

## OVERVIEW

**Ceridian is committed to protecting your personal data. As part of this commitment, Ceridian has established a privacy program that demonstrates our due diligence to privacy laws.**



## SCOPE

This notice applies to the collection, use, sharing, disclosure, retention and deletion of personal data of users of our websites, individuals to whom we market directly and of customer's personal data by Ceridian, its affiliates and third-party service providers.

It applies to all personal data in Ceridian's control, whether it is stored and/or processed on Ceridian property or stored and/or processed by a third-party service provider.

If you are an individual whose employer uses a Ceridian application such as human capital management, and your employer has asked you to submit personal data as part of that service, you should review your employer's separate privacy notice.

If you are a business that has a contract with Ceridian you should review that contract for information concerning how Ceridian collects, uses, shares, and secures the personal that it collects from you, or your employees.

## DEFINITIONS

### Controller

The natural or legal person, public authority, agency or other body which alone or jointly determines the purposes and means of the processing of personal data.

### Customer

An organization who has entered into a business relationship with Ceridian to perform a service.

### Individual

The natural person about who information is being processed.

### Personal Data

Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly by piecing information together.

## Processing

Any activity which is performed on personal data or on sets of personal data from collection through use and disposal, including storing and sharing with others.

## Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

## ACCOUNTABILITY

Ceridian, its employees, and contractors take responsibility for personal data in accordance with Ceridian policies and standards. Ceridian's Chief Privacy Officer, Lisa Clapes, is responsible for defining the requirements of this policy and for ensuring compliance with its provisions. The Chief Information Security Officer, Ron Joyal, is responsible for implementing and maintaining appropriate controls and measures to enable compliance. Ceridian trains its employees with respect to its privacy policies and practices including [Ceridian's Ten Privacy Principles](#).

Ceridian acts as a processor when it processes the personal data of its customers, who are the controllers, in products such as Dayforce, PowerPay, etc. Customer personal data is owned by the customer and Ceridian manages the personal data at the direction of its customers.

In some instances, Ceridian acts as a controller, which means that Ceridian owns and controls the personal data that is being processed. Examples include, but are not limited to:

- Collecting and using personal data for direct marketing purposes of customers and prospective customers
- Managing Ceridian's business operations

Ceridian is liable for personal data it processes and for personal data Ceridian provides to third-party service providers for processing. With respect to personal data that has been transferred to a third-party service provider to be processed, contractual requirements are used to provide a comparable level of protection. Ceridian's liability for a third-party's performance of its obligations is set forth in each agreement that Ceridian signs with its Customers, and Ceridian assumes liability for the performance of the services and obligations subcontracted to such third-party service providers, including those related to the protection of personal data.

Our services also involve the transfer of personal data to third parties (for example, banks, retirement program providers and tax agencies) as instructed by our customers. In these cases, Ceridian does not have a direct relationship with the third party and is not liable for the processing of personal data in their possession. These third parties have their own independent obligations with respect to the personal data, usually by operation of law or through contracts with Ceridian's customers.

Our website, our emails, or our application may link to third parties' websites. It is also possible that third parties' websites or emails may link to our website. We are not responsible for the content or the privacy practices employed by third parties and personal data collected

by third parties is not governed by Ceridian's privacy notice. We encourage you to read the privacy policies of these websites before transmitting any personal data to third parties.

## THE PERSONAL DATA WE COLLECT

Personal data is collected by fair and lawful means. Ceridian provides notice as to the purposes for which personal data is collected, used, retained, and disclosed.

In most cases, Ceridian's customers are responsible for notification of purpose and for obtaining appropriate consent when they collect personal data and transfer it to Ceridian. Personal data that is transferred to Ceridian by our customers to be processed shall be deemed to have been collected with appropriate notification. Ceridian assumes no responsibility for obtaining or validating that appropriate consent has been obtained in respect of personal data transferred to Ceridian by organization(s) and/or customers.

