

Centiro Solutions Inc. - Data Privacy Framework Policy

Date: 2024-05-02

Version 1.1

Revisions

VERSION	CHANGE DESCRIPTION	RESPONSIBLE	DATE
1.0	Document created	Data Protection Officer, Legal Counsel & Compliance Officer	2024-02-09
1.1	Section 2.8 updated to include referenses to UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints. Clarifications made in 2.1.3 and 2.1.4 regarding what types of personal data is collected and the purpose.	Data Protection Officer, Legal Counsel & Compliance Officer	2024-05-02

Table of Contents

1. INTRODUCTION	3
2. Principles	3
2.1 Notice and information	3
2.1.1 Participation	3
2.1.2 Commitment.....	3
2.1.3 Types of Personal Data Collected	3
2.1.4 Purposes of Collection and Use	4
2.1.5 Third-Party Disclosures.....	4
2.2 Choice	4
2.3 Accountability for Onward Transfer	5
2.4 Security	5
2.5 Data Integrity and Purpose Limitation	5
2.6 Access	5
2.7 Inquiries or complaints	6
2.8 Recourse, Enforcement and Liability	6
3. Definitions.....	6

1. INTRODUCTION

Centiro cares about your privacy and protecting the personal data processed by us. All personal data is processed in accordance with applicable data protection legislation.

This Policy describes Centiro Solutions Inc.'s compliance obligations under the Principles of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S Data Privacy Framework.

Centiro Solutions Inc. ("Centiro") is a company within Centiro Group AB (Sweden), providing cloud services for managing flows of goods in e-commerce, logistics and industry, including expert services and consultant and support services, in this Policy collectively referred to as the "Cloud Services". In its course of providing the Cloud Services, Centiro is processing, or may process, EU/EEA, UK and Swiss Personal Data:

- On behalf of our Customers;
- In relation to internal human resources support services

2. Principles

2.1 Notice and information

2.1.1 Participation

Centiro participates in the EU-U.S. Data Privacy Framework- the UK Extension to the EU-U.S. Data Privacy Framework- and the Swiss-U.S Data Privacy Framework Programs. To learn more about the Data Privacy Framework Program and to view Centiro's certification, please visit the U.S. Department of Commerce's Data Privacy Framework Program website at: <https://www.dataprivacyframework.gov/>

2.1.2 Commitment

Centiro commits to apply the Principles on Personal Data received from the EU/EEA, UK and Switzerland, in reliance on the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S Data Privacy Framework.

Centiro acknowledges that the above Frameworks, formed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration, provides U.S. organizations with reliable mechanisms for Personal Data transfers to the United States from the EU/EEA, UK and Switzerland, ensuring the protection of Personal Data is consistent with EU/EEA, UK, and Swiss law.

2.1.3 Types of Personal Data Collected

Centiro hosts and processes Customer Data within the Centiro Group's Cloud Services, including any Personal Data contained therein in the capacity of Processor, at the direction of, and pursuant to, the instructions of Centiro's Customers (Controllers). The following categories of personal data may be subject to processing by Centiro hereunder, depending on solution setup and always subject to compliance with applicable legislation: Name, Address, E-mail, Fax, Phone number, Photo, Signature, Geo coordinates and Customer identification number

In addition, as Controller, Centiro collects general information about our Customers, for billing and contracting purposes. The following categories of personal data may be subject to processing by Centiro hereunder: Name, IP address, E-mail, Phone number and Title.

As Controller, Centiro also collects internal human resources Personal Data about our employees (past or present) in the context of the employment relationship. The following categories of personal data may be subject to processing by Centiro hereunder: Name, Phone number, Social security number and Financial information.

2.1.4 Purposes of Collection and Use

Centiro may use Personal Data submitted by our Customers and their Users as necessary to provide the Cloud Services, including updating, enhancing, securing, and maintaining the Cloud Services according to Centiro's contractual obligations to its Customers. Centiro also obtains general information in connection with providing the Services and maintaining Centiro's relationships with our Customers. The internal human resources Personal Data collected is processed to fulfill the requirements of employments.

2.1.5 Third-Party Disclosures

Centiro may disclose internal human resources Personal Data, and Personal Data that our Customers and Users provide to our Cloud Services:

- to our subsidiaries and affiliates,
- to contractors, business partners and service providers we use to support our Cloud Services,
- in the event Centiro sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution, or liquidation), in which case Personal Data held by us about our Customers will be among the assets transferred to the buyer or acquirer,
- if required to do so by law or legal process, and
- in response to lawful requests from public authorities, including to meet national security, public interest, or law enforcement requirements.

