TCP Software: Global Data Privacy Policy

As a provider of workforce management solutions, TCP Software ("we," or "us") respects the privacy of our clients and others who use our website, mobile application, products, and services. In connection with providing our services and operating our business and website, we process certain Personal Data, including from our Clients, prospective clients, and, for certain Clients, end-users of our products. We have adopted this Global Data Privacy Policy so that you can learn how we collect, use, and otherwise process your Personal Data.

This Global Data Privacy Policy covers information collected through TCPSoftware.com

This Global Data Privacy Policy, which includes each of the sub-policies identified below, applies to the Personal Data we collect from you, including via your access to and use of the Services and, for Clients, is incorporated into and is subject to the TCP Software Terms of Service, which can be found at: https://www.tcpsoftware.com/legal.

The Global Data Privacy Policy consists of and incorporates each of the following:

- TimeClock Plus, LLC Privacy Policy for All Personal Data Except U.S. Resident Biometric Data
- TimeClock Plus, LLC Privacy Policy for the Processing of Biometric Data from U.S. Residents
- TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland

This Global Data Privacy Policy uses certain defined terms identified in the "Definitions" section at the end of this Global Data Privacy Policy.

TCP Software Privacy Policy for All Personal Data Except U.S. Resident Biometric Data

With the exception of biometric data collected from U.S. residents, which is addressed separately within the Global Data Privacy Policy, this policy explains how TCP processes, uses and discloses all Personal Data it collects, including from Clients, end-users of our products (e.g., Client staff) for those Clients for whom TCP hosts data, prospective clients, and individuals who visit our website.

In this Privacy Policy, you will find information regarding:

- Collection and Sources of Personal Data
    - Personal Data We Receive Directly From You
    - Personal Data We Host on Behalf of Clients
    - Personal Data We Receive From Other Sources
    - Cookies and Tracking Technologies
- Purposes for Processing and Disclosures of Personal Data

Collection and Sources of Personal Data.

Personal Data We Receive Directly From You.

TCP may collect the following categories of Personal Data directly from you:

a. *Client Account Data*. We may collect Personal Data in connection with Client management and account set-up and management, finance, dispute resolution, and for consolidated management and reporting. Client Account Data may include contact information, billing and banking information, Client account preferences and settings, and Client communications concerning the implementation and maintenance of the Services.
b. *Communications Data*. We may collect Personal Data that you provide when you express an interest in obtaining additional information about the Services, have questions or concerns about the Services, use our "Contact Us" or similar features, sign up for our emails or attend an event or webinar, or download certain content. Such information may include contact information such as name, job title, company name, phone number, and email address.
c. *Human Resources Data*. We may collect Personal Data from employees and job applicants, including contact information, social security number, background reports, job history, certain health or dietary information, payroll and banking information, and other Personal Data incident to the employment relationship.
d. *Reputation & Creditworthiness Data*. We may collect Personal Data in connection with performing diligence on our Clients, prospective clients, Service Providers or prospective service providers, and business partners or prospects. This data may include contact details, information concerning business practices, creditworthiness, reputation and business history, and job titles or roles.
e. *Transaction and Payment Data.* When you sign up for events or purchase some or all of the Services, we may require that you provide contact information such as name and address, billing information, such as billing name and address, credit card number, or bank account information.

f. *Visitor Data*. We may collect Personal Data from you when you visit our offices, including your name, who you are visiting, company name, and time and date of arrival and departure.

Personal Data We Host on Behalf of Clients.

TCP processes and stores Personal Data concerning Client staff on behalf of those Clients who have engaged us to do so. In particular, we process the following categories of Personal Data for Clients:

a. *Profile Data.* We may process general demographic data about you that you or your employer enters into the Services. Profile data may include username, password, first name, last name, address, email, phone number, job title, employee ID, taxpayer ID, gender, date or birth, hire date, termination date, language preference, payroll classification, employment classification, pay rates, work schedules, employment contracts, and labor union affiliation.
b. *Service Data*. We may process Personal Data collected from you in connection with using the Services, including clock-in time, clock-out time, clock-in location, clock-out location, leave requests, including vacation, sick, and other third-party defined leave reasons, leave accruals, FMLA cases, and hours worked.
c. *EU Resident Special Category Data*. We may collect certain "special categories" of Personal Data, as identified in the GDPR, from EU residents including photographic images, racial, or ethnic data, biometric data, physical or mental health data, and data concerning religious or other beliefs.

Personal Data We Receive From Other Sources.

We may also receive Personal Data about you from other sources, including:

- Third-party lead providers from whom we have purchased Personal Data. We may combine this information with Personal Data provided by you. This "*Lead Data*" may include business contact data, social media data, and usage data (including web user behavior and IP addresses).
- Consumer reporting agencies or other background investigation or credit check service providers in connection with our collection of Human Resources Data and Reputation and Creditworthiness Data.

Cookies and Tracking Technologies.

When you use the Services, we collect certain information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs and web beacons. For example, when you visit our website, we may place cookies on your computer.

Cookies are small text files that websites send to your computer or other Internet-connected device to uniquely identify your browser or to store information or settings in your browser. Cookies can contain and/or automatically collect information, such as a user identification code or IP address, which a website will use to track the pages and number of times you have visited, allowing us to recognize you when you return. They also help us provide a customized experience and enable us to detect certain kinds of fraud. The data read from these cookies may be linked to Personal Data. In many cases, you can

manage cookie preferences and opt-out of having cookies and other data collection technologies used by adjusting the settings on your browser. All browsers are different, so visit the "help" section of your browser to learn about cookie preferences and other privacy settings that may be available.

Cookies fall into the subcategories below.

a. *Essential Cookies*. Certain cookies are used for specific purposes that are essential to your secure use and navigation of our website. Without them, TCP may not be able to provide core website functions and features to you, and the website would not operate as well as you or TCP would like. These cookies collect and use information such as your server preferences, single-session data and corresponding identifier, web beacons and log files (detailed below), and other credential-related information. For EU individuals, essential cookies also help inform TCP whether you require, or have already been served, an affirmative consent request in connection with the GDPR. Essential cookies include analytics cookies, which provide us data that allows TCP to better understand its users and improve the website based on what we have learned from that data.
b. *Preference Cookies*. Other cookies are used to collect and process information about your preferences and similar choices in connection with the website in order to optimize your browsing. Preference cookies include social media cookies, which collect information about your social media usage and other data you may have provided in connection with such usage (if you access the website through a social media website or mobile application, you may have social media cookies). If you wish to modify or change your social media cookies, please visit and review the settings on your applicable social media account(s).
c. *Advertising Cookies*. To help support the Services and further tailor your experience, TCP uses Google Analytics as a third-party vendor. For information on how Google Analytics uses data, please visit "How Google uses data when you use our partners sites or apps", located at http://bit.ly/2jXZ13Y.

We encourage you to consider keeping your cookies enabled because if you choose to disable the receipt of cookies, you may not be able to use or benefit from certain features of the website, particularly the features that are designed to personalize your experience.

Most web browsers automatically accept cookies, but generally allow users to modify their browser settings to display a warning before accepting a cookie, to accept cookies only from certain websites, and/or to refuse all cookies.

Pixel tags and web beacons are tiny graphic images placed on website pages or in our emails that allow us to determine whether you have performed a specific action. When you access these pages or open or click an email, the pixel tags and web beacons generate a notice of that action. These tools allow us to measure response to our communications and improve our web pages and promotions.

In many cases, the information we collect using cookies and other tools is only used in a non-identifiable way, without reference to Personal Data. For example, we use information we collect about website

users to optimize our websites and to understand website traffic patterns. In some cases, we do associate the information we collect using cookies and other technology with your Personal Data. This policy applies to the information when we associate it with your Personal Data.

Although our website does not currently have a mechanism to recognize the various web browser "Do Not Track" signals, we do offer individuals choices to manage their preferences, as described above. We do expect our third-party adverting partners to use reasonable efforts to respect browser "Do Not Track" signals by not delivering targeted advertisements to website visitors whose browsers have a "Do Not Track" setting enabled. However, we understand that some companies do not have this capability today. To learn more about browser tracking signals and "Do Not Track," please visit http://www.allaboutdnt.org/.

