Data Processing Agreement pursuant to Art. 28 GDPR

Agreement between the
Controller – hereinafter referred to as the “Customer”, who agrees to this Agreement
and the
Processor – TimeTrack GmbH, Paulanergasse 13/8, 1040 Vienna, Austria
– hereinafter referred to as the “Provider”.

§ 1. Subject matter and duration of the Agreement

(1) This agreement (hereinafter the “Agreement”) governs the processing of personal data (hereinafter the “Data”) by the Provider on behalf of the Customer (hereinafter “Processing on behalf” / “processing as processor”).

(2) Terms used in the Agreement (e.g. data subject, third party, third country, etc.) shall be interpreted within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “GDPR”), unless the terms used in the Agreement are expressly defined.

(3) The subject matter of the respective processing carried out by the Provider is governed in Annex I to the Agreement. The annexes to the Agreement are an integral part of the Agreement. In the event of contradiction or incompatibility, provisions in the annexes shall take precedence over the provisions in the main part of the Agreement. The Agreement does not govern the economic and legal conditions, nor a precise technical or professional description of the services to be provided by the Provider. The duration of this Agreement corresponds to the duration of the contractual relationship between the Customer and the Provider.

(4) The annexes to the Agreement describe the purpose and type of processing on behalf, the categories of data subjects processed by the Processor and the types of data processed, as well as the technical and organisational measures agreed for the processing on behalf.

§ 2. Specification of the content of the Agreement

The performance of the contractually agreed data processing shall in principle take place in a Member State of the European Union or in another contracting state to the Agreement on the European Economic Area. Processing of personal data in a third country or access to personal data from a third country may only take place insofar as the Customer has granted its consent thereto in advance, either generally or in the individual case, and the special requirements of Art. 44 et seq. GDPR are fulfilled. In this case, the Provider shall ensure that an adequate level of data protection is guaranteed for the respective processing, in particular through an adequacy decision of the European Commission pursuant to Art. 45 GDPR or through appropriate safeguards pursuant to Art. 46 GDPR.

§ 3. Technical and organisational measures

(1) The Provider shall implement the technical and organisational measures described in Annex 2. These measures shall be deemed agreed and form the basis of the processing on behalf. The Provider is entitled to adapt the technical and organisational measures to technical and organisational developments, provided that the agreed level of protection is not undercut. The Provider shall explain material changes to the Customer upon request.

(2) The Provider shall establish security pursuant to Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are measures of data security and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the costs of implementation and the nature, scope and purposes of processing, as well as the differing likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR, shall be taken into account [for details see Annex 2].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Provider is permitted to implement alternative adequate measures. In doing so, the security level of the defined measures may not be undercut. Material changes must be documented.

§ 4. Rectification, restriction and deletion of data

(1) The Provider may not rectify, delete or restrict the processing of the data processed on behalf on its own authority, but only on the documented instruction of the Customer. If a data subject contacts the Provider directly in this regard, the Provider shall forward this request to the Customer without undue delay.

(2) Insofar as covered by the scope of services, deletion concept, right to be forgotten, rectification, data portability and access shall be ensured directly by the Provider on the documented instruction of the Customer.

(3) If the Customer is obliged under applicable data protection laws vis-à-vis an individual person to provide information or disclosures regarding the processing of that person’s data or to guarantee the rights of data subjects under Chapter III (Arts. 12 to 23) GDPR, the Provider shall, taking into account the nature of the processing, support the Customer in fulfilling these obligations with suitable technical and organisational measures in accordance with Art. 28 para. 3 lit. e GDPR where possible.

§ 5. Obligations of the Customer

(1) The Customer is the controller within the meaning of the GDPR for the personal data processed under this Agreement.

(2) The Customer is responsible for the lawfulness of the processing, the issuing of instructions and the safeguarding of the rights of the data subjects.

(3) The Customer is responsible for ensuring that the processing of personal data is based on a valid legal basis and that statutory information obligations are fulfilled.

