

PRIVACY POLICY

DeskTime respects the privacy of its users and is fully committed to protecting their personal data. This Privacy Policy explains how DeskTime (“DeskTime”, “we”, “us”, “our”) processes information about individuals, including personal data, in relation to the use of the DeskTime.com website and the real-time time tracking service that analyzes productivity (“Service”). Below you may find detailed information about what type of information we collect about individuals and why, what we do with it, and how we handle such information.

By accessing or using this website or any of our Services, you agree to the terms set out in this Privacy Policy, Cookie Policy, Terms of Service, and other terms and policies posted on our website. If you do not agree to this Privacy Policy, you must leave this website and discontinue all use of any of our Services.

TABLE OF CONTENTS

1. INTRODUCTION
2. PROCESSING OF DATA ON BEHALF OF CLIENTS BY DESKTIME AS DATA PROCESSOR
3. PURPOSES AND GROUNDS FOR PROCESSING
4. INFORMATION WE COLLECT FROM DESKTIME USERS
5. INFORMATION WE COLLECT FROM DESKTIME WEBSITE VISITORS
6. RETENTION PERIOD
7. SHARING YOUR PERSONAL DATA WITH THIRD PARTIES
8. DATA SUBJECTS’ RIGHTS
9. PERSONAL DATA SECURITY
10. DATA PROTECTION AUDIT
11. PRIVACY POLICY CHANGES
12. GOVERNING LAW
13. CONTACT INFORMATION

1. INTRODUCTION

- 1.1. This Privacy Policy governs the processing of Personal Data of independent individual users (the “User” or “you”) of the DeskTime Service, visitors of the DeskTime website (“you”) as well as the processing of Personal Data by DeskTime on behalf of companies, organizations, institutions, groups of people, etc., that track time of their employees or other individuals within their DeskTime account group (“Client”) within the Service.
- 1.2. DeskTime shall process Personal Data in accordance with applicable data protection laws and in respect of Data Subjects within the European Economic Area (“EEA”) DeskTime shall comply with requirements of European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“GDPR”).
- 1.3. The terms “Personal Data”, “Data Subject”, “Processing”, “Controller”, “Processor” and “Supervisory Authority” as used in this Privacy Policy shall have the same meanings as given in the GDPR.
- 1.4. DeskTime acts as a Data Controller and sets the purpose and means for processing the following data:
 - a) Personal Data of the Users who are themselves the clients of DeskTime and who transmit their Personal Data directly to DeskTime, such as freelancers and other

- individuals who register for DeskTime independently (create DeskTime account for their own use);
- b) Personal Data of individuals who subscribe for receiving commercial communication and other news and updates from DeskTime, but who are not registered users of DeskTime Service.
- 1.5. Identity and contact details of the Data Controller in respect of the aforementioned data - Fast Brands LLC, a company registered in the Delaware, USA, address: 19749 Dearborn St, Chatsworth, California 91311, USA.
- 1.6. When DeskTime processes Personal Data that has been transferred to DeskTime by the Clients, DeskTime acts as the Data Processor.

2. PROCESSING OF PERSONAL DATA ON BEHALF OF CLIENTS BY DESKTIME AS DATA PROCESSOR

- 2.1. This section concerns DeskTime Clients that transfer Personal Data of end-users of the Service, such as personal data of Client's employees, to DeskTime. In respect of such data, the Client sets the purpose and means of processing Personal Data, therefore the Client is the Data Controller.
- 2.2. DeskTime processes end-users' Personal Data on behalf of the Client, and DeskTime only accesses the data for the purpose of rendering the Service, therefore DeskTime is the Data Processor.
- 2.3. If you as a Data Subject are the end-user of DeskTime Service and your profile was created by your employer, the privacy policy of the Client (e.g. your employer or other organization that created your account), on whose behalf we process the data, will apply. This means that any enquiry, request, objection or complaint that you as a Data Subject may have in connection with the processing of Personal Data that forms part of your DeskTime account should be addressed to and resolved by the Client as the Data Controller.

