

# Privacy Statement

This Privacy Statement describes how ePlan Services, Inc. and our parent company, subsidiaries and affiliates transmit, use, share and protect business, financial, and personal information. This statement applies to all information provided, transmitted, or submitted on this website and mobile applications (“Site”). This notice is available on the homepage of this Site and at every login page where personally identifiable information may be requested.

Your privacy, and the privacy of the information provided, is important to us. We use reasonable care to protect data provided by customers or customers’ employees from loss, misuse, unauthorized access, disclosure, alteration and untimely destruction. We do not grant access to personal information about you except as otherwise set forth herein. We do not share or sell personal information provided or transmitted to our site(s) with any third parties for their own marketing purposes.

At times, we will provide you with links to other websites. We encourage our users to be aware when they leave our site, and to read privacy statements regarding personally identifiable information.

## Information and Use

### **What information is provided or transmitted**

We limit the information that customers or customers’ employees provide to ePlan Services, Inc. to the information that we need to administer and improve the Site, to provide our products and services (“Services”) to our customers, and to fulfill any legal and regulatory requirements.

The categories of personal information that we may request that customers or the employees of customers provide includes the following:

- Contact information to allow us to communicate with you
- Employer information, including financial and bank account information, to provide the Services
- Employee information, including social security number, date of birth, financial, bank account, geolocation data, medical and beneficiary information, to provide the Services
- Credit, debit, or cash/payment card information if used, such as for billing
- Credit or debt history regarding your creditworthiness or credit history, with proper disclosures
- Employment history and application information that can be used to determine eligibility for a job opening via our recruiting module

## **How personal information is submitted and/or transmitted**

We do not require you to provide any personal information to have general access to the Site. However, to access or use certain information, features or Services at the Site, you may be required to provide personal information. Personal information is primarily submitted and/or transmitted:

- When you utilize the Services, we obtain from you the information we need to provide the Services
- From applications, forms and other information you provide us on the Site
- When you establish an account, or an account is established for you at the direction of your employer, to receive Services
- From survey responses and/or site registration
- If you provide us with comments or suggestions, request information about our Services, or contact our customer service department via phone, email or other forms of communication
- From consumer and business reporting agencies regarding your creditworthiness or credit history
- From third parties to verify information given to us
- From information you may provide via Social Media. For information regarding safe and productive participation in our social media community, view our [Social Media Guidelines](#)

## **How personal information is used**

We use the information provided on the Site to perform the Services you request. We limit the submission and transmittal of personal customer information that we need to:

- Facilitate customer requested Services, transactions, investments, distributions and benefits
- Provide superior service to our customers
- Comply with legal, reporting and regulatory requirements
- Administer and improve our websites
- Detect fraud or theft to protect our business and customer information
- Contact you with information on Services, new Services or products, or upcoming events
- Facilitate applicant tracking and recruitment

## **Biometrics – Collection, Transmission, Retention and Destruction**

For the purposes of this Policy, “biometrics” may include an individual’s physiological characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Examples of biometrics include, but are not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice

recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted.

In addition, the employees of Paychex customers that use Paychex timekeeping devices may provide an iris, finger or facial scan as part of the timekeeping process, which the technology converts into a mathematical, encrypted algorithm, or template. These templates are sometimes called “biometrics.” For purposes of this Policy, Paychex broadly includes within the term “biometrics” the templates created in the timekeeping process, and even where not required to do so, Paychex complies with all laws related to the use of biometrics. Some details about biometrics:

### **Biometric Collection**

- Biometrics are collected by employers from employees using Paychex’s timekeeping technology.
- Some laws require employers to provide employees with notice of the use of biometrics in timekeeping, and to obtain employee consent.
- Paychex timekeeping devices have “notice and consent” screens that employers can use to provide notice and obtain consent during the enrollment process, or employers can choose to obtain consent from employees through other means. Newer Paychex timekeeping devices require the use of Paychex notice and consent screens.
- If a customer’s employee is using biometrics to record time, Paychex will presume one or more of the above notice and consent processes are being followed at the customer’s worksite.
- Note: Some applications allow the use of a smartphone device, and the device itself collects biometrics for access to the application. The consent process is part of the smartphone, and is controlled by the user/employee. When smartphone devices are used, geolocation information may be provided to the employer to ensure that employees are located at their appropriate work location.