Ceridian collects personal data from customers and customers' employees for the purposes of providing, and promoting the services we offer (including initiating, maintaining, enhancing, and terminating the employee-employer relationship), benchmarking and analytics, continuous improvement and development of products, services and software, and for the operation of Ceridian's business, for example, and needed to comply with legal obligations.

Sometimes, other companies may provide us with the contact information of businesses or individuals who they think may be interested in our products or services. We may also collect contact information from publicly available sources.

Relevant information collected as required to deliver requested services may include, for example, the following categories of data:

- Personal details such as name, birth date, national ID number, marital status, etc.
- Contact details such as address, email address, telephone number, etc.
- Payment details, including bank account number
- Details of employment, education and training
- Qualifications, including CV/resume and references
- Authentication Credentials to use the services, such as username, IP address, PC Name, etc.
- Activities performed by customer users in their use of the services

In some cases, Ceridian collects personal data directly from the individual, for example, when individuals visit a Ceridian website. In these cases, Ceridian is responsible for obtaining appropriate consent, except where inappropriate or if the collection is required/permitted by law without consent.

Individuals who seek to vary or withdraw consent that has been obtained by Ceridian directly may do in writing in the manner set out in the "Monitoring and Enforcement" section of this policy. If you decide you do not want to receive commercial emails from Ceridian you can "opt-

out” by clicking on the “unsubscribe” link provided at the bottom of every commercial email or by clicking [here](#). Subject to legal or contractual restrictions, Ceridian shall abide by the withdrawal or variation of consent, and shall advise the individual of the consequences of a change in the scope of consent. In cases where consent has been obtained by the customer, the individual will be referred to the customer.

On our website, we may collect personal data from you in the following ways:

- **By Asking** - We may collect some personal data from you by asking that you provide it to us. For instance, if you fill out an inquiry form we may ask you for your email address or other business contact information in order to access certain promotional materials.
- **Cookies, Web Beacons and Web Server Logs** – see [Ceridian’s Cookie Notice](#).

Unless required by law, Ceridian shall not use or disclose personal data for any purpose other than the purpose for which it was originally collected without first identifying and documenting the new purpose and obtaining the appropriate consent.

## DO NOT TRACK DISCLOSURE

Do Not Track (DNT) is a preference that users can set for their browsers to opt out of the online tracking activities by some websites. Ceridian does not track its customers over time and across third party websites and thus does not respond to Do Not Track (DNT) signals in browsers.

## HOW WE USE PERSONAL DATA

Ceridian may process personal data on a number of lawful bases, some of which include consent, performance of a contract, compliance with a legal obligation, to protect the vital interests of an individual, performance of a task in the public interest or for legitimate interests. We may rely on legitimate interests for a number of reasons including, but not limited to, corporate governance, fraud prevention, network security, direct marketing and monitoring.

Personal data will be processed for the following purposes:

- Performance of services including but not limited to:
  - Employee HR administration, payroll, benefits, work planning and organization
  - Management of employee development plans and performance evaluation of employees
- Benchmarking and analytics
- Marketing
- Providing access to information systems and premises
- Continuous improvement and development of products, services, software and website

- Compliance with data protection legislation, information security requirements and other legal requirements
- Claims management with and between the customer, Ceridian, individuals and/or third parties, including beyond termination of the Agreement for any reason whatsoever
- Management or administration of Ceridian operations
- Fraud prevention

Ceridian may de-identify or anonymize, personal data. Such data is no longer considered personal data and individuals cannot seek to have their information removed from any such data set, nor is consent for further use required.

## **RETENTION AND DISPOSAL**

Ceridian retains personal data only as long as necessary to fulfill the stated purposes or as legally required and thereafter appropriately disposes of such information. When personal data is no longer necessary or relevant for the identified purpose or to fulfill a legal or business requirement, it shall be securely destroyed. Ceridian will either physically or electronically delete the personal data or de-identify it to make it anonymous.

## **ACCESS AND QUALITY**

Unless Ceridian is permitted or required by law to prohibit access, you may view and if necessary, update or correct your personal data by contacting Ceridian in the manner set out in the “Monitoring and Enforcement” section of this notice. We will respond to your request within the time limit set out by the applicable privacy legislation and, if applicable, we will provide you with an estimate of the of the cost to you associated with administering and responding to your request. Ceridian requires sufficient information to authenticate requests for access.