Details of processing

- 2.4. When the Client creates accounts for end-users in its group the Client transfers the Personal Data of such end-users to DeskTime. In that way the Client instructs DeskTime to process Personal Data in order to provide Service to the Client pursuant to the agreement concluded between the Client and DeskTime.
- 2.5. For the avoidance of doubt, this Privacy Policy contains complete and final instructions of the Client to DeskTime in relation to processing of Personal Data of end-users, and this Privacy Policy constitutes a binding data processing agreement.
- 2.6. DeskTime will always process all Personal Data on behalf of the Client following the Client's instructions and in compliance with the applicable data protection laws and regulations including requirements of GDPR where applicable.

Type of personal data and categories of data subjects

- 2.7. Categories of data subjects whose Personal Data will be processed on behalf of the Client include the Client's employees, representatives and other end-users that will be registered under the Client's group account. The information about these individuals that may contain Personal Data are indicated in Paragraph 4.
- 2.8. Client represents that it has acquired all necessary consents and/or relies on other appropriate legal basis for the processing of Personal Data of end-users. Client

confirms that end-users have been informed about the fact that their Personal Data is transferred to DeskTime as a Processor and other third parties used by DeskTime for the provision of Service.

Duration of the processing

- 2.9. DeskTime will process the aforementioned data for as long as DeskTime provides the Service to the Client and the Client has an active DeskTime account.
- 2.10. When an end-user's account is deleted by the Client, DeskTime will process data of deleted accounts in the Client's group for statistical and analytical interests of the Client. However, such data can be deleted at any time upon Client's request.
- 2.11. After terminating contractual relationship between DeskTime and the Client, we may continue to store some Personal Data, but limited to the minimum amount required, as might be necessary for us to comply with legal obligations, to ensure reliable back-up systems, to resolve disputes between the Client and DeskTime, if any, to prevent fraud and abuse, to enforce DeskTime agreements, and/or to pursue legitimate interests of DeskTime or third parties.

Sub-processors

- 2.12. The Client consents that DeskTime, for the purpose of providing Service to the Clients, uses sub-processors that provide DeskTime the services indicated in Paragraph 7. DeskTime ensures that it only uses sub-processors that comply with the same data protection obligations as set out in this Privacy Policy, in particular provides sufficient guarantees and has implemented appropriate technical and organizational measures and otherwise comply with the requirements of GDPR where applicable. If such sub-processor fails to fulfil its data protection obligations, DeskTime shall remain liable to the Client.

Assistance to the controller

- 2.13. Taking into account the nature of the processing, DeskTime as a Data Processor will assist the Client with provision of technical or organizational measures, insofar as possible, for the fulfilment of the Client's obligations as a Data Controller in relation to:
 - a) Any requests from the Client's end-users in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of their Personal Data that DeskTime processes on behalf of the Client. In the event that a Data Subject sends such a request directly to DeskTime, DeskTime will promptly forward such request to the Client; and
 - b) The investigation of Personal Data breaches and the notification to the Supervisory Authority and Client's end-users regarding such Personal Data breaches; and
 - c) Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

Return and deletion of data

- 2.14. Unless otherwise required by applicable law, DeskTime has no obligation to store the Client's data after termination of the agreement with the Client and deletion of the Client's account and all accounts associated with it.

- 2.15. At the choice of the Client, DeskTime will delete or return all the Personal Data to the Client after the end of the provision of Service relating to processing and shall delete existing copies, unless applicable law requires DeskTime to store such Personal Data.

3. PURPOSES AND GROUNDS OF PROCESSING

- 3.1. DeskTime as a Controller shall process your Personal Data in order to provide you with the Service, to improve our Service, to solve any Service related issues you may have and to ensure that you receive the best customer experience possible.
- 3.2. DeskTime collects and processes your Personal Data including, but not limited for the following purposes:
- Registering you for the use of the Service by creating your DeskTime account;
 - Sending you invoices and processing payments for the Service;
 - Personalizing your use of the Service when you set up your account settings;
 - Analyzing your performance as a feature within our Service;
 - Communicating with you to inform you about DeskTime Service and provide you any Service related support, answer your questions and process your requests;
 - To improve Service or to develop new features within the Service;
 - Analytics and measurement to understand how our Services are used. For example, we analyze data about your usage of the Service to optimize product design, to generate reports and create statistics about use of DeskTime Service;
 - Delivering personalized ads, promotions and offers to you;
 - Protecting legal interests of DeskTime, its Clients, Users and other third persons and for legal reasons such as, e.g. enforcing our Terms & Conditions or Privacy Policy, complying with any applicable law and assisting law enforcement authorities.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

