

Data Processing Agreement

DeskTime · SIA DeskTime — Riga, Latvia

This personal data processing agreement («**DPA**») forms an integral part of the Terms of Service for the use of DeskTime and is a binding agreement between SIA DeskTime («**DeskTime**») and any natural or legal person («**Client**») that uses DeskTime's time tracking and any other Services as provided by DeskTime («**Service**») other than for personal and private use to monitor and process personal data of their employees or other individuals («**End-Users**») within their DeskTime account.

1. Definitions

- «**Data Protection Laws**» means GDPR and laws implementing or supplementing the GDPR, to the extent applicable;
- «**GDPR**» means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- «**Personal Data Breach**» means a breach of security leading to the accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed (in each case as defined under the GDPR);
- «**Personal Data**» means any information relating to a data subject (as defined under Data Protection Laws);
- «**Standard Contractual Clauses**» means the Standard contractual clauses for data transfers between EU and non-EU countries as adopted by the European Commission, amended as required;
- «**Sub-processor**» means any entity (including any third party, but excluding an employee of DeskTime) engaged by DeskTime to process Personal Data on the Client's behalf;
- «**Third Countries**» means all countries outside of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time;
- The terms «controller», «personal data», «processing», «processor», and «supervisory authority» shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly;
- Unless otherwise defined herein, all capitalized terms used in this DPA shall have the meaning ascribed to them in the Terms of Service. In the event of any conflict between the definitions in this DPA and those in the Terms of Service, the definitions in this DPA shall prevail solely for the purposes of data processing activities governed hereby.

2. Scope and roles

2.1 This DPA applies to the processing of Personal Data in the scope of the Service provided by DeskTime to Clients regarding the time-tracking services and any other Services as provided by DeskTime. This DPA constitutes an annex to the Terms of Service, which governs the rights and obligations of the parties regarding the Service provided by DeskTime.

2.2 For the processing of Personal Data under this DPA, the Client shall be regarded as the data controller, and DeskTime shall be regarded as the data processor.

3. Details of processing

3.1 DeskTime shall process Personal Data in a manner consistent with this DPA, the instructions of the Client, and/or to the extent necessary to provide the Services to the Client under the Terms of Service and as further set out in Annex 1. For the avoidance of doubt, unless agreed in writing by the Parties, DeskTime shall not be permitted to process the Personal Data for its own purposes.

3.2 Parties undertake to comply with their obligations under the Data Protection Laws. Each Party is solely responsible for compliance with the Data Protection Laws that apply to it.

3.3 If DeskTime cannot comply with the Client's instructions for whatever reason (including if the instruction violates the Data Protection Laws), it agrees to inform the Client of its inability to comply as soon as reasonably practicable. Any failure by DeskTime to notify the Client shall not affect the Client's responsibility and liability for its instructions.

3.4 The Client confirms that this DPA, along with the Client's configuration of or use of any settings, features, or options in the Service (as may be amended and changed by the Client from time to time), constitutes sufficient instructions to DeskTime regarding the processing of Personal Data, and therefore constitutes a binding data processing agreement in accordance with Data Protection Laws.

4. Duties and obligations of the Client

4.1 The Client represents and warrants that it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in connection with its processing of End-User Personal Data and any processing instructions it issues to DeskTime.

4.2 The Client represents and warrants that End-User Personal Data has been collected on a valid, lawful basis, that it has provided all required notices and obtained all necessary consents, permissions, and rights as required under Data Protection Laws, and that it is entitled to transfer or otherwise make such End-User Personal Data available to DeskTime for processing for the purposes described in this DPA. The Client shall have sole responsibility for the accuracy, quality, legality, and means of acquisition of End-User Personal Data.

5. Return or deletion of Personal Data

5.1 DeskTime shall process Personal Data for as long as the Client has an account with DeskTime. The Client may, at any time, request deletion of End-User Personal Data and export such data using the functionalities made available within the Services.

5.2 Upon termination or expiration of the Terms of Service, DeskTime shall, at the Client's choice, delete or return End-User Personal Data (including by enabling data export through available functionalities) and delete any remaining copies, unless applicable law requires retention. DeskTime may apply irreversible anonymization in lieu of deletion where appropriate. Upon request, DeskTime shall confirm such deletion or return in writing.

5.3 Unless otherwise required or permitted by applicable law, DeskTime has no obligation to store the Client's data after termination of the Service agreement with the Client.

6. Sub-processors

6.1 DeskTime works with third parties (Sub-processors) that provide DeskTime with different services needed in the ordinary course of business. The Sub-processors currently engaged by DeskTime and authorized by the Client are available [here](#).

6.2 DeskTime may continue to use the Sub-processors already engaged at the date of this DPA, ensuring that:

- 6.2.1 DeskTime has carried out adequate due diligence to ensure that the Sub-processor is capable of providing a sufficient level of protection for Personal Data;
- 6.2.2 DeskTime has ensured that the arrangement between DeskTime and the relevant Sub-processor is governed by a written contract that includes terms offering at least the same level of protection for Personal Data as those set out in this DPA and that meet the requirements of Article 28(3) of the GDPR.

