Data Processing Agreement

Between

Customer

– hereinafter referred to as "**Controller**" –

and

Perdoo GmbH

Berlin Betahaus, Rudi-Dutschke-Straße 23, 10969 Berlin

– hereinafter referred to as "**Processor**" –

– each individually a "**Party**", jointly the "**Parties**" –

Preamble

(A) This Data Processing Agreement (including its appendices, the "Addendum") is incorporated into the "***Main Contract***" – as defined in the following – between Perdoo and Customer:

(B) "***Main Contract***" means the contract under which Perdoo has agreed to provide the applicable Services to its Customer. With entering into the main contract Controller has commissioned Processor to perform certain IT and network services.

(C) Since the use of the services provided by the Processor is aimed at determining company-specific key figures (hereinafter "Objective Key Results" or "OKRs") on the basis of the respective company data (of the Controller) and these generally also include personal data (provided by Controller), it cannot be ruled out that Processor will, during the fulfillment of its contractual obligations, gain access to or obtain knowledge of personal data.

(D) In the event of any conflict or inconsistency between the DPA Terms and any other terms in Perdoo's main Contract or other applicable agreements in connection with Perdoo's Services, the DPA Terms, pursuant to Art. 28 (3) p. 1 GDPR, shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Perdoo's Privacy Policy that otherwise may apply to processing of Customer Data, or Personal Data, as defined herein.

Therefore, the Parties agree as follows:

1. Scope of this Agreement

1.1. This Data Processing Agreement (hereinafter the "**Agreement**") shall apply to the processing of personal data related to the Main Contract by Processor or by third parties commissioned by Processor.

1.2. Under this Agreement Processor shall provide the following data processing services to and on behalf of Controller (hereinafter the "**Data Processing**"):

Software-as-a-Service provided by Processor to Controller that enables Controller to set, track and manage its company goals (OKRs). Further details can be found in the Main Contract.

1.3. It cannot be ruled out that Processor will, during the Data Processing, gain access to or obtain knowledge of or process the following personal data:

Type of Personal Data	Categories of Data Subjects
- Personal Master Data (Key Personal Data). - Contact Data: Email, First/Last Name, Job Position, Avatar. - Login information of users. - User IDs / cookie IDs / advertising IDs. - Browser type / version. - Device data. - System data. - Behavioral data (clicked elements, visit period, etc.). - Text entries. - Photographs. - Log data.	- Software / service user. - Customers.

Further details can be found in the Main Contract.

2. General Rights and Obligations of the Parties

2.1. As the person responsible pursuant to Art. 4 No. 7 GDPR, the Controller is responsible for compliance with data protection regulations, in particular the selection of the Processor, the Data transmitted to him and the instructions issued (Art. 28 (3) a, 29 and 32 (4) GDPR).

2.2. Processor may process personal data only within the scope of this Agreement and in accordance with the instructions of Controller, unless required otherwise by the laws of the European Union or its Member States to which the Processor is subject. in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28 (3) p. 2 a GDPR).In particular, Processor shall only correct, delete or limit the processing of personal data according to the instructions of Controller. In the event that an affected data subject addresses Processor directly in such regard, Processor shall, where reasonably possible, immediately forward such request to Controller.

2.3. Controller shall issue verbal instructions to Processor only in urgent cases and immediately thereafter confirm such instructions at least in text form.

2.4. Processor shall process personal data only within the territory of a member state of the European Union or of a signatory state of the Agreement on the European Economic Area. Any transfer and processing of personal data to third countries shall require the prior written consent of Controller and shall only take place if the conditions of Art. 44 et. seq. General Data Protection Regulation of the European Union (GDPR) are met.

2.5. Processor shall ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality.

2.6. If required by law, Processor shall appoint a data protection officer in writing. Processor shall notify Controller of the contact details of such data protection officer to allow Controller to directly contact such data protection officer.

2.7. Processor shall within its capabilities assist Controller in fulfilling Controller's obligations under Art. 12 through 22 GDPR and Art. 32 to 36 GDPR.

2.8. Processor shall only delegate the Data Processing to such employees who are bound by confidentiality obligations or who are subject to an appropriate statutory duty of confidentiality. Persons subordinated to Processor, having access to personal data of Controller, shall process such data exclusively in accordance with the instructions of Controller, unless such persons are legally obliged to process such data.