(4) As a matter of principle, the Provider does not examine the data transmitted by the Customer for their substantive lawfulness, accuracy or completeness.

§ 6. Quality assurance and other obligations of the Provider

In addition to compliance with the provisions of this assignment, the Provider has statutory obligations pursuant to Art. 28 to 33 GDPR; in this respect, it guarantees in particular compliance with the following requirements:

- The safeguarding of confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In carrying out the work, the Provider shall only use employees who are bound to confidentiality and who have previously been made familiar with the data protection provisions relevant to them. The Provider and any person subordinate to the Provider who has access to personal data may process such data exclusively in accordance with the instruction of the Customer, including the powers granted in this contract, unless they are legally obliged to process the data.
- The implementation and compliance with all technical and organisational measures required for this assignment pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [for details see Annex 2].
- The Customer and the Provider shall cooperate with the supervisory authority upon request in the performance of their tasks.
- The immediate information of the Customer about control actions and measures of the supervisory authority, insofar as they relate to this assignment. This shall also apply insofar as a competent authority investigates the Provider in connection with the processing of personal data in processing on behalf within the framework of administrative offence or criminal proceedings.
- Insofar as the Customer is itself exposed to a control by the supervisory authority, administrative offence or criminal proceedings, a liability claim by a data subject or third party, or another claim in connection with processing on behalf at the Provider, the Provider shall support the Customer to the best of its ability.
- The Provider regularly checks the internal processes as well as the technical and organisational measures in order to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the protection of the rights of the data subject is ensured.
- Demonstrability of the technical and organisational measures taken vis-à-vis the Customer within the scope of its control powers under Section 8 of this contract.

§ 7. Sub-processing relationships

(1) Sub-processing relationships within the meaning of this provision shall be understood as such services that relate directly to the performance of the main service. This shall not include ancillary services which the Provider uses, for

example, as telecommunications services, postal/transport services, maintenance and user service, or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Provider is obliged, in order to ensure data protection and data security of the Customer's data also in the case of outsourced ancillary services, to take appropriate and legally compliant contractual arrangements as well as control measures.

To the extent that data processing by a subcontractor under this agreement is permissibly carried out outside a Member State of the European Union or outside another contracting state of the Agreement on the European Economic Area, the Provider shall ensure that such data is encrypted in accordance with current standards to such a high level that it cannot be read by persons other than the Provider using reasonable technical means.

(2) The Customer grants the Provider the general authorisation to use the sub-processors named in this Agreement and its annexes. The Customer agrees to the engagement of the following subcontractors subject to a contractual agreement in accordance with Art. 28 para. 2-4 GDPR:

Name and address of the sub-processor	Place of data processing	Service
DigitalOcean, LLC, 101 6th Ave / 101 Avenue of the Americas, New York, NY 10013, USA	Data centre location: Hanauer Landstraße 302, 60314 Frankfurt am Main, Germany	Hosting infrastructure for the operation of the application on an ISO/IEC 27001-certified Virtual Private Server (VPS)[1]. Data transmission is encrypted. Stored data is stored in encrypted form[2].
Stripe Payments Europe, Limited, One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland	Dublin, Ireland	Payment service provider for credit card payments
Amazon Web Services EMEA S.à r.l., 38 Avenue John F. Kennedy, L-1855 Luxembourg	Luxembourg, Luxembourg	Sending transactional emails
Droptop GmbH / Linevast, Am Grashorn 8, 14548 Schwielowsee OT Geltow, Germany	Schwielowsee, Germany	Hosting and provision of email services

[1] The server is administered exclusively by TimeTrack GmbH. Within the framework of hosted virtualisation, our data is isolated from that of other companies both during transmission and in the cloud operator's network.

[2] Data storage on the DigitalOcean servers takes place using AES encryption. Only TimeTrack GmbH has access to the 512-bit key. Decryption of the stored data is only possible by TimeTrack GmbH.

