*

For Miro to provide, maintain and improve the Services provided to data exporter pursuant to the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:*

Miro will retain Customer Personal Data for up to 180 days after termination or expiry of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

*Duration:*

The term of the Agreement plus any period after the termination or expiry of the Agreement during which Miro will process Customer Personal Data in accordance with the Agreement.

*Subject matter:*

The subject matter of the data processing under this DPA is the Customer Personal Data.

*Nature of the processing:*

The provision of the Services as described in the Agreement and initiated by the Customer from time to time.

## **C. COMPETENT SUPERVISORY AUTHORITY**

### **MODULE TWO: Transfer controller to processor**

*Identify the competent supervisory authority/ies in accordance with Clause 13:*

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

## ANNEX II

### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

#### MODULE TWO: Transfer controller to processor

Miro uses the following technical and organizational measures to protect personal information:

- Measures of pseudonymisation and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

The technical and organisational measures that the data importer will impose on sub-processors are described in the DPA

### ANNEX III

#### Standard Contractual Clauses

- (a) Subject to Section 8.2 of this DPA, where the transfer of Customer Personal Data to Miro is a Restricted Transfer and GDPR or the Swiss DPA require that appropriate safeguards are put in place, the transfer shall be governed by the EU SCCs as follows:
- (i) Module Two (Transfer Controller to Processor) will apply;
  - (ii) in Clause 7 (Docking Clause), the optional docking clause will apply;
  - (iii) in Clause 9 (Use of Subprocessors), Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 3.2 of this DPA;
  - (iv) in Clause 11 (Redress), the optional language to permit data subjects to lodge complaints with an independent dispute resolution body will not apply;
  - (v) in Clause 17 (Governing Law), Option 1 will apply, and the EU SCCs will be governed by Dutch law;
  - (vi) in Clause 18(b) (Choice of forum and jurisdiction), disputes shall be resolved before the courts of Amsterdam, the Netherlands; and
- (b) where the transfer of Customer Personal Data to Miro is a Restricted Transfer and UK GDPR requires that appropriate safeguards are put in place, the UK SCCs will apply in accordance with paragraph (a) above.