TimeClock Plus, LLC
Data Processing Addendum

Last Modified: December 26th, 2024

Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Agreement between TimeClock Plus, LLC. ("TCP"), and Client (jointly "the Parties"). Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.

1. Definitions. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.

a. "Agreement" means any agreement between TCP and a specific Client under which Services are provided by TCP to that Client. Such an agreement may have various titles, including but not limited to "Order Form," "Sales Order," or "Terms of Service."
b. "Client" means the entity which determines the purposes and means of Processing of Client Data.
c. "Client Data" means any "personal data" (as defined in GDPR) that is provided by or on behalf of Client and Processed by TCP pursuant to the Agreement.
d. "Data Privacy Framework" means the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded, or replaced.
e. "Data Privacy Framework Principles" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded, or replaced.
f. "Data Protection Laws" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Client Data under the Agreement.
g. "GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.
h. "CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or "CPRA").
i. "Permitted Purpose" means the use of the Client Data to the extent necessary for provision of the Services by TCP to the Client.
"Security Incident" means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Client Data.
j. "Services" means the TCP services that are ordered by the Client from TCP.
j. "Standard Contractual Clauses" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as may be amended, superseded, or replaced.
k. "Sub-processor" means any entity engaged by TCP to Process Client Data in connection with the Services.
l. "Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.
m. Terms such as "Data Subject," "Processing," "Controller," and "Processor" shall have the meaning ascribed to them in the GDPR.
"Third-Party Services" means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.
n. "UK Addendum" means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded, or replaced.
o. "Europe" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.
p. "European Data" means Personal Data that is subject to the protection of European Data Protection Laws.

2. Data Processing; Details of Processing

a. Subject Matter. TCP's provision of the Services to the Client.
b. Nature and Purpose. TCP will process Client Data for the purposes of providing the Services (including administration, operations, technical and Client support), to Client in accordance with the Terms.

c. Data Subjects. Data Subjects include the individuals about whom data is provided to TCP via the Services by or at the direction of the Client. These include:

(i) Natural persons who submit personal data to Client via use of the Services (including employee information and email communication hosted by TCP on behalf of Client) ("Applicants").

(ii) Natural persons who are employees, representatives, or other business contacts of the Client.

d. Categories of Data. Data relating to individuals provided to TCP via the Services, by or at the direction of Client. The Client may submit Client Data to the Services, and may request for its Employees to submit Employee Data to the Services, the extent of which is determined and controlled by the Client in its sole discretion, and which may include, without limitation:

(i) Client Data of all types that may be submitted by Managers to track, report Time and Attendance. Employees of the Client via the Services for the purpose of time and attendance and workforce management information that enables the employee to perform clock operations, access work schedule information. Please refer to TCP's Global Data Privacy Policy to review the categories and types of data and purpose stored/processed in our applications https://www.tcpsoftware.com/privacy

(ii) Client Data of all types that TCP may include in forms hosted on the Services for the Client, or may be requested by Client via customizable fields.

(iii) Contact and billing details of the Client's employees, authorized end users, and other business contacts. For example: name, title, employer, contact information (company, email, phone, address, etc.), payment information, and other account-related data.

(iv) The Client's users who are authorized by the Client to access and use the Services.

e. Roles of the Parties. The Parties acknowledge and agree that TCP will Process the Client Data in the capacity of a Processor and that Client will be the Controller of the Client Data. Client understands that to the extent Third-Party Services are accessed, Client serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of TCP.

f. Client Instructions. The Parties agree this DPA and the Agreement constitute Client's documented instructions regarding TCP's processing of Client Data. TCP will process Client Data only in accordance with these documented instructions.

g. Compliance with Laws. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR and CCPA. TCP is not responsible for determining the requirements of laws applicable to Client's business or that TCP's provision of the Services meet the requirements of such laws.

3. Client's Obligations

a. Instructions. Client shall warrant that the instructions it provides to TCP pursuant to this DPA comply with the Data Protection Laws.

b. Data Subject and Supervisory Authority Requests. The Client shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Client Data, in accordance with Data Protection Laws. To the extent such requests or communications require TCP's assistance, the Client shall notify TCP of the Data Subject or Supervisory Authority request.

c. Notice, Consent and Other Authorizations. Client is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Client is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for TCP to perform the Services.