Purposes for Processing and Disclosures of Personal Data.

General Purposes for Processing and Disclosures of Any and All Categories of Personal Data

In general, TCP may use and disclose *any* Personal Data it maintains about you as follows, pursuant to TCP's legitimate business interests and need to comply with law:

- To manage and mitigate risk, including for insurance functions, to ensure the proper functioning of the Services, to maintain the privacy and security of our data (such as through threat detection, disaster recovery and business continuity activities), and to conduct audits or investigations, in which case we may disclose your Personal Data to Service Providers, insurance providers, tax or financial authorities or consultants, and legal advisors;

- As needed to assess and ensure compliance with applicable laws, legal requirements and company policies, to protect our assets (including to license and protect intellectual property) or to investigate or defend against any claims of illegality or wrongdoing (including to obtain legal advice), or in response to a court order or judicial or other government subpoena or warrant, in which case we may disclose your Personal Data to law enforcement, regulators, governmental authorities or other bodies, courts, tax authorities, insurance providers, legal advisors, and mediators;

- In the event TCP undertakes or is involved in or contemplating (e.g., in connection with due diligence) any merger, acquisition, reorganization, sale of assets, bankruptcy, or insolvency event, in which case we may disclose your Personal Data to buyers or purchasers (or potential buyers or purchasers) and their representatives.

Other Purposes for Processing and Disclosures of Specific Categories of Personal Data

In addition to the general purposes for processing and disclosing any category of your Personal Data, the chart below includes other purposes for which we may process specific categories of your Personal Data

and to whom such data is disclosed as well as our legal bases for such processing, consistent with the GDPR.

Personal Data We Receive Directly From You.

Category of Personal Data	**Purpose(s) for Processing**	**Legal Basis for Processing**	**Categories of Third Parties to Whom Personal Data may be Disclosed**
Client Account Data	For account management, to maintain Client relationships and provide the Services, for billing, for quality management and troubleshooting, to develop and expand TCP's products and services, and for research, development, analytics, and business intelligence.	Consent. Performance of a contract.	Service Providers, including those used for website and application development and support, customer relationship management, payment processing and financial services, IT security, support and hosting, and marketing and promotions management.
Communications Data	To initiate or expand a business relationship, to develop or improve upon TCP's products and services, to respond to inquiries, to market TCP's products and services, and for research, development, analytics, and business intelligence.	Consent.	Service Providers, including those used for website and application development and support, customer relationship management, IT security, support and hosting, and marketing and promotions management.
Human Resources Data	Employment, including recruitment and hiring, interviewing, administering payroll, and managing employees and other staff, and to ensure the safety and security of TCP and its staff.	Pursuit of legitimate business interests. Consent. Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services. Consumer Reporting Agencies and other background check or identity verification providers.
Reputation & Creditworthiness Data	For quality management and to enforce company standards and policies and for identity verification and risk	Consent. Performance of a contract.	Service Providers, including those used for customer relationship management, financial services, IT security, support and hosting, and legal

Category of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	management and mitigation, including for audit and insurance functions.	Legal requirement.	advice and other professional services. Consumer Reporting Agencies and other background check or identity verification providers.
Transaction and Payment Data	To process payment required for the Services or events or webinars you have registered to attend, to send transaction-related emails or otherwise communicate with you concerning a transaction, to deliver and provide the Services or conduct events, and to maintain Client relationships.	Consent. Performance of a contract.	Service Providers, including those used for customer relationship management, payment processing and financial services, and IT security, support and hosting.
Visitor Data	To ensure the safety and security of TCP and its staff.	Consent. Vital Interest.	Service Providers, including those used for IT security, support and hosting.

