Dayforce Wallet Mobile App

Privacy Statement – United Kingdom (UK)

Last updated: March 27, 2024

Scope

This Privacy Statement describes our general practices relating to the collection, use, and disclosure of the personal data you provide to Dayforce in relation to the Dayforce Wallet Application (the "App") and the data relating to your use of the App.

The Personal Data Dayforce Collects

Dayforce collects personal data directly from you when you download and/or use the App such as:

- When you create an account, we collect your legal name, e-mail address, and mobile phone number, and ask you to create your username and password;
- Your physical address to confirm your identity alongside other information when you contact our customer support center, or to mail you materials;
- Your National Insurance Number (NIN) to prevent fraud or account duplicity;
- When you contact our customer support center, we collect information to authenticate you and voice recordings or chat transcripts for training and quality assurance purposes;
- We may also collect other information you may choose to provide through our interactions;
- Your use of the App and services made available through it.

When you elect to use a card to use in connection with the App (a "Dayforce Card"), Dayforce collects personal data directly from you on behalf of the financial institution partner for the purposes of opening an account and for identity verification, such as:

- your name, physical address, date of birth, mobile phone number, occupation, and National Insurance Number (NIN).

When collecting this information, Dayforce is acting as a data processor for the financial institution. To learn about how they handle personal data, please review their privacy statement made available on their site or through your agreement.

How Personal Data is Used

Dayforce uses personal data to:

- Deliver the services to you, and maintain your App account, including verifying your identity and providing you with support;
- Personalize your experience while using the App;
- Send marketing communications related to the App and ancillary products and services, with your consent; o If you decide you do not want to receive these marketing communications, you can opt-out by clicking the "unsubscribe" link provided at the bottom of every marketing e-mail.
- Send informational communications such as satisfaction surveys and product alerts;
- Improve the App and ancillary products and services;
- Develop new products and services;
- Comply with data protection legislation, information security requirements, and other legal requirements.

How Personal Data is Shared

Financial Institution Partners

We share personal data with our financial institution partners to enable and provide services at your request.

For example, if you request a Dayforce Card we will share your information with our financial institution partner for the purposes of opening up the account and to meet regulatory requirements such as, if applicable, identity verification or, where applicable by law, for tax reporting.

To learn about how they handle personal data, please review their privacy statements made available on their site or through your agreement.

dayforce

Service Providers

We share personal data with companies or individuals that help Dayforce deliver the services or provide Dayforce with services, such as those who help us prepare and distribute communications, to assist and respond to your inquiries, and those who provide ancillary services.

Subsidiaries and Affiliates

We share personal data with subsidiaries and affiliates of Dayforce in support of the uses described above.

Business Transition

In the event that Dayforce, or any portion of our assets, are acquired, sold, or transferred, Dayforce will disclose personal data with the company involved to complete the business transaction.

Law Enforcement

We may report to law enforcement agencies any activities that we reasonably believe to be unlawful, or that we reasonably believe will aid a law enforcement investigation into unlawful activity. In addition, we reserve the right to release your personal data to law enforcement agencies if we determine, in our sole judgment, that either you have violated our policies, or the release of your personal data will protect the rights, property, or safety of Dayforce, or another person.

Legal Process

We may share your personal data with others as required by or permitted by law. This includes sharing your personal data with governmental entities, or third parties in response to subpoenas, court orders, other legal processes, or as we believe is necessary to exercise our legal rights and those of our customers (including where fraudulent behavior is suspected), to defend against legal claims that have been brought against us, or to defend against possible legal claims that we determine in our sole discretion might be brought against us.

How Personal Data is Protected

Dayforce has implemented policies and procedures to protect personal data. Dayforce uses recognized industry-standard security safeguards appropriate to the sensitivity of personal data. Dayforce reviews its security policies and procedures on a regular basis and updates them as needed to maintain their relevance. Dayforce makes reasonable security arrangements to protect personal data from

and against risks, such as loss or theft, as well as unauthorized access, collection, use, disclosure, copying, modification, disposal, and destruction. The methods of protection include physical measures, organizational measures, and technological measures. Dayforce requires all third parties to whom it transfers personal data to maintain adequate safeguards in compliance with applicable laws and standards to protect personal data.

Retention of Personal Data

Dayforce will retain the information we collect from you through the app to open a Wallet account and through your interaction and use of the app for as long as you have a Wallet account and up to 6 (six) years thereafter to comply with legal obligations. In some cases, the retention period may be shorter depending on the type of personal data processed and the purpose for which it was collected. For example, voice recordings or chat transcripts collected during your interaction with our customer support center are retained for no longer than 13 (thirteen) months. We may keep certain information longer than our policies specify in order to comply with legal requirements and for safety and security reasons.

At the end of the retention period, Dayforce will securely delete your personal data. If there is any personal data that we are unable, for technical reasons, to delete entirely from our systems, we will put in place appropriate measures to prevent any further use of such information.

Legal Basis

Dayforce and third parties are required to process your personal data within the confines of permissible purposes under the law, referred to as “legal basis”. The legal basis that we rely on for the lawful handling of your personal data is the performance of a contract between you and Dayforce (e.g. used to allow you to download and register for the Wallet app), the legitimate interest of Dayforce and/or third parties (e.g. used to capture your interactions with our app to improve it), consent (e.g. used for marketing) and legal obligation (e.g. used to report suspected illegal behavior).

International Transfers

Your personal data may be transferred to or accessed by Dayforce and authorized third parties globally. Dayforce complies with laws on the transfer of personal data between countries to keep your data protected. As such, Dayforce uses the Standard Contractual Clauses for the transfer of personal data from the UK to other countries.

How to Exercise Your Rights

You can view and if necessary, update and correct your personal data within the App.

If the processing of your personal information is based on legitimate interests, you have the right to object to the processing on grounds relating to your specific situation. You may also have the right to request to have your personal information deleted or restricted, ask for portability of your personal information, and not be subject to a decision based solely on automated processing. Where the processing of your personal data is based on consent, you have the right to withdraw this consent at any time. This does not affect the lawfulness of the processing based on consent before your withdrawal.

Individuals can submit requests to exercise any of these rights here or by using the information in the "How to Contact Dayforce" section.

Note that, as required by law, we will require you to prove your identity. We may verify your identity by phone call or e-mail. Depending on your request, we will ask for information such as your name and contact information. We may also ask you to provide a signed declaration confirming your identity. In some circumstances, you may designate an authorized agent to submit requests on your behalf. We will require verification that you provided the authorized agent permission to make a request on your behalf.

Individuals can raise concerns or file complaints here. Dayforce will investigate all complaints and take appropriate action to remedy any issues. You may also have the right to complain to the competent supervisory authority. Information about additional rights, when they apply, and the right to complain to the competent supervisory authority can be found at https://ico.org.uk/.

How to Contact Dayforce

Chief Privacy Officer
Dayforce US, Inc.
3311 E. Old Shakopee Road
Bloomington, MN 55425
Telephone: 1-888-975-7674
E-mail: privacy@Dayforce.com

Changes to this Privacy Statement

Dayforce will update this Privacy Statement periodically to reflect changes to our privacy practices. We will provide notice online when we make any material changes to this Privacy Statement.