4. TCP's Obligations

a. Scope of Processing. TCP will Process Client Data on documented instructions from the Client, and in such manner as is necessary for the provision of Services except as required to comply with a legal obligation to which TCP is subject. If TCP believes any documented instruction or additional processing instruction from Client violates the GDPR, CCPA or other Data Protection Laws, TCP will inform Client without undue delay and may suspend the performance of the Services until Client has modified or confirmed the lawfulness of the additional processing instruction in writing. Client acknowledges and agrees that TCP is not responsible for performing legal research or for providing legal advice to Client.

b. Data Subject Requests. If TCP receives a request from any Data Subject made under Data Protection relating to Client Data, TCP will provide a copy of that request to the Client within two (2) business days of receipt. TCP provides Client with tools to enable Client to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. See https://tcpsoftware.com/privacy. To the extent Client is unable to respond to Data Subject's request using these tools, TCP will provide reasonable assistance to the Client in responding to the request.

c. Supervisory Authority Requests. TCP will assist Client in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Client Data.

d. Retention. TCP will retain Client Data only for as long as the Client deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA (up to 45 days), or upon Client's written request, TCP will either anonymize/destroy or return the Client Data to the Client, unless legal obligations require storage of the Client Data.

e. Disclosure to Third Parties and Confidentiality.

(i) TCP will not disclose the Client Data to third parties except as permitted by this DPA or the Agreement, unless TCP is required to disclose the Client Data by applicable laws, in which case TCP shall (to the extent permitted by law) notify the Client in writing and liaise with the Client before complying with such disclosure request.

(ii) TCP treats all Client Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Client Data to commit themselves to confidentiality, and not Process the Client Data for any other purposes, except on instructions from Client.

f. Assistance. Taking into account the nature of the Processing and the information available, TCP will provide assistance to Client in complying with its obligations under CCPA and GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, TCP will provide Client a list of processing operations.

g. Security. TCP will implement and maintain appropriate technical and organizational measures to protect Client Data from Client Data Breaches. TCP will keep Client Data confidential and implement and maintain administrative, physical, technical, and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Client Data transmitted, stored, or otherwise Processed), confidentiality and integrity of Client Data as detailed in Annex 1.

5. Contracting with Sub-Processors

a. General Consent. Client agrees that TCP may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Client Data, TCP will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Client Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. TCP will provide copies of any Sub-processor agreements to Client pursuant only upon reasonable request by Client.

b. Current Sub-processor List. Client acknowledges and agrees that TCP may engage its current Sub-processors listed in **Annex 3** below**,** "Sub-Processors".

c. Written Notice Via This DPA. When necessary, during the course of business, TCP will update this DPA to serve as notice to our clients ("Annex 3 "Sub-Processors") of the addition of any new Sub-processor to the Sub-processor List at any time during the term of the Agreement.

d. Client Objection. If Client has a reasonable basis to object to TCP's use of a new Sub-processor, Client will notify TCP promptly in writing. TCP will use reasonable efforts to make available to Client a change in the affected Services or recommend a commercially reasonable change to Client's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Client. If TCP is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Client may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to TCP.

e. Responsibility. TCP will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause TCP to breach any of TCP's obligations under this DPA.

6. Security Incident Management

a. Notification. TCP shall, to the extent permitted by law, notify Client without undue delay, but no later than 72 hours after becoming aware of any Security Incident.

b. Security Incident. TCP's notification of a Security Incident to the Client to the extent known should include: (i) the nature of the incident; (ii) the date and time upon which the incident took place and was discovered; (iii) the number of data subjects affected by the incident; (iv) the categories of Client Data involved; (v) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (vi) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (vii) the name and contact details of the data protection officer or other contact; and (viii) a description of the likely consequences of the incident. The Client alone may notify any public authority.

7. Data Transfers

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed by TCP, Inc. in the United States and to other jurisdictions where TimeClock Plus, LLC. Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

8. THIRD PARTY CERTIFICATIONS AND AUDITS

a. SOC2 Type 2 Report. In addition to the information contained in this DPA, upon written Client's request, and subject to the confidentiality obligations set forth under a signed NDA, TCP will make available an independent third party ("Auditor") SOC 2 report under AICPA's Trust Principles of Security, Availability, Confidentiality, and Processing Integrity, so that Client can reasonably verify TCP's compliance with its obligations under this DPA.

b. Audits. To the extent the reports provided in Section 8.a do not verify TCP's compliance with its obligations under this DPA, Client may request to audit TCP's compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to TCP. Before the commencement of any such on-site audit, Client must submit a detailed proposed audit plan to TCP at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and state date of the audit. TCP will review the proposed audit plan and provide Client with any concerns or questions. TCP will work cooperatively with Client to agree on a final audit plan. The results of the inspection and all information reviewed during such inspection will be deemed TCP's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions noted above. Notwithstanding any other terms, the Auditor may only disclose to the Client specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to Client any of the records or information reviewed during the inspection.

