

Data Processing Agreement according to art. 28 GDPR

Version 2.0

Agreement between

The Controller – hereinafter referred to as the „Customer“, who agrees to this agreement

and

TimeTrack GmbH, Paulanergasse 13/8, 1040 Vienna, Austria – the Processor – hereafter referred to as the „Provider“.

§ 1 Subject matter and duration of the Agreement

(1) The subject matter of the Agreement is the transfer of data for the provision of services. These services are set out in the General Terms and Conditions applicable at the time of the confirmation of this agreement, the product description on the website www.timetrackapp.com and, if applicable, a signed quotation (collectively referred to as the „Service Agreement“).

(2) The duration of this Agreement corresponds to the duration of the Service Agreement. The cancellation of this Agreement automatically corresponds to the cancellation of the Service Agreement.

§ 2 Specification of the Agreement Details

(1) The undertaking of the contractually agreed Processing of Data shall be carried out within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Customer and shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection offered by named subcontractors in Section 6 is either established via a decision of the European Commission (Article 45 Paragraph 3 GDPR) or is the result of an approved Certification Mechanism (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).

(2) The type of personal data and categories of data subjects used are precisely defined in [Appendix 1](#) of this Agreement.

§ 3. Technical and Organisational Measures

(1) Before the commencement of processing, the Provider shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Agreement, specifically with regard to the detailed execution of the Agreement, and shall present these documented measures to the Customer for inspection. Upon acceptance by the Customer, the documented measures become the foundation of the Agreement. Insofar as the inspection/audit by the Customer shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Provider shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in connection with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account [Details in Appendix 2].

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Provider to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

§ 4. Rectification, restriction and erasure of data

(1) The Provider may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer. Insofar as a Data Subject contacts the Provider directly concerning a rectification, erasure, or restriction of processing, the Provider will immediately forward the Data Subject's request to the Customer.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Provider in accordance with documented instructions from the Customer without undue delay.

§ 5. Duties of the Customer

(1) The Customer is the owner of Customer data and the bearer of all rights concerning Customer data.

(2) The Customer is responsible for the lawfulness of processing of Data Subjects as well as the adherence to the rights of the Data Subjects.

(3) The Customer is responsible for record keeping with respect to national or Member State law. Provider assumes no liability for the completeness of data for adherence to any regulations or laws.

§ 6. Quality assurance and other duties of the Provider

In addition to complying with the rules set out in this Agreement, the Provider shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Provider ensures, in particular, compliance with the following requirements:

- Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Provider entrusts only such employees with the data processing outlined in this Agreement who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Provider and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Customer, which includes the powers granted in this Agreement, unless required to do so by law.
- Implementation of and compliance with all Technical and Organisational Measures necessary for this Agreement in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 2].
- The Customer and the Provider shall cooperate, on request, with the supervisory authority in performance of its tasks.
- The Customer shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement. This also applies insofar as the Provider is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Agreement.
- Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the data processing by the Provider, the Provider shall make every effort to support the Customer.
- The Provider shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- Verifiability of the Technical and Organisational Measures conducted by the Customer as part of the Customer's supervisory powers referred to in item 8 of this Agreement.

§ 7. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not

include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services 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 equipment. The Provider shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Customer's data, even in the case of outsourced ancillary services.

(2) The Provider may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Customer. The Customer agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company	Address, Country	Service
Digital Ocean	101 Avenue of the Americas, 10th Floor, New York, NY, 10013, United States (Data Center in Frankfurt, Deutschland)	Hosting Provider (not applicable for on-premise customers)
Stripe	1 Grand Canal Street Lower, Grand Canal Dock, D02 H210, Dublin, Ireland	Payment Processing
AWS-Amazon Webservices	5 rue Plaetis, L-2338, Luxemburg, Luxemburg	Transactional E-Mails
Droptop GmbH/Linevast	Am Grashorn 8, 14548 Schwielowsee, Deutschland	Website- and Mail-Hosting

Changing an existing subcontractor is permissible when:

- the Provider submits such an outsourcing to a subcontractor to the Customer in writing or in text form with appropriate advance notice; and

- the Customer has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Provider; and
- the subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Customer to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Provider shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor requires the express consent of the main Customer (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

§ 8. Audit rights of the Customer

(1) The Customer has the right, after consultation with the Provider, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. The Customer has the right to convince itself of the compliance with this agreement by the Provider in its business operations by means of random checks, which are to be announced in good time.