Unless Ceridian is permitted or required by law to prohibit access, and where feasible, Ceridian makes personal data available for review and updating, either directly through the self-service feature in its products, by directing individuals to their employer for access, or through an access request made to established contacts within Ceridian. Where such access is not feasible, Ceridian provides a written explanation to individuals.

In delivering services, Ceridian relies on its customers and its customers’ employees to supply Ceridian with accurate, complete and up-to-date personal data that is relevant to Ceridian’s delivery of the services. Individuals are asked to review their records on a regular basis and make the appropriate updates or notify their employer of errors promptly. Ceridian makes reasonable efforts to maintain the integrity of the personal data within its products as necessary to fulfill the purposes for which the personal data is to be used.

Where Ceridian collects personal data outside of the performance of its services, Ceridian makes reasonable efforts to keep personal data as accurate, complete and up-to-date as is necessary to fulfill the purposes for which the information is to be used. Ceridian provides a means for individuals to update or correct the personal data Ceridian possesses.

## HOW WE SHARE PERSONAL DATA

We may share personal data about you with third parties in certain circumstances including in the following situations:

- **Affiliates** - We may share information with companies that we own or control, that are owned or controlled by us, or that are under common ownership or control.
- **Behavioral Advertisers** - We may participate in behavioral-based advertising. This means that a third party may use technology, such as a cookie on your browser or a web beacon, to identify you on our website so that they can provide advertising about products and services tailored to your interest. That advertising may appear either on our website, or on other websites. If you would like to opt out of receiving behavioral advertising based on your use of this website, you can do so by visiting the [Network Advertising Initiative](#) and the [Digital Advertising Alliance](#).
- **Blogs, Online Postings, and Testimonials** - We may decide to allow users to share comments, postings, testimonials, or other information. If you choose to submit such information to us, the information that you submit may be available generally to the public. Information you provide in these areas may be read, collected, and used by others who access them.
- **Business Transition** - In the event that Ceridian, or any portion of our assets, are acquired, sold, or transferred, Ceridian may disclose personal data with the company involved to complete the business transition.
- **On-line Applications and Tools** - We may offer tools, widgets, or applications on our website, such as search engine functionalities, that are powered by third parties. If you use those applications or tools, any personal data that you provide may be shared with the third party that provides that functionality. The third party's use of that personal data is subject to their privacy notice.
- **Law Enforcement** - We may report to law enforcement agencies any activities that we reasonably believe to be unlawful, or that we reasonably believe may 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 may protect the rights, property, or safety of Ceridian HCM, or another person.
- **Legal Process** - We may share your personal data with others as required by, or permitted by, law. This may include sharing your personal data with governmental entities, or third parties in response to subpoenas, court orders, other legal process, or



as we believe is necessary to exercise our legal rights, 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.

- **Partners** - We may share personal data with other companies that provide products or services that we think may be of interest to you.
- **Service Providers** - We may share personal data with companies or individuals that provide us with services. These services may include, among other things, providing products or services to you on our behalf, creating or maintaining our databases, researching and analyzing the people who request information from us, preparing and distributing communications, or responding to inquiries.
- **Employer Designated Third Parties** – As part of the services Ceridian delivers to employers, Ceridian transfers personal data to third parties such as banks, tax agencies, and benefit providers.

If Ceridian has knowledge that a third party uses or discloses personal data in an unapproved manner, Ceridian takes reasonable steps to prevent or stop the use or disclosure. Ceridian does not sell any personal data to third parties for marketing.

Where applicable, to limit or opt out of the disclosure of personal data, individuals should contact their employer or Ceridian in the manner set out in the “Monitoring and Enforcement” section.

## CROSS BORDER TRANSFER

Ceridian transfers personal data outside of a local jurisdiction only with adequate protections in place and in compliance with applicable laws and standards. Ceridian maintains operations in the United States (US), Canada, Australia, Mauritius and the United Kingdom (UK) and all of its entities process personal data. Ceridian also transfers personal data to other countries as directed by its customers.