9. Additional Provisions for European Data

a. Scope. This 'Additional Provisions for European Data' section will apply only with respect to European Data.
b. Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that Client is the Controller of European Data and TCP is the Processor.
c. Instructions. If we believe that Client Instruction infringes European Data Protection Laws (where applicable), we will inform Clients without delay.
d. Transfer Mechanisms for Data Transfers.

(i) TCP will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) (a) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including the Data Privacy Framework; (b) to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws; or (c) to a recipient that has executed the Standard Contractual Clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(ii) Client acknowledge that in connection with the performance of the Subscription Services, TCP is a recipient of European Data in the United States. To the extent that TCP, Inc. receives European Data in the United States, TCP will comply with the following:

(a) Data Privacy Framework (DPF). TCP will use the Data Privacy Framework to lawfully receive European Data in the United States as well as UK Extension to the EU-U.S. Data Privacy Framework and ensure that it provides at least the same level of protection to such European Data as is required by the Data Privacy Framework Principles and will let Client know if it is unable to comply with this requirement. DPF can now receive personal data transferred from the United Kingdom and Gibraltar to the United States in reliance on the UK Extension to the EU-U.S. DPF.

(b) Standard Contractual Clauses. If European Data Protection Laws require that appropriate safeguards are put in place (for example, if the Data Privacy Framework does not cover the transfer to TCP and/or the Data Privacy Framework is invalidated), the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:

(1) In relation to European Data that is subject to the GDPR [i] Client is the "data exporter" and TCP. is the "data importer"; [ii] the Module Two terms apply to the extent the Client is a Controller of European Data and the Module Three terms apply to the extent the Client is a Processor of European Data; [iii] in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the 'Sub-Processors' section of this DPA; [iv] The parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be determined in accordance with the 'Contracting Entity; Applicable Law; Notice' section of the Jurisdiction Specific Terms or, if such section does not specify an EU Member State; [v] the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; [vi] the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR; and [vii] if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA the Standard Contractual Clauses will prevail to the extent of such conflict.

(2) In relation to European Data that is subject to the UK GDPR, UK Extension to the EU-U.S. Data Privacy Framework will first apply and/or UK Extension to the EU-U.S. DPF is invalidated, the Standard Contractual Clauses will take place in accordance with sub-section (1) and the following modifications [i] the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; [ii] Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "neither party"; and [iii] any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(3) In relation to European Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with sub-section (1) and the following modifications [i] references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; [ii] references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and [iii] references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

(4) Client agrees that by complying with our obligations under the 'Sub-Processors' section of this DPA, TCP, Inc. fulfills its obligations under Section 9 of the Standard Contractual Clauses. For the purposes of Clause 9(c) of the Standard Contractual Clauses, Client acknowledges that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can. Client also acknowledges and agrees that you will exercise your audit rights under Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the measures described in the 'THIRD PARTY CERTIFICATIONS AND AUDITS' section of this DPA.

(5) Where the TCP contracting entity under the Agreement is not TCP, such contracting entity will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by TCP, and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity. If TCP cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses or UK Addendum (as applicable) for any reason, and you intend to suspend the transfer of European Data to TCP or terminate the Standard Contractual Clauses ,or UK Addendum, you agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If we have not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Subscription Service in accordance with the Agreement without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).

(iii) Alternative Transfer Mechanism. In the event that TCP is required to adopt an alternative transfer mechanism for European Data, in addition to or other than the mechanisms described in sub-section (ii) above, such alternative transfer mechanism will apply automatically instead of the mechanisms described in this DPA (but only to the extent such alternative transfer mechanism complies with European Data Protection Laws), and you agree to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.

10. Additional Provisions for California Personal Information

a. Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.
b. Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business, and we are a Service Provider for the purposes of the CCPA.
c. Responsibilities. We certify that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Subscription Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA. Further, we certify we (i) will not Sell or Share California Personal Information; (ii) will not Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; and (iii) will not combine the California Personal Information included in Client Data with personal information that we collect or receive from another source (other than information we receive from another source in connection with our obligations as a Service Provider under the Agreement).
d. Compliance. We will (i) comply with obligations applicable to us as a Service Provider under the CCPA and (ii) provide California Personal Information with the same level of privacy protection as is required by the CCPA. We will notify you if we make a determination that we can no longer meet our obligations as a Service Provider under the CCPA.
e. CCPA Audits. You will have the right to take reasonable and appropriate steps to help ensure that we use California Personal Information in a manner consistent with Client's obligations under the CCPA. Upon notice, you will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of California Personal Information.
f. Not a Sale. The parties acknowledge and agree that the disclosure of California Personal Information by the Client to TCP does not form part of any monetary or other valuable consideration exchanged between the parties.

11. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Score of processing' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA.
b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.
c. Governing Law. This DPA will be governed by and construed in accordance with the 'Contracting Entity', 'Applicable Law', and 'Notice' sections of the Jurisdiction Specific Terms, unless required otherwise by Data Protection Laws.

12. Parties to this DPA

a. Permitted Affiliates. By signing the Agreement, you enter into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "Client", "you" and "your" will include you and such Permitted Affiliates.
b. Authorization. The legal entity agreeing to this DPA as Client represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. The parties agree that (i) solely the Client entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Client entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Client entity that is the contracting entity is responsible for coordinating all Instructions, authorizations, and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.
d. Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'THIRD PARTY CERTIFICATIONS AND AUDITS' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Client entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

13. Miscellaneous

a. Obligations Post-termination. Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.
b. Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

Annex 1 - Details of Processing

A. List of Parties

Data exporter:

Name: The Client, as defined in the TCP Client Terms of Service (on behalf of itself and Permitted Affiliates)

Address: The Client's address, as set out in the Order Form

Contact person's name, position, and contact details: The Client's contact details, as set out in the Order Form and/or as set out in the Client's TCP's Account

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Client's use of the TCP Subscription Services under the TCP Client Terms of Service

Role (controller/processor): Controller

Data importer:

Name: **TimeClock Plus, LLC ("TCP")**

Address: See as specified in the Data Processing Agreement.

Contact person's name, position, and contact details: See as specified in the Data Processing Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Client's use of the TCP Subscription Services under the TCP Client Terms of Service

Role (controller/processor): Processor

B. Description of Transfer

Categories of data subjects whose personal data is transferred

PII (Personal identifiable information)

Categories of personal data transferred

Only full name and email address is necessary for account opening in TCP application.

Sensitive data transferred and applied restrictions or safeguards The parties do not anticipate the transfer of sensitive data

The frequency of the transfer

Data can be transferred in one-off or on a continuous basis. **Nature of the processing**

For Time and Attendance, and Scheduling purposes. **Purpose(s) of the data transfer and further processing**

For Time and Attendance, and Scheduling purposes.

The period for which the personal data will be retained

Client data is held in our systems only while the account is active, and some data is held for longer (e.g. IP addresses of client access, audit logs, invoices…), due to legal requirements. When the account is canceled, clients PII data is held in our application up to 45 days.

C. COMPETENT SUPERVISORY AUTHORITY

TCP has further committed to refer unresolved privacy complaints under the Data Privacy Framework (DPF) Principles to an independent dispute resolution mechanism, the BBB EU DATA PRIVACY FRAMEWORK, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to you.

Annex 2 - Security Policies, Procedures, Controls

TCP currently observe the Security measures described in This Annex 2. All capitalized terms not otherwise defined herein will have the meanings as set forth in the Terms and Conditions on our Legal webpage. For more information on these security measures, please refer to TCP's SOC 2 Type II Report, SOC 3 Report, TCP Security Overview and Penetration Test Summaries. All those documents can be requested from our Compliance team under NDA (compliance@tcpsoftware.com)

TCP implements the following security measures with respect to the Client Data:

1. Access Control of Processing Areas. Processes to prevent unauthorized persons from gaining access to the TCP data processing equipment (namely telephones, database and application servers and related hardware) where the Client Data are processed or used, to include:

a. establishing security areas;

b. protection and restriction of access paths;

c. securing the data processing equipment and personal computers;

d. establishing access authorization for employees and third parties, including respective authorization;

e. all access to the data centers where Client Data are hosted is logged, monitored, and tracked; and

f. the data centers where Client Data are hosted is secured by a security alarm system, and other appropriate security measures.

2. Access Control to Data Processing Systems. Processes to prevent TCP data processing systems from being used by unauthorized persons, to include:

a. identification of the terminal and/or the terminal user to the data processor systems;

b. automatic time-out of user terminal if left idle, identification and password required to reopen;

c. regular examination of security risks by internal personnel and qualified third-parties;

d. issuing and safeguarding of identification codes;

e. password complexity requirements (minimum length, expiry of passwords, etc.); and

f. protection against external access by means of firewall and network access controls.