2.9. Upon completion of the Data Processing and upon termination of the Main Contract in its entirety at the latest, Processor shall, at the choice of the Controller, and as far as Processor is not bound by statutory retention duties, either return all personal data as well as all documents, data and copies obtained in connection with this Agreement to Controller, or upon the prior written consent of Controller, delete or destroy such personal data, documents, data and copies.

3. Information Obligations

3.1. In the event Processor becomes aware that an instruction of Controller violates any data protection laws, Processor shall immediately notify Controller thereof. However, mere acceptance of an instruction does not confirm or imply that such instruction complies with Data Protection Regulations. Processor shall be entitled to suspend the execution of such instruction until such instruction is confirmed or altered in writing by Controller.

3.2. Processor shall immediately notify Controller of control actions and measures of investigating and supervisory authorities, to the extent such measures are related to the Data Processing under this Agreement.

3.3. In the event Processor becomes aware of any violation of the protection of personal data in relation to this Agreement, Processor shall notify Controller without undue delay.

4. Technical and Organizational Measures

4.1. Processor shall implement technical and organizational measures for the protection of personal data appropriate to comply with the requirements of the GDPR, in particular measures ensuring confidentiality, integrity, availability and resilience of the systems and

services used for Data Processing (each of these technical and organizational measures hereinafter individually "**TOM**", jointly "**TOMs**").

4.2. The particular TOMs implemented by Processor are further described in **Annex 1**.

4.3. Processor shall be entitled to replace any of the implemented TOMs at any time with alternative measures that provide a comparable level of protection.

4.4. Processor shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Article 32 (1) p. d GDPR; Article 25 (1) GDPR).

5. Processing in Third Countries

5.1. The processing of Data as contractually specified is usually carried out only in a Member State of the European Union or in another state party to the Agreement on the European Economic Area (EEA).

5.2. The processing of Data in a third country, also by subprocessors, may only be carried out on documented instructions from the Controller and if the particular requirements of Art. 44 ff. GDPR are met, unless the Processor is obliged to carry out processing in the third country by the law of the Union or the Member States to which the Processor is subject, in which case the Processor shall notify the Controller of these legal requirements before processing, unless the law prohibits such an information on important grounds of public interest (Article 28 (3) S. 2 a. GDPR).

5.3. The authorisation of the Controller for processing in the third country shall be considered to have been given in respect of the processes listed under Clause 6.2 of this Agreement.

6. Subcontractors

6.1. Processor shall be entitled to subcontract certain parts of the Data Processing to third parties ("**Subcontractors**") only with Controller's prior written consent. Controller shall not withhold its consent unless on important grounds of data protection law.

6.2. The authorisation of the Controller to the commissioning of Subcontractors by Processor (also for processing in third countries shall be considered to have been given in respect of the Subcontractors listed in the following:

Subcontractor	Address	Subcontractor's Services
Amazon Web Services (AWS)	Frankfurt. Germany	Cloud Infrastructure Services
Chargebee	21155 Smith Switch Road, Ashburn, VA, USA. **Signed SCC's in place*	Billing Solutions (financial services, only billing contact data)
FirstPromoter	Str. Talmacelului 30 555700, Sibiu, Romania	Partner Program Software
Intercom (Intercom R&D Unlimited Company)	Amazon Web Services (AWS) facilities (us-east-1), USA **Signed SCC's in place.*	In-app Messaging Services

LearnWorlds	Google Cloud Platform - Central EU(Netherlands, Belgium, Germany)	LMS System
Postmark	2400 Market Street, No. 200, Suite 235B, Philadelphia, PA 19103 **Signed SCC's in place.*	Email Infrastructure Service (Transactional / system mails)
Render.com	Frankfurt, Germany	Cloud Infrastructure Services
Salesforce	Frankfurt, Germany	Customer Relationship Management
Zapier, Inc.	548 Market Street, #62411 San Francisco, CA 94104 United States	Automation services

6.3. Processor shall impose its data protection obligations under this Agreement on any Subcontractor.

6.4. Clauses 6.1 and 6.2 shall apply *mutatis mutandis* to the replacement of any Subcontractor by Processor and to the further subcontracting of the Data Processing to another third party by Subcontractor.

7. Audits and inspections

7.1. The Controller has the right to audit the Processor's compliance with the legal requirements and the regulations of this Agreement, in particular the technical and organisational measures, at any time to the required extent (Art. 28 (3) h. GDPR).

7.2. On-site inspections are carried out within normal business hours, must be announced by the Controller within a reasonable period (at least 14 days, except in emergencies) and have to be supported by the Processor (e.g. by the provision of the necessary personnel).

7.3. The inspections are limited to the necessary scope and must take into account the Processor's trade and business secrets as well as the protection of personal data of third parties (e.g. other Controllers or employees of the Processor). Only qualified inspectors are permitted to carry out the inspection, who also can identify themselves and who are bound to confidentiality with regard to the business and trade secrets and processes of the Processor and personal data or other confidential information of third parties.

7.4. Instead of audits and on-site inspections, the Processor may refer the Controller to an equivalent inspection or audit by independent third parties (e.g. neutral data protection auditors), compliance with approved rules of conduct (Art. 40 GDPR) or suitable data protection or IT security certifications in accordance with Art. 42 GDPR. This applies in particular if business and trade secrets of the Processor or personal data or other confidential information of third parties would be at risk due to the audits or inspections.

7.5. If the acceptance and cooperation in the inspections or adequate alternative measures of the Controller exceeds the contractual obligations of the Processor in accordance with the Principal Agreement and are not based on misconduct on the part of the Processor, the

Controller shall reimburse the Processor separately for the additional time and effort arising therefrom.

8. Term and Termination

This Agreement shall become effective when Customer enters into Perdoo's Main Contract.. The provisions of the Main Contract regarding term and termination shall apply *mutatis mutandis* to this Agreement. This Agreement shall automatically end if the Main Contract ends in its entirety, unless agreed otherwise in writing.

9. Liability

9.1. In the internal relationship, the Controller and the Processor shall be liable for compensation for damages suffered by the affected party due to inadmissible or incorrect data processing or use within the scope of order processing in accordance with the data protection laws in accordance with their respective share of cause and fault.

9.2. The contracting parties release themselves from liability if one of the contracting parties proves that it is not responsible for the circumstance through which the damage occurred to an affected party.

10. Miscellaneous

10.1. This Agreement constitutes the entire agreement between the Parties in respect to its subject matter and supersedes and extinguishes all prior negotiations, arrangements, understandings, course of dealings or agreements made between the Parties in relation to its subject matter, whether written, oral or implied.

10.2. Valid amendments or supplements to this Agreement must be made in writing in the sense of sec. 126 German Civil Code (whereas sec. 127 (2) German Civil Code is hereby excluded). The same shall apply to any agreement to deviate from or cancel this requirement of written form.

10.3. This DPA shall only oblige the Processor in so far as this is necessary to fulfil the statutory obligations, in particular in accordance with Art. 28 ff. GDPR and does not impose any further duties on the Processor.

10.4. This Agreement shall be governed by and construed in accordance with the laws of the Federal Republic of Germany excluding its conflict of laws provisions.

10.5. The exclusive place of jurisdiction for any disputes resulting from or in connection with this Agreement is Berlin, Germany.

10.6. Should any provision of this Agreement be or become ineffective or invalid in whole or in part, the effectiveness and validity of the other provisions of this Agreement shall not be affected. Such ineffective or invalid provision shall be replaced by a provision which comes as close as legally possible to what the Parties would have agreed, pursuant to the meaning and purpose of the original provision and of this Agreement if they had recognised the ineffectiveness or invalidity of the original provision. If the ineffectiveness or invalidity of a provision is based on the determination of a certain level of performance or a certain time (deadline or fixed date), such ineffective or invalid level or time shall be replaced by the

level or time which comes as close as legally possible to the original level or time. The foregoing shall also apply to any possible omission in this Agreement that was not intended by the Parties. It is the express intention of the Parties that this savings clause does not just have the effect of shifting the burden of proof but that sec. 139 German Civil Code is entirely dispensed with.

Annex 1 Description of TOMs

Annex 1

Description of Technical and Organizational Measures (TOMs)

TOMs implemented by Processor:

1. Confidentiality Measures

1.1. Physical Access Control

Physical measures to prevent unauthorized persons from accessing data processing systems.