For personal data transfers to the US from the European Union (EU), Ceridian complies with the US-EU Privacy Shield Framework regarding the collection, use, retention and disclosure of personal data from the EU and EEA (European Economic Area) to the US. Ceridian certifies its adherence to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, enforcement, and the applicable supplemental principles. To learn more about the Privacy Shield Principles please visit [www.privacyshield.gov](http://www.privacyshield.gov).

Ceridian may utilize the adequacy determinations made by the European Commission to transfer personal data to countries with data protection that is adequate to the EU. Ceridian also utilizes Standard Contractual Clauses (SCCs) for the transfer of personal data from the EU to other countries.

## HOW WE SECURE PERSONAL DATA

Ceridian has implemented policies, procedures and practices to protect personal data. Ceridian protects personal data using recognized industry standard security safeguards appropriate to the sensitivity of the personal data. Ceridian reviews its security policies and procedures on a regular basis and updates them as needed to maintain their relevance. Ceridian makes reasonable security arrangements to protect personal data in its custody or under its control 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.

Ceridian requires all third parties to whom it may transfer personal data to maintain adequate security safeguards in compliance with applicable laws and standards to protect personal data.

## MONITORING AND ENFORCEMENT

Ceridian monitors its compliance with privacy policies and procedures and has processes to address access requests, complaints and disputes. Where appropriate, individuals may request [access](#) and raise concerns or [complaints](#) regarding their personal data with Ceridian. **PLEASE NOTE:** If Ceridian is processing your personal data on behalf of your employer (i.e., one of Ceridian's customers), you must contact your employer directly to submit an access request, concern or complaint.

If an individual files a complaint Ceridian will investigate. It is Ceridian's practice to respond to the individual within 30 days of receiving the complaint. Ceridian will take all appropriate action to remedy any such issues. If the matter cannot be settled, Ceridian agrees to cooperate with the dispute resolution system set forth below.

If individuals feel that their complaint was not satisfied, they may file a formal complaint with the regulatory bodies below.

- In Canada, the Privacy Commissioner of Canada or the Privacy Commissioner in the applicable province

Office of the Privacy Commissioner of Canada  
30 Victoria Street  
Gatineau, Quebec  
K1A 1H3  
Phone: 1-800-282-1376

- In the U.S., the Attorney General in the applicable State
- In the E.U., the United Kingdom's Information Commissioner's Officer or their member state Data Protection Authority.



Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF  
Phone: +44 0303 123 1113  
Email: [casework@ico.org.uk](mailto:casework@ico.org.uk)

To contact the DPAs directly see [http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm)

- In Switzerland, the Swiss Federal Data Protection and Information Commissioner  
Office of the Federal Data Protection and Information Commissioner FDPIC  
CH - 3003 Berne  
Telephone: +41 (0)58 462 43 95  
Telefax: +41 (0)58 465 99 96

Regarding any Privacy Shield complaints, grievances should be filed with the entities in the following order: Ceridian, the applicable EU Data Protection Authority, The Department of Commerce, the Federal Trade Commission (FTC), then the Privacy Shield Panel. The individual may apply to the Privacy Shield Panel to invoke binding arbitration.

Ceridian will conduct periodic assessments to confirm the accuracy of this notice and verify its adherence to [Ceridian's Ten Privacy Principles](#). In addition, Ceridian will deploy internal auditing measures to monitor its compliance and to address all questions or complaints.

## CONTACTING CERIDIAN

For privacy-related questions, comments or concerns, contact Ceridian at:

Chief Privacy Officer  
Ceridian HCM, Inc.  
3311 E. Old Shakopee Road  
Minneapolis, MN 55425  
Telephone: 1-866-975-7674  
[privacy@ceridian.com](mailto:privacy@ceridian.com)

## CHANGES TO THIS POLICY

Ceridian may update this privacy policy to reflect changes to our practices and reserves the right to change its policies at its own discretion without notice.

***Last Updated on July 31, 2018.***