(2) The right shall ensure that the Customer is able to verify compliance with the obligations of the Provider in accordance with Article 28 GDPR. The Provider undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the technical and organisational measures.

(3) In exercising the rights under this section, the customer must act with consideration to not affect the business operations of the provider, otherwise the customer may be charged reasonable administrative costs.

§ 9. Communication in the case of infringements by the Provider

(1) The Provider shall assist the Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. This includes: e.g.:

- ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of

a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;

- the obligation to report a personal data breach immediately to the Customer;
- the duty to assist the Customer with regard to the Customer's obligation to provide information to the Data Subject concerned and to immediately provide the Customer with all relevant information in this regard;
- supporting the Customer with its data protection impact assessment;
- Supporting the Customer with regard to prior consultation of the supervisory authority.

(2) The Provider may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Provider.

§ 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 never be created without the knowledge of the Customer, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) Within 30 days of termination of the Agreement, Customer may request the return of Customer data (to the extent that any data has not already been deleted by the Customer). Data will be provided in a commonly used and open format. Requests for such data shall be sent to info@timetrack.com. 30 days after effective termination date of the Agreement, Provider shall delete all Customer data (including copies) in their possession or control, unless Provider is required by applicable Union or Member State law to retain some or all of Customer data. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Agreement shall be stored beyond the Agreement duration by the Provider in accordance with the respective retention periods. They may hand such documentation over to the Customer at the end of the Agreement duration to relieve the Provider of this contractual obligation.

§ 12. Relationship with General Terms and Conditions

Provided no special arrangements have been made in this Agreement, the provisions of the General Terms and Conditions apply. In the case of conflict between this Agreement and provisions of other agreements, in particular under the General Terms and Conditions, the provisions under this Agreement shall prevail.

§ 13. Effectiveness of Agreement

The acceptance of this Agreement may only be carried out by authorised persons of the Customer.

This Agreement applies upon written or electronic confirmation. This Agreement orients itself on the GDPR and is therefore effective as of 25th May 2018.

Appendix 1 – Data Processing

1. Categories of Data Subjects

Employees, contractors, agents, clients and other data subjects on behalf of Customer that should have access to and use TimeTrack systems, collectively known as “Users”.

2. Types of Personal Data

Category	Data
Name	First name*, Last name*
User Identification	Username*
Electronic identification data	IP address*
Contact Information	E-Mail address*, Phone number, Contact address and country
Localisation Data	GeoLocation/GPS data
Customer Entered Data	This covers any other Personal Data which the customer may input into user-defined

Data marked “*” are required. Any other data are considered optional.

Appendix 2 – Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

Physical Access Control

- No unauthorised access to offices. Authorised users have access, visitors must be permitted entry to the premises
- Access control system. Logging of employee arrival and departure. Access only granted to employees; access revoked as part of employee off-boarding process.
- Visitor logging; monitored reception area which unregistered visitors may not leave. Visitor escorting on premises; visitors are not left unattended.
- Fire detection systems in every room; linked to central control panel in building with direct link to fire services

Internal Access Control, User Rights

- No unauthorised Reading, Copying, Changing or Deletion of Data; actions are logged and reviewed. Training of employees as to what is permissible.
- Rights authorisation concept. Employees only have granular access for the activities they need to perform.
- Access rights granted on a per role and need basis. Periodically reviewed. Employees only granted access to resources and systems strictly required for their job.
- Logging of access and system events, such as connection, disconnection, changes, deletions.

Isolation Control

- Separation of customer accounts in databases
- Separation of customer data within account in database tables
- Separate environments for development, staging and production

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

Data Transfer Control

- No unauthorised Reading, Copying, Changing or Deletion of Data
- Visitors have separate Wireless Network

Data Entry Control

- Verification, whether and by whom personal data are entered into a Data Processing System by Provider
- Protocol of access attempts, including IP address and username
- Protocol of account activity, such as request logs

- User rights and roles within Software of Provider, preventing unauthorised manipulation

Employee Adherence

- Data Protection Awareness training, with periodic review processes
- Confidentiality agreements on handling data and responsibilities associated
- IT Security Policy
- Employee onboarding/offboarding processes

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

- Multiple data centres, increasing redundancy *
- Off-site backup policy, with backups hosted in a different data centre *
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR) *
- Status page, openly communicating availability of services and components *
- Disaster Recovery Plan *

Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Data Processing Agreements with subcontractors

* not applicable for on-premise customers