3. Access Control to Use Specific Areas of Data Processing Systems. Measures to ensure that persons entitled to use TCP data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Client Data cannot be read, copied or modified or removed without authorization, to include by:

a. implementing binding employee policies and providing training in respect of each employee's access rights to the Client Data;

b. assignment of unique user identifiers with permissions appropriate to the role;

c. effective and measured disciplinary action against individuals who access Personal Data without authorization;

d. release of data to only authorized persons; and

e. policies controlling the retention of back-up copies.

4. Transmission Control. Procedures to prevent Client Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Client Data by means of data transmission facilities is envisaged, to include:

a. use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;

b. implementation of encrypted connections to safeguard the connection to TCP systems;

c. constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and

d. monitoring of the completeness and correctness of the transfer of data (end-to-end check).

e. In-transit: We require HTTPS encryption (TLS1.2 or higher) (also referred to as SSL or TLS) on all login interfaces and on every client subdomain hosted on the TCP product. Our HTTPS implementation uses industry standard algorithms and certificates.
f. At-rest: All data at rest are encrypted with AES-256 encryption. We have implemented all security best practies to ensure that stored data is encrypted at the proper way.
5. Input Control. Measures to ensure that it is possible to check and establish whether and by whom Client Data has been input into data processing systems or removed, to include:

a. authentication of the authorized personnel;

b. protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;

c. Segregation and protection of stored data via database schemas and logical access controls;

d. utilization of user codes (passwords);

e. proof established within data importer's organization of the input authorization; and

f. providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked.
g. Detection. We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal and external systems (Security Operation Center) aggregate log data and alert (24/7/365) appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, IT, Cloud Operations and support personnel, are responsive to known incidents.
h. Response and tracking. We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, IT, Cloud Operations or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Client damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

6. Availability Control. Measures to ensure that Client Data are protected from accidental destruction or loss, to include:

a. automatic failover between sites;

b. infrastructure redundancy; and

c. regular backups performed on database servers.

7. Segregation of Processing. Procedures to ensure that data collected for different purposes can be processed separately, to include:

a. separating data through application security for the appropriate users;

b. storing data, at the database level, in different tables, separated by the module or function they support; and

c. designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately.

Annex 3 – Sub-Processors

To help TCP deliver the Subscription Service, we engage Sub-Processors to assist with our data processing activities.

A list of our Sub-Processors and our purpose for engaging them is located below:

SUB-PROCESSOR NAME	COUNTRY	KEY FUNCTIONS
Amazon Web Services (AWS)	US	IaaS and SaaS provider, for live (production) and development environments, for storing backups, file storage and Lambda functions
Equinix	US	IaaS, PaaS, and SaaS provider, for live (production) and development environments, for storing backups, file storage
Flexential	US	IaaS, PaaS, and SaaS provider, for live (production) and development environments, for storing backups, file storage
Rackspace	US	IaaS, PaaS, and SaaS provider, for live (production) and development environments, for storing backups, file storage
Superb	US	IaaS, PaaS, and SaaS provider, for live (production) and development environments, for storing backups, file storage
Aptum	US	IaaS, PaaS, and SaaS provider, for live (production) and development environments, for storing backups, file storage
Cloudflare	US	Web Application Firewall
Zoom	US	to communicate with clients
Okta	US	Identity management and secure access provider
DUO	US	Identity management and secure access provider
OpenVPN	US	Virtual Private Network (VPN) service provider
Artic Wolf	US	Managed security services and threat hunting
Salesforce	US	to unite our Sales and Support efforts and to improve and simplify communication with our clients and trials
Segment	US	used for better understanding of client journeys across TCP website and application
Gainsight	US	used for gaining better visibility of TCP clients concerns regarding our applications to improve user experience along with proactive engagement
Microsoft O365	US	internal company's mail and document store system
Sentry.io	US	error tracking and application health monitoring
Zuora	US	integrations partner – for billing/payment processing/subscription tracking
Matillion	US	data integration tools used to extract, transform and load data into company's AWS account (Amazon Redshift & S3).

Data Importer TCP (TimeclockPlus, LLC.). (Provider) .

Data Exporter:

_____
Signature

_____
Signature

_____
Name:

_____
Name:

_____
Title/Position:

_____
Title/Position: