Time Doctor Customer DPA

Last Updated: 01.05.2023

This Data Processing Addendum ("**DPA**") between MyStaff LLC t/a Time Doctor ("**Time Doctor**") and the party identified as the Customer in the Agreement (defined below), forms part of and is subject to the Time Doctor Terms of Service (currently located at https://www.timedoctor.com/terms_of_service.html) or other written or electronic agreement incorporating this DPA governing the Customer's access and use of the Time Doctor Services ("**Agreement**"). Capitalized terms used herein and not otherwise defined in this DPA shall have the meaning set forth in the Agreement.

Customer enters into this DPA (including the Standard Contractual Clauses and UK Addendum, where applicable) on behalf of itself and any Affiliates authorized to use the Services under the Agreement and who have not entered into a separate contractual arrangement with Time Doctor. For the purposes of this DPA only, and except where otherwise indicated, the term "Customer" shall include Customer and such Affiliates.

The Parties agree as follows:

1. Definitions

1.1 "**Affiliates**" means any entity under the control of a Party where "control" means ownership of or the right to control greater than 50% of the voting securities of such entity.

1.2 "**CCPA**" means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq.), as may be amended, superseded or replaced.

1.3 "**Customer Data**" means any data (including personal data) submitted by or on behalf of Customer to the Services and the output of the Services that incorporates such content or data or is otherwise specific to Customer.

1.4 "**Data Protection Laws**" means European Data Protection Laws and the CCPA, as applicable to the processing of Personal Data under this DPA.

1.5 "**Europe**" means for the purposes of this DPA, the European Economic Area and/or its member states, the United Kingdom and/or Switzerland.

1.6 "**European Data Protection Laws**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) in respect of the United Kingdom, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and the Data Protection Act 2018 (together the "**UK Privacy Laws**"); (v) the Swiss Federal Data Protection Act ("**Swiss DPA**");

1.7 "**Personal Data**" means any information which is protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Law which Time Doctor processes on behalf of Customer under the Agreement, as more particularly described in **Annex A** of this DPA.

1.8 "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a

transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

1.9 "**Security Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed by Time Doctor under this DPA. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.10 "**Services"** means unless otherwise defined in the Agreement, the Time Doctor services to which the Customer has subscribed under and as more particularly described in the Agreement.

1.11 **"Standard Contractual Clauses"** or **"EU SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 and currently located at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf.

1.12 "**Sub-processor**" means any third party that has access to Personal Data and which is engaged by Time Doctor to assist in fulfilling its obligations with respect to providing the Services under the Agreement. Sub-processor's may include Time Doctor Affiliates but shall exclude Time Doctor employees, contractors and consultants.

1.13 "**Supervisory Authority**" means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with Data Protection Law.

1.14 **'UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

1.15 The lower case terms **"controller"**, "**personal data**" **"processor"**, "**process**", "**processing"** and **"data subject**" have the meanings given to them in applicable Data Protection Laws or if not defined therein, the GDPR, and the term **"service provider**" has the meaning set forth in the CCPA.

2. Scope of this DPA

2.1 This DPA applies where and only to the extent Time Doctor processes Personal Data on behalf of Customer that is subject to Data Protection Law as a processor (for the purposes of European Data Protection Law) or service provider (for the purposes of the CCPA) in the course of providing the Services pursuant to the Agreement.

2.2 Any processing of Personal Data under the Agreement shall be performed in accordance with applicable Data Protection Laws. However, Time Doctor is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that is not generally applicable to Time Doctor as a service provider.

3. Processing of Personal Data

3.1 **Permitted Purposes.** Time Doctor shall process Personal Data in accordance with Customer's documented lawful instructions, except where required by applicable law(s). For these purposes,

Customer instructs Time Doctor to process Personal Data for the following purposes: (a) to perform any steps necessary for the performance of the Agreement; (b) to provide, maintain and improve the Services provided to Customer in accordance with the Agreement; (c) processing initiated by end users in their use of the Services; (d) to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement (including this DPA); and (e) to comply with Time Doctor's legal obligations under applicable law, including Data Protection Law (collectively and individually the **"Permitted Purpose"**).

3.2 **Processing Instructions.** The Parties agree that the Agreement (including this DPA), and Customer's use of the Services in accordance with and as described in the Agreement, set out Customer's complete and final processing instructions and any processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Time Doctor. Customer shall ensure its instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate Data Protection Laws.

3.3 **Customer Responsibilities.** Customer is responsible for determining whether the Services are appropriate for the storage and processing of Personal Data under Data Protection Law. Customer further agrees that: (a) it will comply with its obligations under Data Protection Law regarding its use of the Services and the processing of Personal Data; (b) prior to the commencement of the relevant processing, it has provided notice and obtained all consents, permissions and rights necessary for Time Doctor and its Sub-processors to lawfully process Personal Data for the purposes contemplated by the Agreement (including this DPA); and (c) it will notify Time Doctor if it is unable to comply with its obligations under Data Protection Law or its processing instructions will cause Time Doctor or its Sub-processors to be in breach of Data Protection Law.

4. Sub-processors

5. Customer acknowledges and agrees that Time Doctor may engage Sub-processors in order to provide the Services. Customer specifically authorizes the engagement of those Sub-processors listed at https://timedoctor.com/subprocessors.html (or such other successor URL notified to Customer from time to time) ("Sub-processor List"). Time Doctor will restrict Sub-processors' access to Personal Data to what is necessary to assist Time Doctor in providing or maintaining the Services and will remain responsible for any acts or omissions of Sub-processors to the extent they cause Time Doctor to breach its obligations under this DPA. Security

5.1 **Security Measures**. Time Doctor shall implement and maintain appropriate technical and organizational security measures designed to protect Personal Data from Security Incidents and preserve the security and confidentiality of Personal Data, in accordance with the measures described in **Annex B** ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Time Doctor may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

5.2 **Access and Confidentiality.** Time Doctor restricts its personnel from processing Personal Data without authorization and shall ensure that any person who is authorized by Time Doctor to process Personal Data is under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3 **Customer Responsibilities**. Notwithstanding the above, Customer is responsible for reviewing the information made available by Time Doctor relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Law. Customer further agrees that Customer is responsible for its secure

use of the Services, including securing its account authentication credentials and taking any appropriate steps to backup any Personal Data processed in connection with the Services.

5.4 **Security Incidents**. Upon becoming aware of a Security Incident, Time Doctor shall notify Customer without undue delay and, where feasible, within 48 hours. Time Doctor shall provide Customer with timely information relating to the Security Incident as it becomes known or is reasonably requested by Customer to fulfil its obligations under Data Protection Law. Time Doctor will also take reasonable steps to contain, investigate, and mitigate any Security Incident.

6. Audits

6.1 **Security Reports.** Customer acknowledges that Time Doctor is regularly audited against ISO 27001. Upon Customer's written request, Time Doctor will provide Customer with a summary copy of its then-current ISO 27001report ("**Report**"). Time Doctor shall also provide written responses to all reasonable requests made by Customer for information relating to Time Doctor's processing of Personal Data, including responses to information and security audit questionnaires submitted to it by Customer and that are necessary to confirm Time Doctor's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year or when Customer is expressly requested or required to provide this information to a Supervisory Authority.

7. International Transfers

Customer acknowledges and agrees that Time Doctor may transfer and process Personal Data to and in the United States and the other locations in which Time Doctor, its Affiliates or its Sub-processors maintain data processing operations as more particularly described in the Sub-Processor List. Time Doctor shall ensure that such transfers are made in compliance with Data Protection Law and this DPA.

8. Deletion or Return of Personal Data

Upon termination or expiry of the Agreement, at Customer's written request Time Doctor shall delete or return all Personal Data in its possession or control in accordance with the terms of the Agreement and this DPA. This requirement shall not apply to the extent Time Doctor is required by applicable law to retain some or all of the Personal Data, or to Personal Data archived on back-up systems, which data Time Doctor shall securely isolate and protect from any further processing (to the extent permitted by applicable law). The Parties agree that the certification of deletion of Personal Data described in Clause 8.5 and 16.(d) of the EU SCCs shall be provided by Time Doctor to Customer only upon Customer's written request. In the event that no election is made by Customer in accordance with this Section 8, Time Doctor will delete all Personal Data in its possession after 90 days in accordance with Time Doctor's Data Retention and Deletion Protocol https://www.timedoctor.com/data-retention-and-deletion-protocol.