Personal Data We Host on Behalf of Clients.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
Profile Data	To comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients and other entities when instructed by TCP's Clients, including payroll processors, benefits administration providers, and enterprise resource planning vendors. Service Providers, including those used for application development and support and

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
			IT security, support and hosting.
Service Data	To comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients and other entities when instructed by TCP's Clients, including payroll processors, benefits administration providers, and enterprise resource planning vendors. Service Providers, including those used for application development and support and IT security, support and hosting.
EU Resident Special Category Data	*Biometric Data*: Our Clients are contractually obligated to process biometric data only for employment-related purposes. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Consent. Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.
	Photographic images: Our Clients are contractually obligated to process photographic images data only for employment-related purposes. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Consent. Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	Physical or mental health data: Our Clients determine the purpose for which this information is collected. They may wish to process this data to accommodate disabilities and dietary needs and to address emergency health needs. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.
	Racial or ethnic data: Our Clients determine the purpose for which this information is collected. They may wish to process this data to facilitate affirmative action and other inclusion programs. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.
	Religion or beliefs: Our Clients determine the purpose for which this information is collected. They may wish to process this data to meet an individual's specific needs or requests, including dietary requests and to respect religious holidays and other observances. TCP's purpose for processing this data is to comply with our	Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	contractual obligations and provide the Services to our Clients.		

Personal Data We Receive From Other Sources.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
Lead Data	To identify new customers, initiate or expand a business relationship, and create more tailored advertising to provide products and services that may be of interest to you.	Consent. Performance of a contract.	Service Providers, including those used for website and application development and support, customer relationship management, IT support and hosting, data storage, and marketing and promotions management.
Human Resources Data	Employment, including recruitment and hiring, interviewing, administering payroll, and managing employees and other staff, and to ensure the safety and security of TCP and its staff.	Pursuit of legitimate business interests. Consent. Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services.
Reputation & Creditworthiness Data	For quality management and to enforce company standards and policies and for identity verification and risk management and mitigation, including for audit and insurance functions.	Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services.

Cookies and Tracking Technologies.

Pursuant to TCP's legitimate business interests and/or your consent, TCP may use information obtained via Cookies and tracking technologies to personalize and optimize your browsing experience and the Services by:

- Providing you tailored content and ads;
- Enabling social media features;
- Safeguarding against spam and malware;
- Analyzing trends, traffic, and user behavior;
- Administering the website;
- Gathering demographic information about our user base as a whole;
- Tracking web and advertising analytics throughout our website and our affiliate websites;
- Remembering your preferences and voluntarily-submitted information;
- Performing location-related functionalities and analytics;
- Participating in market research; and
- to improve the Services.

TCP may disclose this information to Service Providers, including those used for website and application development and support, IT support, security and hosting, and marketing and promotions management.

Data Sales.

TCP does not and will not sell or rent your Personal Data.

Data Retention.

TCP will only retain your Personal Data for as long as necessary to fulfill the purposes for which it is processed, to comply with applicable Data Protection Laws, or as otherwise required for other legitimate legal purposes. TCP has implemented a Data Retention Policy for all types of Personal Data that TCP processes. Personal Data is generally retained in accordance with the retention schedules defined therein. When the retention period has expired, Personal Data will be securely deleted or destroyed.

Protection of Personal Data.

TCP has implemented and maintains commercially reasonable organizational, technical, and physical controls to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. In each case, TCP will strive to provide security that is proportional to the sensitivity of the Personal Data being protected, with the greatest effort being focused on protecting sensitive Personal Data and other Personal Data whose compromise could result in substantial harm or inconvenience.

Please note that you should also take steps to protect your data. For example, when you register for the Services, choose a strong password, and do not share it with anyone else. TCP will never ask you for your password in an unsolicited phone call or email.

In the event TCP learns of a data security breach, TCP (potentially with the help of others such as third-party forensic investigators, legal counsel, and TCP's insurance provider) shall investigate and document the facts relating thereto, its effects and the remedial actions taken and shall notify you within a reasonable period of time to the extent required by and in accordance with applicable Data Protection Laws.

International Data Transfers.

TCP is headquartered in the United States of America. Your Personal Data may be stored and processed by TCP in the United States and TCP may transfer Personal Data pertaining to individuals located outside of the United States to our affiliates and suppliers in the United States, as permitted by applicable Data Protection Laws. Therefore, your Personal Data may be processed outside the European Economic Area ("EEA"), and in countries which are not subject to an adequacy decision by the European Commission and which may not provide for the same level of data protection as the EEA. In this event, we will ensure that such recipient offers an adequate level of protection, for instance by verifying that the recipient is Data Privacy Framework (DPF) certified (TCP is self-certified - see the TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland below), by entering into standard contractual clauses for the transfer of data as approved by the European Commission (Art. 46 GDPR), or by asking for your prior consent to such transfer.