### **Biometric Transmission and Storage**

- Following collection at the employer’s worksite, the resulting templates are stored in the timekeeping device, and are also transmitted for storage on a database hosted by either the customer, Paychex or a third-party web hosting service.
- Paychex requires that reasonable care be used for transmission of biometrics to storage on any Paychex-hosted or third-party database.
- Paychex provides secure transmission and storage for biometrics, which use reasonable standards of care within Paychex’s industry, and which are the same as the manner in which other confidential and sensitive information is transmitted and stored.
- Paychex does not sell, lease, trade, or otherwise profit from biometrics.
- Paychex collects latitude and longitude coordinates from the device as part of the timekeeping process when geolocation services are enabled.

## **Biometric Destruction**

- Biometric templates are and remain the property of the customer/employer, which is responsible for biometric template destruction when the biometric template is no longer needed, or within (1) year from the employer's last contact with an employee, whichever is first.
- When instructed by its customers to destroy biometric templates, Paychex will promptly comply with that request.
- Paychex will destroy the biometric templates of former or inactive customers who fail to destroy such data, within a reasonable time period after Paychex's last interaction with the customer.

## **How aggregated, non-personal information is used**

We may collect general, non-personal, statistical information about the users of the Site and our services to determine information regarding the use of our Site and general information about our customers. We may also group this information to provide general aggregated data, but that aggregated data will not personally identify any customers or visitors to the Site.

## **How cookies are used**

A "cookie" is a piece of data that our Site may provide to your browser while you are at our Site. The information stored in a cookie is used for user convenience purposes, such as reducing repetitive messages, tracking helper tool versions, and retaining user display preferences. If a user rejects the cookie, they will be able to browse the Site but will be unable to use our online application.

ePlan Services, Inc. may use third-party service providers to use cookies, web beacons, and similar technologies to collect, transmit, or receive information from our website and elsewhere on the internet and use that information to provide measurement services and target ads. You can opt-out of this information tracking using a web browser that supports Do Not Track functionality, or by manually opting out via sites like the Digital Advertising Alliance Consumer Choice Page. (<http://www.aboutads.info/choices>)

## **Children under 13 years of age**

This site is not intended for children under 13 years of age. We do not knowingly collect and/or transmit personal information from children under 13 years of age. All dependent data needed for benefits enrollment is customarily provided by the employee/guardian and kept secure as indicated in this Statement.

## **Your California privacy rights**

Under California Civil Code 1798, California residents with an established business relationship can request information about sharing their personal information with third parties for the third parties' direct marketing purposes. If you are a California resident and would like more information, please contact your service provider.

## Parties With Whom Information May Be Shared

Information is shared to facilitate the Services needed in order to properly and efficiently handle duties related to your account. We may share information with:

- Government agencies to fulfill legal, reporting and regulatory requirements
- Attorneys, accountants and auditors
- Credit reporting agencies to supply vendor references on client's behalf
- Our employees, affiliated companies, subsidiaries, agents and third party service vendors to perform Services related to your account, to offer additional Services, perform analysis to determine qualification to receive future services or collect amounts due.
- Banking and brokerage firms to complete payroll processing and securities transactions
- Credit bureaus and similar organizations, law enforcement or government officials. We reserve the right to release information if we are required to do so by law or if, in our business judgment, such disclosure is reasonably necessary to comply with legal process, in a fraud investigation, an audit or examination.

## How to Access and Correct Your Information

Keeping your information accurate and up-to-date is very important. You can review or correct your account information by contacting a customer service representative. If you have an account at the Site, you can make changes to your account information after you login to the Site from your PC or wireless device and use the online tools. Note that some information changes may be done by or have to be done through your employer.

## Security Center

For information about our commitment to protecting the security and integrity of our customers' information, please [refer to the Security Center](#).

## Changes to This Privacy Statement

This statement may be revised from time to time due to legislative changes, changes in technology or our privacy practices or new uses of customer information not previously

disclosed in this Statement. Revisions are effective upon posting and your continued use of this Site will indicate your acceptance of those changes. Please refer to this Statement regularly.

If you have any comments, concerns or questions about this Privacy Statement, please contact your service provider.

Last Updated November 15, 2019