6.3 If any of the engaged Sub-processors are unable to fulfill their duties in accordance with the data processing agreement referred to in Section 6.2.2., DeskTime shall remain fully liable to the Client for the Sub-processor's duties and activities. DeskTime shall be liable for any consequences of the Sub-Processor's activities in connection with the processing of Personal Data.

6.4 DeskTime shall notify the Client 30 days prior to any intended changes in the Sub-processors. If the Client objects to the proposed Sub-processor based on reasonable data protection grounds, the Client shall notify DeskTime in writing within a 15-day period, specifying the basis for the objection. DeskTime will consider such objection in good faith and may, at its discretion, take reasonable steps to address the concern. If the objection cannot be reasonably resolved, DeskTime may either refrain from engaging the Sub-processor for the relevant processing or allow the Client to terminate the use of Services. In such cases, the Client shall not be liable under the Terms of Service or applicable law for any termination by the Client under this Section.

6.5 Subject to the requirements of Clause 6.2, the Client agrees that DeskTime may use Sub-processors located outside the European Economic Area (EEA). In such cases,

DeskTime shall ensure that any transfer and processing of Personal Data complies with applicable Data Protection Laws, including through the use of EU Standard Contractual Clauses, adequacy decisions of the European Commission, or other valid transfer mechanisms recognized under applicable law.

7. Security

7.1 DeskTime shall take appropriate technical, organizational, and administrative safeguards designed to protect the confidentiality, integrity, and availability of Personal Data. The specific security measures implemented by DeskTime are described in Annex 1 of this DPA.

7.2 DeskTime shall treat all Personal Data as confidential. DeskTime shall ensure that all persons and parties (employees, agents, and other persons involved in processing of the Personal Data) have signed and are bound by an adequate confidentiality agreement or are under any other binding obligation of confidentiality.

7.3 DeskTime is not violating the non-disclosure obligation if disclosure of personal data is mandatory under applicable laws.

8. Personal Data Breach

8.1 In case of a Personal Data Breach, DeskTime shall notify the Client without undue delay and in compliance with the obligations set out in the Data Protection Laws. When notifying the Client, DeskTime shall provide details on the nature of the Personal Data Breach, likely consequences, contact point for further information, and the measures taken or proposed to address and mitigate the breach.

8.2 If the information cannot be provided simultaneously, such information may be provided in phases without undue delay.

8.3 Any notification or response by DeskTime regarding a Personal Data Breach shall not be interpreted as an admission of fault or liability. DeskTime shall not be responsible for reviewing or determining any legal or regulatory notification obligations applicable to the Client. The Client remains solely responsible for assessing and fulfilling any obligations to notify regulators or data subjects due to a Personal Data Breach.

8.4 Notifications of Personal Data Breach shall be sent to the main contact point of the Client as set in the Client account, and the Client is responsible for ensuring that such contact information remains accurate and up to date.

9. Assistance to the Client

9.1 Taking into account the nature of the processing, DeskTime shall provide reasonable assistance to the Client in fulfilling its obligations under applicable Data Protection Laws, including by providing appropriate technical and organizational support in connection with the investigation of Personal Data Breaches and related notification obligations, demonstrating compliance with Data Protection Laws, and, where applicable, conducting data protection impact assessments and consultations with supervisory authorities.

9.2 If DeskTime receives (i) any request from an End-User relating to Personal Data processed during the Services (including requests for access, rectification, erasure, restriction, portability, or similar rights), (ii) any complaint or claim relating to the processing of Personal Data, or (iii) any order, demand, warrant, or other legal request requiring disclosure of Personal Data, DeskTime shall promptly notify the Client, unless prohibited by applicable law.

9.3 DeskTime shall not respond to such requests, complaints, or legal demands without the Client's prior authorization, unless required to do so under applicable law or by a competent authority.

10. Audit

10.1 Upon Client's written request, DeskTime agrees to provide sufficient information to demonstrate compliance with the obligations laid down in this DPA and Data Protection Laws. This information should be provided to the extent that such information is within DeskTime's control, and DeskTime is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

10.2 If the provided information is not sufficient to confirm DeskTime's compliance with this DPA, DeskTime agrees to allow and contribute to a data processing audit, provided that any such audit does not involve the review of any third-party data and that the records and information access in connection with such audit are treated as confidential information.

10.3 Such audits are allowed to be carried out by the Client or independent auditors authorized by the Client. The Client shall bear the costs of any such audit.

10.4 Such an audit shall be carried out at the time agreed between the parties, within 1 month from the moment the Client has requested the audit in writing. The auditor will have to sign a confidentiality agreement, which includes an obligation not to disclose business information in its audit report, and the final report will also be provided to DeskTime. The audit will be carried out during the normal working hours of DeskTime, without interfering with DeskTime's business activities.

11. Term and Termination

11.1 This DPA shall take effect as of the moment of agreeing to the Terms of Service of DeskTime by the Client and continue in full force and effect as long as the Client is using the Services and has an account with DeskTime, and until all Personal Data is returned to the Client or deleted in accordance with the provisions of this DPA or applicable Data Protections Laws, after which this DPA will automatically simultaneously terminate, with the exception of the clauses which by their nature should continue to remain in full force and effect.