Your Rights & Choices.

Communication Preferences.

TCP will send direct marketing materials if you have provided opt-in consent or if applicable Data Protection Laws otherwise permit. You have the right to opt-out of these communications. To opt-out of commercial emails, simply click the link labeled "unsubscribe" at the bottom of any email we send you. Additionally, you may opt-in or opt-out of communications by calling us at +1 (325) 223-9500. Please note that if you are currently receiving services from TCP and you have decided to opt-out of promotional emails, this will not impact the messages we send to you for purposes of delivering such services.

Review, Correction, Erasure, and Other Individual Rights.

You have the right to request a copy of the Personal Data maintained by or on behalf of TCP unless otherwise prohibited by applicable Data Protection Laws. If the Personal Data is incorrect, incomplete, or not processed in compliance with applicable Data Protection Laws or this Privacy Policy, you have the

right to have the Personal Data rectified, restricted, or erased (as appropriate) subject to applicable Data Protection Law.

Additionally, you have the right to object to the processing of your Personal Data on the basis of compelling grounds related to your particular situation or in connection with any direct marketing communications. Restrictions may be lifted if they were temporary, based on certain grounds such as a dispute about data accuracy or the lawfulness of processing or if TCP is in the process of reviewing an objection request, and the basis of the restriction has been resolved. You will be notified about the removal of any such restriction via email or mail. In addition, once a restriction has been implemented, processing can only resume if you grant explicit consent or you request to lift the original restriction and there is no conflict with applicable Data Protection Laws.

You may contact us using the contact information provided in the "Contact Us" section below to request access to your data and to exercise any of the other individual rights afforded to you by applicable Data Protection Laws. TCP will receive, investigate, document, and respond to requests as soon as possible and in accordance with applicable Data Protection Laws. In cases where the request cannot be fulfilled by TCP, we will use best efforts to notify any third-party processing relevant data of the required correction and/or erasure.

In some cases, requests to delete data may be denied in accordance with applicable Data Protection Laws, including, for example, when the data is still needed for processing, where you gave consent and did not withdraw consent, where there has been a previous processing objection that has been granted, and where the data was processed lawfully or there is a not a legal requirement to delete the data. TCP may also reject the request if it needs access to the data to comply with a law, defend a legal claim or for research/historic/scientific purposes.

Individuals Located in the EEA.

In addition to the rights stated above and below, you also have the right to data portability, as well as the right to be notified of automated decision-making or profiling related to your Personal Data.

Individuals in the EEA, the UK, and Switzerland

Individuals located in the EEA, the UK, and Switzerland may file a complaint if they believe TCP has violated this policy or applicable Data Protection Law. Please see TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland for additional information concerning how you may file such a complaint. TCP's Data Protection Officer will receive, investigate, and document each complaint and respond within a reasonable timeframe in accordance with applicable Data Protection Laws of the outcome of the investigation. of the outcome of the investigation.

VeraSafe has been appointed as TCP's representative in the European Union for data protection matters, pursuant to Article 27 of the GDPR. VeraSafe can be contacted in addition to TCP, only on matters related

to the processing of Personal Data. To make such an inquiry, please contact VeraSafe using this contact form: https://www.verasafe.com/privacy-services/contact-article-27-representative

Alternatively, VeraSafe can be contacted at:

VeraSafe Ireland Ltd
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

California Residents

If you are a California resident, California's "Shine the Light" law, Civil Code sections 1798.80 – 1798.84, includes provisions for securing and disposing of Personal Data, notifying you of a breach of your Personal Data, and for responding to requests by you asking about the businesses' practices related to disclosing Personal Data to third-parties for the third-parties' direct marketing purposes. TCP complies with California Civil Code sections 1798.80 – 1798.84. TCP does not share your Personal Data with third-parties for the third-parties' direct marketing purposes. For more information about your rights under California's Civil Code sections 1798.80 – 1798.84, please visit https://leginfo.legislature.ca.gov.