> We deploy security locking systems with keys and only use transponders for our main doors. Our transponder system allows us to instantly disable a transponder if lost and shows us a log of who and when someone entered our facilities. In addition we carefully select our cleaning and maintenance personnel.

1.2. Systems Access Control

Measures to prevent the use of data processing systems by unauthorized persons.

> We have two-factor authentication (2FA) and strong password policies for all services that our employees use. Every laptop that we hand out to employees enforces password protection, an encrypted hard drive and automatic screen lock. In addition, we use a services that let us remotely lock an entire machine, should it be abducted or lost somehow.

1.3. Data Access Control

Measures to ensure that persons authorized to use data processing systems have access to only such data that is covered by their authorization and that personal data cannot be read, copied, altered or removed during processing, use or after storage.

> All data is encrypted both at rest and in transit (see Security Policy at https://www.perdoo.com/security/). Our CTO is the only employee with direct data processing systems access and he uses a VPN at all times (connection is blocked for him while the VPN loads or is unavailable).

1.4. Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

Our production and sandbox environment, as well as the different web/mobile clients we use or offer are completely isolated instances.

2. Integrity Measures

2.1. Disclosure Control

Measures to ensure that personal data cannot be read, copied, altered or removed during electronic transmission, transport or storage on data carriers, and to ensure that it is possible to verify and establish the points envisaged for the transfer of personal data by data transmission systems.

Our services are served entirely over HTTPS. All data sent to or from us is encrypted in transit using 256 bit encryption, utilizing AES_128_GCM and ECDHE_RSA as key exchange mechanism. Our API and application endpoints are TLS/SSL only and score an “A” rating on SSL Labs’ tests. In addition, all connections from our application servers to our databases are TLS encrypted. All databases used by us are also encrypted at rest, meaning that we also encrypt the database files on the hard disks themselves. Data encryption is deployed using industry standard encryption and best practices for the frameworks we use.

2.2. Input Control

Measures to ensure retrospective verification and assessment whether and by whom personal data has been entered, changed or removed within the relevant data processing systems.

Any data that is altered using our internal administration panel is logged in an own database. All of our Subcontractors also offer access logs, that allow us to see if and how and entries have been changed.

3. Availability and Resilience Measures

Measures to ensure that personal data are protected against accidental or wilful destruction or loss and can be recovered quickly after an incident.

We run daily database backups that are also stored on AWS. Additionally, we also create backups of each application build that we deploy, for both our servers and our clients. This enables us to rapidly rollback a database, server or client application, should an incidence occur. AWS deploys uninterruptible power supplies (see here: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf).

4. Testing, Assessment and Evaluation Processes

4.1. Data Protection Management

Measures to plan and organize data protection requirements.

We run a security briefing as part of our onboarding process for every new employee that joins Perdoo. Our internal HR tool enforces the completion of this step, so we can be sure it will not be skipped. We review our data protection processes and TOMs twice a year, together with our Data Protection Officer. In addition, our product and engineering teams are in close contact with our Data Protection Officer and consult him/her whenever changes are made to Perdoo that could have an impact on our data processing.

4.2. Incident-Response-Management

Measures to respond to detected or suspected security incidents within the area of data processing systems used.

If we become aware of a data incident, we will immediately notify our CTO (if he is not involved yet) or contact our Engineering lead over the phone. We have backup lines available but our technical executives ensure access to internet and availability over the phone whenever possible. We will ensure that reasonable measures are taken to mitigate the harmful effects of the incident and to prevent further unauthorized access or disclosure. Following that, we will promptly notify affected Controllers and describe, to the extent possible, the details of the incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for the Controller to minimize the impact of the incident.

4.3. Order Control

Measures that ensure that personal data processed on behalf of Controller can only be processed in accordance with the instructions of Controller.

We have appointed a Data Protection Officer to ensure the ongoing enforcement of this Agreement. All our employees are contractually obliged to treat any data they handle as confidential. We have a strict process for changing our sub-contractors, to ensure that they only access and use data to the extent required to perform the obligations sub-contracted to them, and do so in accordance with our agreements and this Agreement.