2.2 Choice

In accordance with the Principles, Centiro will offer Customers and employees an opportunity to opt out if their Personal Data is to be disclosed to a third party unless their rights are preserved through written agreement.

Centiro will also offer Customers and employees an opportunity to opt out if their Personal Data is to be used for other purposes than for which it was originally collected or subsequently authorized by the Customer or employee.

Centiro may disclose Personal Data of Customers and employees without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors that Centiro has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. Centiro also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a

portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution, or liquidation).

2.3 Accountability for Onward Transfer

Centiro complies with the Principles regarding accountability for onward transfers. Centiro remains liable under the Principles if its onward transfer recipients process Personal Data in a manner inconsistent with the Principles, unless Centiro proves that it was not responsible for the event giving rise to the damage.

2.4 Security

Centiro maintains appropriate administrative, physical, and technical security measures to protect Personal Data within the Cloud Services, in compliance with ISO/IEC 27001 standard framework (or other equivalent framework).

2.5 Data Integrity and Purpose Limitation

Centiro limits the Processing of Personal Data only to information that is relevant for the purposes of Processing. Centiro Processes Personal Data only for the specified, explicit and legitimate purpose for which it was originally collected. To the extent necessary for such purposes, Centiro takes reasonable and appropriate measures so that Personal Data is accurate, complete, current and otherwise reliable with regard to its intended use.

Centiro retains Personal Data only for as long as it serves a purpose of Processing, and the Personal Data will only be retained in accordance with our business purposes, and our obligations to comply with legal requirements and in adherence with the Principles.

2.6 Access

Individuals in the EU/EEA, UK and Switzerland generally have the right to access their Personal Data. As a Processor, Centiro does not own or control the Personal Data that we process on behalf of our Customers and do not have a direct relationship with the end-customers whose Personal Data may be processed in connection with providing the Cloud Services. Since each Centiro Customer, in the capacity of Controller, is in control of what Personal Data it collects from its end-customers, how that Personal Data is used and disclosed, and how that information can be changed, Users of the Cloud Services should contact the applicable Customer administrator with any inquiries about how to access or correct Personal Data contained in Customer Data. To the extent an end-customer user would submit an access or correction request to Centiro, we will refer the request to the appropriate Centiro Customer and will support such Customer as needed in responding to any request.

To access or correct any general information Customer has provided, the Customer shall contact their Centiro account representative directly or by using the contact information in section 2.7.

In the capacity of Controller, Centiro is in control of the internal human resources Personal Data collected, and how that Personal Data is used and disclosed, and how that information can be changed. To access or correct any Personal Data an employee has provided, the employee shall contact their Centiro manager directly or through the contact information in section 2.7.

2.7 Inquiries or complaints

If you have any inquiries or complaints about this Policy, our privacy practices, or if you request to update, change, or remove your personal information, contact us at: centiroprivacy@centiro.com or by regular mail addressed to:

Centiro Solutions Inc.
Attn: Privacy
399 Boylston Street
Suite 812, 6th Floor
Boston Massachusetts, 02116 USA

Upon receipt, Centiro will respond within 45 days.

2.8 Recourse, Enforcement and Liability

If your complaint cannot be resolved through Centiro's internal processes, Centiro will cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework DPF to find appropriate remedy. In such cases, please contact your EU DPA (https://edpb.europa.eu/about-edpb/about-edpb/members_en) for more information or to file a complaint. Centiro is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) with respect to the Data Privacy Framework.

An individual may, under certain conditions, invoke binding arbitration. Please visit the U.S. Department of Commerce's Data Privacy Framework Program website <https://www.dataprivacyframework.gov/> for more information on conditions giving rise to binding arbitration.

3. Definitions

For the purposes of this Policy, the following definitions apply:

- **Controller** – means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- **Customer** – means any entity that purchases the Cloud Services.
- **Customer Data** – means the electronic data uploaded into the Cloud Services by or for a Customer or its Users.
- **Data Privacy Framework** – means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S Data Privacy Framework..
- **Personal Data** – means any information relating to an identified or identifiable natural person and is received by Centiro in the U.S. from the EU/EEA, UK and Switzerland in connection with Centiro providing the Cloud Services.

- **Policy** – means Centiro Solutions Inc. - Data Privacy Framework Policy
- **Principles** – means the EU-U.S. Data Privacy Framework Principles issued by the U.S. Department of Commerce.
- **Processing** – means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
- **Processor** – means any natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of a Controller.
- **User** – means an individual or company authorized by Customer to access and use the Cloud Services