- 3.3. DeskTime only collects and processes your Personal Data where we have lawful basis. Legal grounds for the processing of your Personal Data vary depending on the specific group of data and the purposes for processing it. Note that we may be processing the same Personal Data for several purposes simultaneously and, respectively, on more than one legal ground.

Contract. Most of the time the legal basis for processing your Personal Data is the contractual relationship between you as the User of Service and DeskTime since we need certain information to conclude the contract and to fulfil our obligations arising out of this contract.

Legal obligation. In some cases, DeskTime processes Personal Data on basis of legal obligations imposed on us by applicable law, such as financial and tax reporting obligations or if we have to respond to legal process.

Legitimate interests. Processing of your Personal Data is necessary for pursuing legitimate interests of DeskTime or for the legitimate interests of third parties, always provided that such processing shall not outweigh your rights and freedoms. For example, we may process your data for marketing purposes based on our legitimate interest of growing and improving our business. Other legitimate interests include maintaining Service to meet the needs of our Users and Clients, advertising to make our Service freely available for users, detecting and preventing fraud, abuse, security and technical issues with the Service, fulfilling obligations to our partners, enforcing legal claims, etc.

Consent. Some Personal Data we process based on your consent. This is the information that we do not need for performance of the contract, but you voluntarily may provide us with such information. By taking such clear affirmative action as uploading your photo to DeskTime account, entering notes, entering your e-mail address in blog subscription field and clicking “subscribe” you signify your consent to the processing of your respective Personal Data. By using the absence calendar and adding “away time” you take affirmative action and manifestly make this information available at your DeskTime account. Note that you have the right at any time to delete this information and withdraw your consent.

4. INFORMATION WE COLLECT FROM DESKTIME USERS

- 4.1. DeskTime collects, generates and receives information in a variety of ways when you use the Service. Some of this information constitutes Personal Data.

Information you provide upon creating your account

- 4.2. As a User of DeskTime Services you provide us with information containing your Personal Data. Upon registration and creating your profile you provide us with the following information:

- Full name
- E-mail address
- Password
- Payment information
- Phone number
- Social media account information (if you register by linking your social media account to your DeskTime account)
- Photo (voluntary)

- 4.3. Please note that some options within the Service allow our Users to voluntarily disclose their Personal Data such as your photo, or any data that you enter into notes, as well as some special category data, e.g. data concerning health, when using the absence calendar function. DeskTime does not oblige Users to submit such data since it is not essential for provision of the Service, and Users are able to use the Service without providing us with the aforementioned data.

Third-party integrations

- 4.4. You can choose to integrate third-party services in relation to certain aspects of DeskTime Service. A third-party service is software that integrates with the Service and you can enable or disable such integration for your DeskTime account.
- 4.5. Once enabled, the relevant third-party service provider may share certain information with us. For example, if you choose to use a third-party service (such as Facebook, Twitter, LinkedIn) to sign up for the Service, then the provider of such a service may send us your name, user ID, email address. Or if some other third-party application (e.g., project management service, Google or Outlook calendar) is enabled to permit data to be imported into Service, we may receive such information as you have elected to let the application make available to us. You should check the privacy settings of these third-party services to understand what data may be disclosed to us.

Information you provide by configuring your account

- 4.6. Upon configuring settings of your DeskTime account, including performance tracking preferences, you provide us with the following information, which in connection with other information may contain Personal Data:

Location, time zone, start and end time of your workday, work duration, start and stop time of work tracking, working days, tracking days, hourly rate, offline time input options, private time input options, application names to be collected, options to hide owners, absence calendar, information about colleagues, option to use calculation tool of project costs.

