CORPORATE GLOBAL PRIVACY POLICY

U.S. | CANADA | U.K. | MAURITIUS

OVERVIEW

Ceridian is committed to protecting the privacy of our employees, our customers, and their employees. As part of this commitment, Ceridian has established a privacy program that demonstrates our due diligence to privacy laws.

POLICY

1. Scope

Ceridian's global Privacy Policy governs the principles and the practices that Ceridian HCM, Inc. ("Ceridian") will follow in order to adhere to the federal, provincial, state, legislative and regulatory requirements concerning the handling and management of personal information. This policy describes how we collect, use, share and secure personal information processed by Ceridian.

2. Definitions

Customer – A company who has entered into a business relationship with Ceridian for Ceridian to perform a service.

Individual – The person whose data Ceridian has processed, for example, an employee of Ceridian, an employee of a customer, or a person using a Ceridian website, service or tool.

Personal Information – Any data element or combination of data elements that enables the identification of a individual, including, but not limited to, name, address, human resources data, personal health information, government identification such as social security number, name, biometric identifier, home address, driver's license number, credit card number, or account number.

Processed - personal information that is in Ceridian's possession or under its control.

3. Accountability

Ceridian, its employees, and contractors take responsibility for personal information in accordance with Ceridian policies and standards. Ceridian's Chief Privacy Officer is responsible for defining the requirements of this policy and for ensuring compliance with its provisions. The Chief Information Security Officer is responsible for

CERIDIAN Makes Work Life Better™

implementing and maintaining appropriate controls and measures to enable compliance. Ceridian shall make known, upon request, the identity of the Chief Privacy Officer and the Chief Information Security Officer.

Ceridian is accountable for personal information it processes, including personal information that has been transferred to a third party to be processed. Contractual requirements will be used to provide a comparable level of protection while information is being processed by a third party on Ceridian's behalf.

Ceridian trains its employees with respect to its privacy policies and practices.

4. Notice, Choice and Consent

Ceridian provides notice as to the purposes for which personal information is collected, used, retained, and disclosed.

In most cases, customers are responsible for notification of purpose and for obtaining appropriate consent when they collect personal information and personal information 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 data transferred to Ceridian by organization(s)/customers.

In some cases, Ceridian collects personal information directly from the individual for example, when individuals visit a Ceridian website, or when individuals use certain confidential services. In these cases, Ceridian is responsible for obtaining appropriate consent, except where inappropriate or if the collection is required/permitted by law without consent. Where appropriate, Ceridian describes any choices available within the services to individuals and obtains appropriate 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 Enforcement Section of this policy. 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.

Unless required by law, Ceridian shall not use or disclose personal information 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.

Once data has been de-identified, aggregated or summarized it shall no longer be considered personal information, and individuals cannot seek to have their information removed from an aggregated data set, nor is consent for further use required.

5. Collection and Use

Ceridian does not collect data indiscriminately. Ceridian collects personal information only for the purposes of providing and promoting the services we offer and limits use to those purposes, including initiating, maintaining, enhancing, and terminating the employee-employer relationship. Personal information shall be collected by fair and lawful means, and not by misleading or deceiving individuals about the purpose for which information is collected.

Ceridian may also collect personal information from other sources, either with the consent of the individual or where permitted or required by law. Examples of indirect sources of personal information include background checks, employers or personal references.

6. Retention and Disposal

Ceridian retains personal information only as long as necessary to fulfill the stated purposes or as legally required and thereafter appropriately disposes of such information. Ceridian will specify minimum and maximum retention periods for the various records containing personal information.

When personal information 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 erase the personal information or make it anonymous in a non-recoverable manner.

7. Access

Unless Ceridian is permitted or required by law to prohibit access, Ceridian makes personal information available for review and updating, either directly through the self-service feature in its products, by directing individuals to the employer for access, or through an access request made to established contacts within Ceridian.

Where applicable, individuals may contact Ceridian in the manner set out in the “Enforcement” section of this policy. Ceridian responds to requests within the time limit set out by the applicable privacy legislation and, if applicable, provides the individual with an estimate of the cost associated with administering and responding to the request. Ceridian requires sufficient information to authenticate requests for access.