9. Cooperation

9.1 **Data subject requests.** To the extent that Customer is unable to independently access the relevant Personal Data within the Services, Time Doctor shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer in responding to any requests from individuals relating to the processing of Personal Data under the Agreement. In the event that any such request is made to Time Doctor directly, Time Doctor shall promptly notify Customer and shall not respond to the request directly except to direct the data subject to the Customer without Customer's prior authorization, unless and to the extent legally compelled to do so.

9.2 **Law enforcement requests.** If a law enforcement agency sends Time Doctor a demand for Personal Data (for example, through a subpoena or court order), Time Doctor will attempt to

redirect the law enforcement agency to request that Personal Data directly from Customer. As part of this effort, Time Doctor may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Time Doctor will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Time Doctor is legally prohibited from doing so.

9.3 **General cooperation.** Each Party will reasonably cooperate with the other in any activities contemplated by this DPA and to enable each Party to comply with its respective obligations under Data Protection Law.

10. California

10.1 To the extent that Personal Data is subject to the CCPA, Time Doctor agrees that it shall process Personal Data as a service provider and shall not (a) retain, use or disclose Personal Data for any purpose other than the purposes set out in the Agreement and this DPA and as permitted by the CCPA, including retaining, using or disclosing the Personal Data for a commercial purpose other than providing the Services specified in the Agreement; (b) retain, use or disclose the Personal Data outside of the direct business relationship between the Parties, (c) "sell" the Personal Data, as the term "sell" is defined under the CCPA; (d) share the Personal Data, as the term "share" is defined under the CCPA; (e) combine the Personal Data with personal information that Time Doctor receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, except as otherwise permitted under the CPRA.

10.2 Time Doctor, considering the type of Service provided and the processing involved, shall provide commercially reasonable assistance to Customer to (a) carry out risk assessments and cybersecurity audits as required under the CCPA, and (b) to respond to queries, inquiries, complaints or to conduct prior consultations with Supervisory Authorities over compliance with Data Protection Law.

11. Europe

11.1 To the extent that Personal Data is subject to European Data Protection Law, the terms in this Section 11 shall apply in addition to the terms in the remainder of this DPA.

11.2 **Processing Instructions**. Without prejudice to Section 3.3 (Customer Responsibilities), Time Doctor shall notify Customer in writing, unless prohibited from doing so under Data Protection Law, if it becomes aware or believes that any processing instructions from Customer violate European Data Protection Law.

11.3 **Sub-processor Obligations**. Time Doctor shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Personal Data as required by this DPA (to the extent applicable, considering the nature of the services provided by the Sub-processor).

11.4 **Changes to Sub-processors**. Time Doctor will provide ten (10) days' prior notice via updating the Sub-processor List (or such other notification mechanism made available by Time Doctor) if it intends to make any changes to its Sub-processors. Customer may object in writing to Time Doctor's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g., if making Personal Data available to the Sub-processor would violate European Data Protection Law or weaken the protections for Personal Data) by notifying Time Doctor in writing to [privacy@timedoctor.com] within five (5) days of receiving notification from Time Doctor. In such event, the Parties shall discuss Customer's concerns in good faith with a view to achieving a mutually acceptable resolution. If the Parties cannot reach a mutually acceptable resolution, Time Doctor shall, at its sole discretion, either not appoint the Sub-processor, or permit Customer to suspend or terminate the affected Services in accordance with the Agreement without liability to

either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

11.5 **Application of Standard Contractual Clauses**.