Information generated when using the Service

- 4.7. Some of the information processed by DeskTime is created by you using the Service, and this information may also contain Personal Data. DeskTime records the following information when you use the Service:

IP address where you logged in, browser type and browser software version, names of applications used, names of tasks to be worked on, websites visited, DeskTime client version, path to the application, start and end time of use, time spent on breaks, screenshots of your computer screen. DeskTime may record the number of keystrokes or mouse movements, but we do not record what you type or where you click.

- 4.8. When you are just the end-user and not the Client of the Service, the above-mentioned information is provided to DeskTime by the Client (e.g. your employer).

5. INFORMATION WE COLLECT FROM DESKTIME WEBSITE VISITORS

- 5.1. Upon visiting our website we may collect and process the following information that may contain your Personal Data:

- Your device and browser
- Your IP address
- Other information that is collected from cookies and similar technology we use.

Learn more about how we use cookies on our website by reading our [Cookie Policy](#).

- 5.2. When you subscribe to DeskTime blog, leave comments on blog entries, or submit a question to us, you are providing DeskTime with the following information that contains your Personal Data:

- Your name
- Your e-mail address

- 5.3. When you subscribe to our blog or newsletter we will process your e-mail address to send you informative materials, such as newsletters, advertisements and others. At any point in time you can unsubscribe from receiving the above-mentioned information in your e-mail footers.

6. RETENTION PERIOD

- 6.1. DeskTime retains Personal Data of User account for as long as you maintain your DeskTime account or as otherwise necessary for DeskTime to provide you the Service.
- 6.2. Data created by you when using the Service (paragraph 4.7) is kept by DeskTime for 13 months. After 13 months only general information like “arrival time”, “left time”, “deskttime time”, and “time at work” are kept for statistical purposes.

- 6.3. After you as a User terminate your relationship with us by deleting your DeskTime account or otherwise terminating the contract for DeskTime Service, we may continue to store certain information as reasonably necessary to comply with our legal obligations, to resolve disputes, if any, to prevent fraud and abuse, to enforce our agreement, and/or to protect our legitimate interests.

7. SHARING YOUR PERSONAL DATA WITH THIRD PARTIES

- 7.1. For DeskTime to be able to provide you with our Service, we work with third parties that provide us with different services we need in ordinary course of our business. Therefore, we share your Personal Data with such third-party service providers. They process your personal data on behalf of DeskTime.
- 7.2. The categories of recipients of your Personal Data include, hosting and server co-location service providers, communication and content delivery networks, data and cyber security service providers, billing and payment processing service providers, fraud detection and prevention service providers, web analytics, email distribution and monitoring service providers, session recording service, marketing service providers, legal and financial advisors, among others (“**Third-Party Service Providers**”).
- 7.3. Third-Party Service Providers only receive strict minimum amount of Personal Data as necessary for them to provide us with requested service. DeskTime shares Personal Data only with such Third-Party Service Providers that are able to demonstrate that they have implemented appropriate measures to ensure that Personal Data is processed in compliance with GDPR and other applicable laws and regulations.
- 7.4. In certain situations we might have a legal obligations to share your information with third parties. Such situation may arise when sharing your Personal Data with third party is required by law or when information is requested by public authorities.
- 7.5. DeskTime may share your Personal Data if DeskTime organizes the operation of Services within a different framework, or through another legal structure or entity, or if DeskTime is acquired by, or merged into or with another entity, or if DeskTime enter bankruptcy, provided however, that those entities agree to be bound by the provision of this Privacy Policy, with respective changes taken into consideration.
- 7.6. Personal Data processed by DeskTime may be transferred to Third-Party Service Providers that are located outside of EEA. If DeskTime transfers Personal Data to a Third-Party Service Provider located outside of EEA, DeskTime will only send Personal Data to such recipients that have taken adequate data processing and protection requirements and that are able to ensure an adequate level of protection or have provided adequate guarantees.