The Provider shall inform the Customer in text form of any intended change regarding the involvement or replacement of sub-processors in good time, at least 14 days before their use. The Customer may object to such a change within 10 days from receipt of the information for important data protection reasons in text form.

(3) The Provider shall conclude an agreement with each sub-processor which imposes on it at least those data protection obligations that are required under Art. 28 GDPR and that apply to the processing activities taken over by the sub-processor. The Provider shall remain responsible vis-à-vis the Customer for the fulfilment of the sub-processor’s data protection obligations.

(4) Insofar as a sub-processor or another service provider used by the Provider processes personal data outside the EU or the EEA or accesses such data from a third country, the Provider shall ensure that the requirements of Art. 44 et seq. GDPR are complied with.

(5) Any further engagement of sub-processors by a sub-processor requires the prior general or separate consent of the Customer.

§ 8. Control rights of the principal

(1) The Customer has the right, after reasonable prior notice, to carry out inspections itself or to have them carried out by a reviewer to be named in the individual case and bound to confidentiality. In doing so, the legitimate operational and business secret interests of the Provider shall be taken into appropriate account.

(2) The Provider shall ensure that the Customer can satisfy itself that the Provider complies with its obligations under Art. 28 GDPR. The Provider undertakes to provide the Customer, upon request, with the necessary information and, in particular, to prove the implementation of the technical and organisational measures.

(3) Insofar as controls by the Customer go beyond the provision of customary evidence, information and documents or cause on-site inspections, the Provider may charge an appropriate expense announced in advance.

§ 9. Notification in the event of breaches by the Provider

(1) The Provider shall support the Customer in complying with the obligations referred to in Articles 32 to 36 GDPR regarding the security of personal data, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, inter alia:

- ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights through security gaps and enable the immediate identification of relevant breach events;

- the obligation to report personal data breaches to the Customer without undue delay;
- the obligation to support the Customer within the framework of its duty to inform the data subject and in this connection to make all relevant information available to it without undue delay;
- support for the Customer in its data protection impact assessment;
- support for the Customer within the framework of prior consultations with the supervisory authority.

(2) For support services that are not included in the service description or are not attributable to misconduct by the Provider, the Provider may claim remuneration.

§ 10. Authority of the Customer to issue instructions

(1) The Customer shall communicate all instructions in text form.

(2) The Provider shall inform the Customer immediately if they consider that an instruction violates Data Protection Regulations. The Provider shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.

§ 11. Copying, deletion and return of personal data

(1) Copies or duplicates of the data shall not be created without the knowledge of the Customer. Excluded from this are backup copies insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

(2) After termination of the provision of services, the Provider shall, on instruction of the Customer, either delete the personal data or surrender it in a common machine-readable format, unless a statutory retention obligation prevents this. Data that must be retained by law shall be deleted after expiry of the retention obligations.

(3) Documentation serving as proof of data processing in accordance with the assignment and in an orderly manner shall be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods. For its discharge, it may hand them over to the Principal at the end of the contract.

§ 12. Validity of this Agreement

This Agreement is an integral part of the contractual relationship existing between the parties and enters into force upon conclusion of the main contract or upon separate acceptance by the Customer.

Annex 1 – Data processing

1. Subject matter, purpose and type of processing on behalf

The subject matter of the processing on behalf is the provision, operation and technical support of the TimeTrack software. The purpose of the processing is the carrying out of time recording and time planning for employees of the controller. The type of processing includes in particular the collection, storage, organisation, provision and other processing of personal data on the systems operated by the processor.

2. Categories of data subjects

Employees, subcontractors, representatives, customers and other data subjects on the Customer’s side who are to have access to TimeTrack systems and use them are collectively referred to as “Users”.

3. The types of personal data:

Category	Data
Name	First name*, Last name*
User identification	Username*, terminal-related identification data, access-related identification data
Electronic identification data	IP address*
Personal details	Gender, date of birth, place of birth, birth name
Contact Information	Email address*, telephone number, contact address and country
Localisation Data	Location data (GPS data)
Social insurance	Social insurance number
Employment information	Role, entry date, exit date, personnel number, working time records, reason for absence
Organisational data	Department affiliation, department function, projects, project hours, project expenses
Other personal data entered by the Customer	This includes other personal data that the Customer records in user-defined fields

Data marked with “*” are mandatory. All other data are optional and depend on the respectively selected or activated software functions.