8. Sharing

Ceridian does not use or disclose personal information for purposes other than those for which it is collected, unless required by law.

Ceridian discloses personal information to third parties only to fulfill the purposes for which it is collected. These services may include, among other things, providing products or services to you or your employer on our behalf, creating or maintaining our databases, researching and analyzing the usage and performance of the application, preparing and distributing communications, responding to inquiries, or as part of our process. If Ceridian has knowledge that a third party uses or discloses personal information in an unapproved manner, Ceridian takes reasonable steps to prevent or stop the use or disclosure.

Where applicable, to limit or opt out of the disclosure of personal information, individuals should contact their employer or Ceridian in the manner set out in the Enforcement Section.

When required to provide information in response to a legal enquiry or order and for national security purposes Ceridian exercises reasonable caution to ensure that the order or request is valid and only legally required personal information is disclosed. Under certain circumstances, the law may require that Ceridian not notify individuals whose information has been requested by legal order. If not prohibited and where practical, Ceridian notifies individuals that their information has been subject to a legal inquiry.

Ceridian does not sell any personal information to third parties for marketing or any other commercial purposes.

9. Cross Border Transfer

Ceridian transfers personal information outside of a local jurisdiction only with adequate protections in place and in compliance with applicable laws and standards.

For data transfers to the U.S. from the E.U. Ceridian complies with the U.S.-E.U. and the U.S.-Swiss Safe Harbor Frameworks regarding the collection, use, retention and disclosure of personal information from the E.U., E.E.A., and Switzerland to the U.S., and certifies its adherence to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor Principles please visit http://www.export.gov/safeharbor/.

Although the Safe Harbor framework has been invalidated in the E.U., Ceridian's data protection program continues to protect customer data using the same security and privacy controls as we always have. Additionally, Ceridian has entered into Model Clause Agreements with customers upon request, which are templates approved by the E.U. Data Commissioner to transfer data outside of the E.U.

Ceridian UK has Model Clause Agreements in place with both its U.S. and Mauritius entities that cover the transfer of Ceridian employee data and customer data.

10. Safeguards

Ceridian has implemented policies, procedures and practices to protect personal information.

Ceridian protects personal information using recognized industry standard security safeguards appropriate to the sensitivity of the information. 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 information 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 information as required to perform its services, to maintain adequate security safeguards in compliance with applicable laws and standards to protect personal information.

11. Quality

In delivering services, Ceridian relies on employers and employees to supply Ceridian with accurate, complete and up-to-date information 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 data within its products as necessary to fulfill the purposes for which the information is to be used.

Where Ceridian collects information outside of service delivery, Ceridian makes reasonable efforts to keep personal information 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 information Ceridian possesses.

12. Monitoring and Enforcement

Individuals may raise concerns or complaints regarding their personal information with Ceridian by completing appendix A and submitting it via email to: Privacy@Ceridian.com or by mailing it to the Chief Privacy Officer at Ceridian HCM, Inc. 3311 E. Old Shakopee Road, Minneapolis, MN 55425, Tel: 952-853-8100.

If an individual files a complaint, Ceridian will investigate the matter or suspected failure to comply with this notice or Ceridian's Privacy Principles. 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, free of charge, 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 E.U., the United Kingdom's Information Commissioner's Officer, their member state Data Protection Authority, or the E.U. Data Protection Supervisor.

  The Information Commissioner's Office
  Information Commissioner: Mr. Christopher Graham
  c/o ICO International Team
  Water Lane, Wycliffe House
  Wilmslow-Cheshire SK9 5AF
  Phone: +44 1 625 54 5 246
  Email: International.Team@ico.org.uk

CERIDIAN Makes Work Life Better™

To contact the DPAs directly see 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

- In the U.S., the Attorney General in the applicable state

Ceridian will conduct periodic assessments to confirm the accuracy of this policy and verify its adherence to Ceridian's Privacy Principles. In addition, Ceridian will deploy internal auditing measures to monitor its compliance with the Principles and to address all questions or complaints.

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.