Effective January 1, 2020, the CCPA provides California residents with additional rights related to data privacy.

Pursuant to the CCPA, upon making a verifiable request, California residents may:

- request (in a format that is portable and, to the extent technically feasible, in a readily useable format that will allow you to transmit it to another entity) access to the specific pieces and categories of Personal Data that we have collected about you over the past twelve months, the categories of sources of that information, our business or commercial purposes for collecting the information, and the categories of third parties with whom the information was shared;

- submit a request for deletion of Personal Data, subject to certain exceptions, including (without limitation) in the event that we may need to retain Personal Data to complete the transaction for which the Personal Data was collected, detect security incidents or protect against illegal activity, exercise free speech, comply with a legal obligation, or for lawful internal use compatible with the context in which the information was provided by you. If your request is subject to any exception, we may deny your request to delete your data.

Please note that you must verify your identity and request before further action is taken by us. To do so, we may request certain information from you, including a copy of a government-issued ID or other identifier.

To exercise these rights, you may contact us at: DPO@tcpsoftware.com or 1-800-749-8463. You have the right not to be discriminated against for exercising your rights under the CCPA. Consistent with California law, you may designate an authorized agent that is registered with the Secretary of State to make a request on your behalf. In order to designate an authorized agent, please contact us at DPO@tcpsoftware.com. We will require written proof that the person acting as your agent is in fact authorized to act on your behalf.

If you have any questions about this section or whether it applies to you, please contact us at DPO@tcpsoftware.com.

Other Important Information about Our Practices.

Third-Party Content.

This policy only addresses the use and disclosure of information by TCP. Third-party websites, applications, services, goods or advertisements that may be accessible through our website have their own privacy statements and data collection, use and disclosure practices. We encourage you to familiarize yourself with the privacy statements provided by third-parties prior to providing them with information or taking advantage of an offer or promotion. TCP does not control and is not responsible for the content or privacy and data protection practices of third-party websites, applications, services, goods, or advertisements. If you link to or otherwise interact with third-party content, you do so at your own risk. TCP does not endorse, recommend, or make any representations or warranties regarding websites, applications, services, goods, or advertisements that may be linked to or otherwise incorporated into the Services.

Forums, Product Reviews and Other Public Areas.

Our Services, including social media, may provide forums and other public areas where you may communicate with others and publicly post information. Prior to posting in these areas, please read the Third-parties' Terms of Use carefully. The information you post may be accessible to anyone with Internet access, and Personal Data you include in your posting may be read, collected, and used by others. For example, if you post your email address on a forum or in a public area, you may receive unsolicited messages from third parties. Please use caution when posting Personal Data. We do not assert any ownership over your posts and we are not liable for any statements or representations in posts provided by you. You are solely responsible for your posts.

Children.

TCP's Services, related marketing channels and materials are not directed at children. We do not knowingly collect or sell any Personal Data from children under the age of sixteen (16). If you are a parent or guardian and believe your child has provided TCP with Personal Data without your consent,

please contact us by using the information in the “Contact Us” section, below, and we will take necessary steps to remove such Personal Data from our systems.

Changes to this Privacy Policy.

From time to time, we may update this Privacy Policy to reflect new or different privacy practices. Please review our website periodically to check for the latest changes. Under “Last Updated,” you can see the date on which this Privacy Policy was last updated. We will notify you about material changes in the way we treat your information by placing a prominent notice on the website so that you can choose whether to continue using the Services.

Contact Us.

Please contact us if you have questions, comments or other concerns about this policy or about TCP’s data privacy practices or if you wish to exercise any of your rights under this policy or applicable Data Protection Law at Privacy@tcpsoftware.com. You may also reach us via mail at the address below. If you send us a letter, please provide your name, address, email address, and detailed information about your question, comment, request, or complaint. Letters can be sent to:

TimeClock Plus, LLC
Attn: Legal
1 Time Clock Dr.
San Angelo, TX 76904; USA

TimeClock Plus, LLC Privacy Policy for the Processing of Biometric Data from U.S. Residents

Introduction.