The Parties agree that when the transfer of personal data from Customer (as "data exporter") to Time Doctor (as "data importer") is a Restricted Transfer and European Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA, as follows:

(a) the EU SCCs shall apply, completed as follows:

i. Module Two (Controller to Processor) will apply;

ii. in Clause 7, the optional docking clause will not apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 11.4 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA; and

viii. Subject to section 5.3 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA;

(b) **Swiss Transfers**: In relation to transfers of Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA ;

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", " or "Swiss law";

iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

v. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is Swiss Federal Data Protection Information Commissioner;

vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland.; and

viii. with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland,

(c) **UK Transfers**: In relation to transfers of Personal Data that are protected by UK Privacy Laws, the EU SCCs: (i) shall apply as completed in accordance paragraph (a) above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall deemed executed by the parties and incorporated into and form an integral part of this DPA. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex A and B of this DPA and table 4 in Part 1 shall be deemed completed by selecting "neither party".

(d) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

11.6 **Alternative transfer arrangements**. To the extent Time Doctor adopts an alternative lawful data export mechanism for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall upon notice to Customer apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred) and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism.

11.7 **Data Protection Impact Assessments**. To the extent Time Doctor is required under applicable European Data Protection Law, Time Doctor shall provide reasonably requested information regarding Time Doctor's processing of Personal Data under the Agreement to enable Customer to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by law.

12. Limitation of Liability

12.1 Any claim or remedy Customer or its Affiliates may have against Time Doctor, its employees, agents and Sub-processors, arising under or in connection with this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in the Agreement. Accordingly, any reference in the Agreement to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under and in connection with the Agreement and this DPA together.

13. General

13.1 **Conflicts.** Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement and this DPA, this DPA shall control with respect to any terms as they relate to Time Doctor's processing of any Personal Data. Each Party acknowledges that the other Party may disclose the Standard Contractual Clauses, this DPA and any privacy related provisions in the Agreement to any European or US regulator upon request.

Modifications. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Sections 3.2, Time Doctor may periodically make modifications to this DPA where necessary to (i) comply with a request or order by a Supervisory Authority or other government or regulatory entity; (ii) comply with Data Protection Law; or (iii) implement or adhere to new standard contractual clauses, approved codes of conduct or certifications, or other compliance mechanisms, which may be permitted under Data Protection Law. Unless otherwise specified by Time Doctor, these changes will become effective for Customer upon posting of the modified DPA (see "Last Updated" date above). Time Doctor will use reasonable efforts to notify Customer of the changes through Customer's account, email, or other means. In any event, continued use of the Services will constitute Customer's acceptance of the version of the DPA in effect.

13.2 **Severability.** The provisions of this DPA are severable. If any phrase, clause or provision or Annex (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA or the remainder of the Agreement, which shall remain in full force and effect.

13.3 **Governing law and jurisdiction.** This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Law.

Annex A

Description of Data Processing / Transfer

Annex 1(A): List of parties	
Data exporter	**Name of the data exporter**: The entity identified as the Customer in this DPA. **Address:** The address for the Customer associated with its Time Doctor account or otherwise specified in this DPA or the Agreement**.** **Contact person's name, position and contact details**: The contact details associated with Customer's account, or otherwise specified in this DPA or the Agreement. **Activities relevant to the data transferred**: The activities specified in Annex 1(B) below. **Role (Controller/Processor)**: Controller **Signature and date**: See front end of this DPA.
Data importer	**Name of the data importer**: MyStaff LLC t/a Time Doctor **Address:** 1925 Village Center Circle Suite 150, Las Vegas, NV, U.S.A. 89134. **Contact person's name, position and contact details**: DPO contactable at dpo@timedoctor.com **Activities relevant to the data transferred**: The activities specified in Annex 1(B) below. **Role (Controller/Processor)**: Processor **Signature and date**: See front end of this DPA.
Annex 1(B): Description of the processing / transfer	
Categories of Data Subjects whose Personal Data is transferred	Current and former employees and other personnel of the Customer.
Categories of Personal Data transferred	The types of Personal Data processed by Time Doctor are determined and controlled by the Customer in its sole discretion and may include, but is not limited to the following categories of Personal Data: • Contact data (name, title, address, phone number, username, email address, phone number) • Professional data (employer, position, title, performance) • IP address • Geolocation • MAC address • Tasks data (including date when task was created)