8. DATA SUBJECT’S RIGHTS

- 8.1. Individuals located in certain countries, including the European Economic Area, have certain statutory rights in relation to their Personal Data. Subject to any exemptions provided by law, you may have the right to request access to your Personal Data to seek to update, delete or correct this data, to restrict or object to processing of your data, as well as right to portability of your Personal Data.
- 8.2. You can use these rights by logging into your DeskTime account or by getting in touch with DeskTime using the contact information provided below in Paragraph 13.
- 8.3. Furthermore, if you believe that DeskTime has unlawfully processed your Personal Data, you have the right to submit a complaint to DeskTime by using the contact

information provided below, or you may submit complaint to a respective data protection supervisory authority in your country.

- 8.4. If you are an individual whose Personal Data has been provided to DeskTime by the Client (e.g. employee of the Client), please contact the Client to exercise your rights as a Data Subject stated above.
- 8.5. In case DeskTime receives complaint or request from individual, whose Personal Data has been provided to DeskTime by the Client, exercising his/her rights as a Data Subject, DeskTime will not respond to such complaint or request without prior written authorization by the Client.

9. PERSONAL DATA SECURITY

- 9.1. DeskTime uses reasonable organizational, technical, and administrative measures to protect the confidentiality, integrity, and availability of Personal Data. Unfortunately, no data transmission or storage system is guaranteed to be 100% secure, therefore we cannot guarantee absolute security of information. We encourage Users, Clients and their end-users to take care of their own Personal Data as well as Personal Data in their possession and set strong passwords for DeskTime account, limit access to computer and browser by signing out after end of session, and as possible avoid providing DeskTime with any sensitive information, disclosure of which could cause substantial harm to Data Subject.
- 9.2. All of DeskTime's authorized personnel involved in the processing of Personal Data provided to us have committed themselves to confidentiality obligations and shall not access or otherwise process Personal Data without authorization and if it's not necessary for the purposes such data was obtained in the first place.
- 9.3. In the event a Personal Data breach occurs, we will notify you in compliance with the obligations set out in applicable laws and will provide reasonable assistance regarding the investigation of Personal Data breaches and the notification to the supervisory authorities and data subjects regarding such personal data breaches.

10. DATA PROCESSING AUDIT

- 10.1. Upon Client's written request, DeskTime agrees to provide the Client with sufficient information to demonstrate compliance with obligations laid down in this Privacy Policy and applicable laws and regulations. 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 information provided to the Client does not provide sufficient information to confirm DeskTime's compliance with this Privacy Policy, then DeskTime agrees to allow for and contribute to data processing audits.
- 10.3. Such audits are allowed to be carried out by independent third party with good market reputation, provided that it has sufficient experience and competence to carry out data processing audits, and election of such auditor must be mutually agreed by both the Client and DeskTime.
- 10.4. The timing and other practicalities related to any such audit or inspection are determined by us and any such information and assistance are provided at exclusively the cost and expense of the Client, and we reserve the right to charge the Client for any additional work or other costs incurred by us in connection with the Client using such rights. The Client has rights to request the audit once every 2 years.

10.5. The auditor will have to sign confidentiality agreement which includes obligation not to disclose business information in its audit report, and the final report will also have to be provided to DeskTime.

11. PRIVACY POLICY CHANGES

11.1. DeskTime may occasionally amend this Privacy Policy for example in cases when we introduce new services or new features. The amendments to this Privacy Policy enter into force and are applied from the moment they have been uploaded to this page.

11.2. Therefore, we encourage you to check this page from time to time. By continuing to use our Services or otherwise providing Personal Data to us, after the amendments to this policy have been implemented, you agree to the updated terms of Privacy Policy.

12. GOVERNING LAW

This Privacy Policy shall be governed by the laws of California, and any action or proceeding related to this Privacy Policy (including those arising from non-contractual disputes or claims) will be brought in the courts of California, USA.

13. CONTACT INFORMATION

In case you have any questions about this Privacy Policy or our data processing practices, or if you would like to exercise any of your rights as a Data Subject regarding your Personal Data, please contact us by email support@desktime.com, or by using the contact details below:

Fast Brands, LLC
Attn: Data Protection Officer
Address: 19749 Dearborn St,
Chatsworth, California 91311,
USA

This Privacy Policy is effective from 25 May 2018