Data Processing Agreement

Between

_____

_____

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

and

Perdoo GmbH

Invalidenstraße 112, D-10115 Berlin

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

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

Preamble

(A) By way of Perdoo Order form dated _____ Controller has commissioned Processor to perform certain IT and network services. It cannot be ruled out that Processor will, during the fulfilment of its contractual obligations under the aforementioned contract and under further contracts entered between the Parties in connection therewith (collectively, hereinafter the "**Main Contract**"), gain access to or obtain personal data provided by Controller to Processor within the contractual relationship of the Parties.

(B) In order to comply with applicable data protection laws and for the purposes of the protection of personal data, Controller and Processor intend to enter into a data processing agreement.

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 "**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 Agreement.

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

Category of Data	Data Subjects
Personal Master Data (Key Personal Data), Contact Data	Employees of Controller

Further details can be found in the Main Agreement.

2. General Rights and Obligations of the Parties

2.1. The Data Processing shall be conducted by Processor on behalf of Controller. Controller shall be responsible for compliance with applicable data protection laws.

2.2. Processor may process personal data only within the scope of this Agreement and in accordance with the instructions of Controller. 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 be given if the conditions of Art. 44 et. seq. General Data Protection Regulation of the European Union (GDPR) are met.

2.5. Processor shall regularly audit its internal processes and data protection security mechanisms for compliance with applicable data protection laws.

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. The costs thereof shall be borne by Controller.

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 complete termination of the Main Contract at the latest, Processor shall, at the choice of the Controller, and as far as Processor is not bound by statutory retention duties, either (a) return all personal data as well as all documents, data and copies obtained in connection with this Agreement to

Controller, or (b) 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. 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 competent governmental, regulating or supervisory authorities, to the extent such measures are related to the Data Processing.

3.3. In the event Processor becomes aware of any violation of the protection of personal data in relation to this Agreement, Processor shall immediately notify Controller thereof.

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 organisational 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.

5. Subcontractors

5.1. 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 unreasonably withhold its consent.

5.2. Controller hereby consents to the commissioning of Subcontractors by Processor as follows:

Subcontractor	Address	Subcontractor's Services
Amazon Web Services	410 Terry Avenue North, Seattle WA 98109, USA	Cloud Infrastructure Services
Auth0	10900 NE 8th Street, Suite 700, Bellevue, WA 98004, USA	Enterprise Single Sign-on Solutions
Chargebee	SP Info City, #40 M.G.R Salai, Chennai, TN, 600096, India	Billing Solutions
Intercom	55 2nd Street, San Francisco, CA 94105, USA	In-app Messaging Services
Heroku	The Landmark @ 1 Market St., Suite 300, San Francisco, CA 94105, USA	Cloud Infrastructure Services

TalentIms	315 Montgomery Street, 9th Floor, San Francisco, CA 94104, USA	Online Learning Management System

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

5.4. Clauses 5.1 and 5.2 shall apply *mutatis mutandis* to the replacement of any Subcontractor by Processor and to the further subcontracting of the Data Processing (in whole or in part) to another third party by Subcontractor.

6. Proof of Compliance

6.1. Processor shall allow Controller or an external auditor commissioned by Controller to verify Processor's compliance with this Agreement (including the implementation of the TOMs pursuant to Clause 4).

6.2. Processor may demonstrate compliance with this Agreement by providing (a) appropriate test reports, certificates, and data protection certificates issued by independent institutions, (b) self-audits, and (c) reports of compliance with approved codes of conduct.

6.3. If necessary for the purposes laid down in Clause 6.1 and, cumulatively, if compliance with this Agreement cannot be demonstrated by Processor in accordance with Clause 6.2, Processor shall enable Controller to carry out, once per calendar year during normal business hours and without disrupting Processor's business, inspections at Processor's business premises. Such inspections shall be announced by Controller at least 14 business days in advance and shall only be performed by independent external auditors. Such auditors shall not be entitled to gain access to company secrets, business secrets or confidential information of Processor or to any data which is not subject to this Agreement. Processor may object to the appointment of an external auditor for good cause, including, where an auditor is a competitor of Processor. Controller shall bear the costs of any inspections and supporting actions of Processor hereunder (if any).

7. Term and Termination

This Agreement shall become effective upon signature by both Parties. 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, unless agreed otherwise in writing.

8. Liability

The provisions of the Main Contract regarding liability of the Parties shall apply *mutatis mutandis* to this Agreement. Where an action or omission of a Party gives rise to a liability under both the Main Contract and this Agreement, any cap to such Party's total liability as agreed in the Main Contract shall only apply onetime.

9. Miscellaneous

9.1. 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.

9.2. 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.

9.3. Until 25 May 2018, all references to the GDPR contained in this Agreement shall be considered references to the corresponding provisions of the German Federal Data Protection Act (BDSG).

9.4. 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.

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

9.6. 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

Place	Date	Place	Date
		Berlin	
_____		_____	
Controller		Perdoo GmbH	
…….. (Name)		…….. (Name)	
…….. (Position)		…….. (Position)	

Annex 1

Description of Technical and Organisational 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.