	• Worklog data (including time tracked, breaks data, start and end working time).Device data (device name, browser/OS version, device configuration settings) • Device data (desktop screenshots (if enabled), web and app monitoring – application names, website URLs and website titles (if enabled by Customer) • File attachments
Sensitive Data Transferred (if appropriate) and applied Restrictions or Safeguards:	The types of Personal Data processed by Time Doctor are determined and controlled by the Customer in its sole discretion. Time Doctor does not intentionally collect any special categories of data in connection with the Services. Any sensitive data (if any) will be protected in accordance with the Security Measures described in Annex B of this DPA.
Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Personal Data may be transferred on a continuous or one-off basis depending on the Customer's use of the Services and the Customer's processing instructions.
Subject matter of the processing:	The Personal Data described in this Annex A.
Nature of the Processing:	The provision of the Services as described in the Agreement and initiated by the Customer from time to time.
Duration of the Processing:	The duration of the Agreement plus the period from the expiry of the Agreement until deletion of the Personal Data by Customer in accordance with the Agreement.
Purposes of the data transfer and further processing:	The Permitted Purposes (as defined in this DPA)
Period for which the Personal Data will be retained, or if that is not possible the criteria used to determinate that period, if applicable:	The Customer determines the duration of processing in accordance with the Agreement and this DPA.
Annex 1(C): Competent supervisory authority	
Competent supervisory authority	The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

Annex B

Security Measures

Time Doctor shall implement the technical and organizational security measures described in Time Doctor's security policy, the latest version of which is available here: https://www.timedoctor.com/iso-27001.html (or such other URL as may be notified to Customer from time to time).

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymisation and encryption of personal data	Time Doctor encrypts the data with unique encryption keys and pseudonymize the data in order to keep all the personal related data completely protected.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Time Doctor uses encrypted storages, logically separated into multi-tenant infrastructure which gives the organization high level of availability and security
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Time Doctor uses Public and Private cloud multi zone set up which gives the company high availability in a case of infrastructure problems.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Time Doctor performs regular stress, security and performance testing in order to ensure security and high availability.
Measures for user identification and authorisation	Time Doctor software uses unique authentication keys for each user which are generated upon email, password and optional 2 Factor Authentication
Measures for the protection of data during transmission	All the data goes through secured and encrypted communication protocols and the encryption mechanism is regularly reviewed and updated.
Measures for the protection of data during storage	All data is encrypted at rest and key rotation for full encryption is automated in order to avoid any security issues.

Measures for ensuring physical security of locations at which personal data are processed	All DCs are having maximum security and all necessary certifications for information security.
Measures for ensuring events logging	Event logging is managed by multiple services internally in the organization which allows the Time Doctor to collect investigate and manage any event happened in the past.
Measures for ensuring system configuration, including default configuration	Default configuration is overwritten with custom one. Dedicated teams are managing configuration management for the whole infrastructure and it's audited on a regular basis
Measures for internal IT and IT security governance and management	Time Doctor ensures that ISO 27001 related policies are followed as written.
Measures for certification/assurance of processes and products	Time Doctor ensures that ISO 27001 related policies are followed as written.
Measures for ensuring data minimisation	Time Doctor collects only data which is required to perform its own services without collecting any additional data.
Measures for ensuring data quality	Time Doctor has developed data verification services in order to ensure that the data quality is always matching the expected format.
Measures for ensuring limited data retention	Time Doctor's Data Retention and Deletion Protocol is available at https://www.timedoctor.com/data-retention-and-deletion-protocol .
Measures for ensuring accountability	Time Doctor provides public Privacy policy outlining data management and accountability in regards of customer data.
Measures for allowing data portability and ensuring erasure	Time Doctor applies all necessary standards and requirements when transferring data between services including full encryption ,encryption at rest and all protocols for communication being encrypted too. For erasing the data Time Doctor is using a hard delete processes which guarantee that all the data is completely removed.