Annex 2 – Technical and Organisational Measures

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

Physical access control

- No unauthorised access to the office premises;
- Access is granted exclusively to actively employed employees;
- Office visitors are always accompanied by employees.
- Video surveillance of the entrance area.

Access control

- No unauthorised system use; access is restricted by authentication mechanisms;
- Password policies;
- Locking mechanisms for workplaces ("clean desk policy" as well as automatic locking after a period of inactivity);
- Private/public keys for all server accesses.

Authorisation control

- No unauthorised reading, copying, modification or deletion of data. All activities are recorded and reviewed;
- Authorisation concepts: employees receive restricted access according to their job description;
- Logging of accesses and activities (login, logout, changes, deletions).

Separation control

- Separation of customer accounts in the databases;
- Separation of customer data within an account in databases;
- Separate environments for development, staging and production.

Pseudonymisation

- Pseudonymisation of user data where possible

2. Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

- Data transmissions and accesses are logged insofar as this is technically provided for and permissible under data protection law;
- Firewall for the protection of data traffic and end devices in the network.

Input control

- Records of whether, by whom and at what time personal data were entered into or changed in the data processing system;
- Access logs of access attempts;
- Account logs, e.g. request logs
- User rights and roles in the Provider's software in order to prevent unauthorised manipulation.

Encryption

- at rest: LUKS2 encryption with aes-xts-plain64 (key length 512 bits)
- backups: AES-256-CBC encryption on the application server (separate storage)

Compliance by the employee

- Data protection training with regular reviews
- Declaration of commitment to data secrecy
- IT security provisions
- Onboarding/offboarding processes for employees

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- ISO 27001-certified data centre in Frankfurt, Germany; self-managed VPS infrastructure
- External backup arrangements
- Measures to ensure rapid recoverability in accordance with Article 32(1)(c) GDPR, including a disaster recovery plan. Daily full backup of the database server; restoration of individual customer databases is possible (RPO up to 24 hours, RTO up to 24 hours).

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- **Data protection management including regular employee training:** The Provider provides its employees with all necessary information and means for implementing measures in order to ensure a data protection-compliant design of technology and organisation. All employees of the Provider are obliged to preserve and actively promote the security of information and information systems to which they have access.
- **Vulnerability assessments:** The Provider conducts regular vulnerability assessments and security reviews of the systems and web applications used. The reviews are based on recognised standards and best practices, in particular the OWASP Web Security Testing Guide (WSTG), the OWASP Top 10, and NIST SP 800-115.
- **Incident response management:** The aim is to restore the defined operating condition of an IT service for the Customer within the scope of the agreed service quality in order to achieve minimisation of the impairment of business processes. As soon as incident management sees compliance with the

service levels at risk, escalation takes place. Within the IT organisation, incident management forms the interface to other IT service areas (e.g. problem, change, configuration, release ...). In addition to disruptions, other customer inquiries (service requests) of users are also recorded, initial assistance is provided and, if necessary, further processing is coordinated in the downstream support units.

- **Data protection by design and by default (Art. 25 para. 2 GDPR):** In the planning phase for the procurement of a new data application or modification of an existing data application, an internal catalogue of requirements is created. On the basis of the catalogue of requirements, the lawfulness of the intended data processing is examined internally in advance. Under the aspects of data avoidance and data minimisation, the requirements for a data protection-compliant design of the data application as well as the technical and organisational prerequisites are defined.
- **Order control of sub-processing relationships**: No processing on behalf within the meaning of Art. 28 GDPR without corresponding instruction of the controller, e.g.: strict selection of the processor (ISO certification, ISMS), prior duty to satisfy itself, follow-up controls.