12. Miscellaneous

12.1 DeskTime may occasionally change this DPA, for example, when new services or features are introduced. In case of amendments or any changes, DeskTime will inform the Client in due time by sending an electronic notification to the Client's representative and indicating the nature and scope of the amendments, giving the Client the right to terminate the Services. The amendments are applied from the moment indicated in this section of the webpage.

12.2 DeskTime shall not be liable for any claims or complaints from data subjects regarding any action taken by DeskTime in accordance with instructions received from the Client. The Client shall indemnify and hold harmless DeskTime against all claims, liabilities, costs, expenses, loss, or damage (including consequential losses, loss of profit, loss of reputation, all interest, penalties, legal, other professional costs and expenses) incurred by DeskTime arising directly or indirectly from the breach by the Client.

12.3 This DPA shall be governed by the laws of the Republic of Latvia, and any action or proceeding related to this DPA (including those arising from non-contractual disputes or claims) shall be brought in the courts of the Republic of Latvia.

In case of any questions about these Terms or DeskTime's data processing practices, please contact us by email at support@desktime.com or by using the contact details below:

SIA DeskTime

Data Protection Officer

Address: Riga, Ojāra Vācieša iela 6B, Latvia

ANNEX 1

Details of Processing of Personal Data

This Annex 1 forms a part of the DPA and includes details of the processing of Personal Data that DeskTime will perform on behalf of the Client.

Nature and purpose of processing

DeskTime processes End-User Personal Data on behalf of the Clients to provide its Services, including the collection and storage of data on working hours, attendance, tasks, and activity, generation of reports and analytics, and the facilitation of End-User management functions such as project tracking and time planning.

Categories of data subjects

Client's employees, representatives, and other End-Users that are registered in the Client's account.

Categories of personal data

Depending on the use of Services and available features enabled by the Client, DeskTime may process the following End-User Personal Data:

- Full name, email address, password, phone number, photo
- Location, time zone, start and end time of workday, work duration, hourly rate, offline time, time spent on breaks, private time, absence calendar, information about colleagues, screenshots of the computer screen, information provided in the calculation tool of project costs, number of keystrokes or mouse movements
- IP address (including the IP address indicated by the Client as workplace IP address)
- Browser type, browser software version, names of applications used, names of tasks to be worked on, websites visited, DeskTime Client version, the path to the application
- Communication history if customer service is provided
- Other data that DeskTime can receive during the provision of the Service and that, in connection with other information, may contain personal data

Technical and organizational security measures

DeskTime maintains an information security management system aligned with industry best practices and is certified under ISO/IEC 27001, ensuring a systematic approach to managing and protecting information security.

1. Physical security measures

- Physical access to premises is restricted through controlled entry mechanisms (e.g., locked facilities, access controls)
- Access rights to facilities are documented and regularly reviewed
- Appropriate measures (e.g., video surveillance or equivalent controls) are implemented to detect and prevent unauthorized physical access

2. Network and system security

- Firewalls and appropriate network security controls are implemented and maintained to protect against unauthorized access
- Systems are monitored to detect and prevent cyber threats and unauthorized activities
- Network segmentation and secure configurations are applied where appropriate

3. Encryption and data protection

- Personal Data is protected using industry-standard encryption in transit and at rest, where appropriate
- Encryption keys are securely managed, including regular rotation and access restrictions

4. Access control and authentication

- Access to systems and Personal Data is restricted on a need-to-know basis and in accordance with the principle of least privilege
- User authentication and access management processes are implemented and regularly reviewed
- Access rights are promptly updated or revoked when no longer required

5. Logging and monitoring

- The DeskTime system and access activity are logged to provide an audit trail
- Logs are regularly reviewed to detect anomalies, unauthorized access, or security incidents
- Continuous monitoring is implemented where appropriate to ensure system security and availability

6. Data integrity and availability

- Measures are in place to ensure the integrity and accuracy of Personal Data
- Regular data backups are performed and tested to ensure availability and recovery
- Systems are monitored to detect errors and ensure ongoing availability of services

7. Organizational security measures

- Internal policies and procedures governing data processing and information security are established and maintained
- Employees receive regular security and data protection training
- Personnel are subject to confidentiality obligations
- Data protection and security responsibilities are clearly assigned

8. Incident management

- An incident response plan is established and maintained to detect, respond to, and mitigate security incidents
- Security incidents are documented and managed in accordance with established procedures

9. Business continuity and risk management

- Business continuity and disaster recovery plans are implemented and regularly tested
- Risk assessments are conducted periodically to identify and mitigate security risks
- IT systems and continuity measures are regularly evaluated and updated

10. Compliance and effectiveness review

- Security measures are regularly tested, assessed, and evaluated for effectiveness
- Audits and reviews are conducted to ensure ongoing compliance with applicable Data Protection Laws
- Security measures are updated as necessary to address evolving risks and industry standards

SIA DeskTime · Data Processing Agreement · Annex 1 · Riga, Latvia