Not all TCP products and services utilize biometric authentication, and not all of TCP's biometric products and services require TCP's participation in the collection, storage or use of biometric data. However, in some cases, TCP may provide hosting services for certain biometric data collected by Clients on such Client's behalf. TCP has instituted the following policy related to any U.S. resident biometric data that is collected, processed and/or stored by TCP and that is subject to the requirements of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA"), or any similar law expressly governing the collection, storage, use and/or disclosure of biometric data.

Biometric Information.

The biometric data covered by this policy includes "Biometric Identifiers" as defined by BIPA (i.e., a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and "Biometric Information" as defined by BIPA (i.e., any information, regardless of how it is captured, converted, stored, or shared, based on an individual's Biometric Identifier used to identify an individual). With respect to its own employees, TCP may collect, store and /or use biometric data directly for the purpose of authenticating TCP employees, tracking their time and attendance, and for other human resources-related purposes. TCP will inform any such employees, in writing and prior to collection of biometric data, that biometric data is being collected, stored, and/or used and of the specific purpose(s) and length of time for which it is being collected, stored, and/or used and will obtain a written release regarding the same. At the direction and on behalf of its Clients, TCP may also collect, store and/or use biometric data. Clients may utilize TCP's products and services to collect, store and/or use biometric data solely for employment-related purposes, including tracking of time and attendance, in accordance with this policy and applicable law.

Client's Responsibilities.

Clients must maintain their own data collection, disclosure, retention, and storage policies in compliance with applicable law, including BIPA.

TCP Clients agree that any use of TCP's products and services to collect, store and/or use biometric data shall be in compliance with applicable law. With respect to any and all biometric data collected or controlled by Clients, Clients must (unless Client and TCP are expressly exempted under applicable law):

a. Inform the individual from whom biometric data will be collected, in writing and prior to collecting his or her biometric data, that biometric data is being collected, stored, and/or used;

b. Indicate, in writing, the specific purpose(s) (which may not be other than employment-related purposes) and length of time for which biometric data is being collected, stored, and/or used; and
c. Receive a written release from the individual (or his or her legally authorized representative) authorizing the Client, TCP, and TCP's third-party service providers (who are subject to restrictions no less restrictive than those imposed on TCP herein) to collect, store, and/or use the biometric data and authorizing the Client to disclose such biometric data to TCP and TCP's third-party service providers.

Client must ensure that TCP is immediately notified upon termination or other discontinuation of use of TCP's biometric products or services with respect to an employee or other individual.

Disclosure and Sharing of Biometric Information.

TCP will not sell, lease, trade or otherwise profit from any biometric data that it receives from (i) its Client's employees or (ii) TCP's employees. Biometric data will not be used for any purpose other than as described herein.

TCP will not disclose, redisclose or otherwise disseminate any biometric data to any person or entity other than, with respect to biometric data received from its Clients, the Client and TCP's third party service providers and, with respect to biometric data collected from TCP's own employees, TCP's third party service providers, without/unless:

a. First obtaining the written consent of the individual whose biometric data has been collected (or his or her authorized representative) to the disclosure or redisclosure;
b. Disclosure or redisclosure is required by state or federal law or municipal ordinance; or
c. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule.

TCP will retain biometric data until the initial purpose for collecting or obtaining such biometric data has been satisfied, or within three (3) years of an individual's last interaction with the Client and/or TCP, as applicable, whichever occurs first, at which time TCP will permanently delete such biometric data.

Biometric Data Storage.

TCP will use a reasonable standard of care, consistent with the industry in which TCP operates, to store, transmit and protect from disclosure all biometric data, and shall store, transmit, and protect from disclosure all biometric data in a manner that is the same as or more protective than the manner in which TCP stores, transmits, and protects other confidential or sensitive data that can be used to uniquely identify an individual or an individual's account or property.

Your Rights & Choices.

See the “Your Rights & Choices” section of TCP’s Privacy Policy for All Personal Data Except U.S. Resident Biometric Data for information concerning your rights.

TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland

TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) and the UK Extension to the EU-U.S. DPF with regard to the processing of personal data received from the European Union and the UK (including Gibraltar) in reliance on the EU-U.S. DPF. TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

With respect to personal data received or transferred pursuant to the Data Privacy Framework (DPF), TCP is subject to the regulatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Pursuant to the Data Privacy Framework (DPF), EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also may correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Data Privacy Framework (DPF), should direct their query to Privacy@TimeClockPlus.com. If requested to remove data, we will respond within a reasonable timeframe.

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to Privacy@TimeClockPlus.com.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

TCP's accountability for personal data that it receives in the United States under the Data Privacy Framework (DPF) and subsequently transfers to a third party is described in the Data Privacy Framework (DPF). In particular, TCP remains responsible and liable under the Data Privacy Framework (DPF) Principles if third-party agents that it engages to process the personal data on its behalf do so in a

manner inconsistent with the Principles, unless TCP proves that it is not responsible for the event giving rise to the damage.

In compliance with the Data Privacy Framework (DPF) Principles, TCP commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Data Privacy Framework (DPF). European Union, UK, and Swiss individuals with DPF inquiries or complaints should first contact TCP by email at Privacy@TimeClockPlus.com. TCP's Data Protection Officer will receive, investigate, and document each complaint and respond to the Individual within a reasonable timeframe of the outcome of the investigation.

By Email:
Data Protection Officer
DPO@tcpsoftware.com

By Mail:
TimeClock Plus, LLC
Attn: Data Protection Officer
1 Time Clock Dr.
San Angelo, TX 76904; USA

TCP has further committed to refer unresolved privacy complaints under the Data Privacy Framework (DPF) Principles to an independent dispute resolution mechanism, DATA PRIVACY FRAMEWORK SERVICES, operated in the United States 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.

In compliance with the EU-U.S. Data Privacy Framework (DPF), TCP commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF in the context of the employment relationship. Complaints related to human resources data should not be addressed to the BBB National Programs Dispute Resolution Process.

Contact details for the EU data protection authorities can be found at https://edpb.europa.eu/about-edpb/about-edpb/members_en

If your Data Privacy Framework (DPF) complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Data Privacy Framework (DPF) Annex 1 at https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf

Contact Us.

For more information about TCP's Privacy Policies, including the TCP Privacy Policy for Client Data Processing, please contact the Data Protection Officer at Privacy@tcpsoftware.com.

Definitions

The following definitions apply throughout the Global Data Privacy Policy:

- ***"CCPA"*** means the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §§ 1798.100-199.
- "***Client***" or "***Clients***" means TCP's business customers, each of which purchases some or all of the Services and enters a service agreement with TCP.
- ***"Data Protection Laws"*** means all applicable laws and regulations governing the use, disclosure, storage, and transfer of Personal Data, including the GDPR and CCPA.
- "***GDPR***" means the European General Data Protection Regulation (EU 2016/679).
- "***Personal Data***" means "personal data" as defined by the GDPR and "personal information" as defined by the CCPA and includes any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. For purposes of this Global Data Privacy Policy, Personal Data does not include data that has been de-identified, whether through aggregation or otherwise, in accordance with applicable Data Protection Laws.
- "***Service Providers***" means any third party entity that processes Personal Data on behalf of TCP and to which TCP discloses Personal Data for a business purpose pursuant to a written contract, provided that the contract prohibits such entity from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services identified in such contract. For the avoidance of doubt, with respect to individuals in the European Union, "Service Providers" are equivalent to sub-processors pursuant to Article 28(4) of the GDPR. TCP uses Service Providers for various functions, including website and application development and support, customer relationship management, human resources management, payment processing and financial services, IT support, security and hosting, legal advice and other professional services, and marketing and promotions management.
- "***Services***" means the TimeClock Plus website (www.tcpsoftware.com) as well as any product, media form, media channel, mobile website or mobile application related thereto or otherwise provided by TCP, including: (a) software for time and attendance tracking, employee absence management, and workforce scheduling together with any integrations for payroll management, enterprise resource planning, and human capital management; and (b) related support services.