ControlUp Privacy Whitepaper

Last updated: August 2023

Table of Contents

About ControlUp

ControlUp is transforming the way IT professionals manage systems, troubleshoot issues, and help deliver a great user experience. More than 1,500 organizations around the world rely on ControlUp to save time, money, and precious human resources while ensuring business continuity.

The GDPR in a nutshell

The General Data Protection Regulation (GDPR) was established for the protection of European citizens' data. The regulation dictates a set of compliance and security processes for managing personally identifiable information (PII) so that it is not misused. Currently there is no official certification or license required or available for GDPR. Nevertheless, ControlUp has been certified with ISO 27701, ensuring GDPR articles are supported and maintained.

What is ControlUp's take on the GDPR

ControlUp welcomes the positive changes the GDPR brings, such as the increased harmonization and the "privacy by design and privacy by default" approach. Our view is that the GDPR is not only an obligation but also an opportunity to build privacy-friendly products while further fostering customer trust. Our engineering, product, security, and compliance teams work diligently to align our procedures, documentation, contracts, and services to support compliance with GDPR guidelines.

Processing Customer Data

As part of its service offering, ControlUp processes personal data contained in customer data, as defined in the ControlUp EULA and Privacy Policy. During the provision of its services in its platform, ControlUp acts as the 'processor' - acting on controller instructions - while the customer is the 'controller' who determines the purposes of the processing.

What is ControlUp doing in order to comply?

This is a high-level summary of what we have done so far:

Data Processing Agreement

ControlUp has published a Data Processing Agreement (DPA) which incorporates the appropriate definitions required by the GDPR. The DPA was drafted in accordance with Article 28 of the GDPR for signature with our customers upon request. All customers using ControlUp services to process personal data that is subject to the GDPR, must implement a DPA with ControlUp to allow both the customer and ControlUp to comply with the GDPR DPA requirements.

Sub-processor Information

As required by the GDPR and other privacy regimes, ControlUp provides customers and users with information about affiliates and trusted third-party vendors engaged as sub-processors of ControlUp solutions and services.

Data Types

There are five types of data collected by ControlUp which are processed through different pipelines and stored in the following locations:

1. User registration information separates into three pipelines:
    - New user management data (collected from customer upon registration to app.controlup.com - ControlUp DEX), is stored in PostgreSQL databases, located in Azure in Frankfurt for European customers, Azure in North Virginia, Canada and Australia for other customers.
    - Legacy Real-Time DX user registration data (collected from the customer upon registration to ControlUp Real-Time DX), is stored in Active Directory databases, located in AWS North Virginia, and AWS Ireland.
    - Legacy Edge DX user registration data (collected from Edge DX standalone), is stored in OpenSearch in each customer's dedicated tenant hosted in Azure in their chosen location. For European customers, these optional locations are: Germany North (Berlin), West Europe (Amsterdam), Sweden Central (Galve), France Central (Paris) and Switzerland North (Zurich).
2. User settings and configuration data separates into three pipelines:
    - New configuration service data of the ControlUp

Solve application, is stored in PostgreSQL databases, located in AWS in Frankfurt and Ireland for European customers or in AWS in North Virginia for other customers.

- Legacy configuration service of the ControlUp Real-Time DX application is stored in LDS databases, located in AWS Ireland for European customers and in AWS North Virginia for other customers.
- Edge DX user settings and configuration are stored in OpenSearch in each customer's dedicated tenant hosted in Azure in their chosen location. For European customers, these locations are: Germany North (Berlin), West Europe (Amsterdam), Sweden Central (Galve), France Central (Paris) and Switzerland North (Zurich).

3. Customer data telemetry which includes all the performance metrics and system information, separates into two pipelines:
    - New streaming data pipeline is stored in SQL databases located in Azure in Frankfurt for European customers, Azure in North Virginia US, Canada and Australia for other customers.
    - Legacy data pipeline (ControlUp Insights) is stored in SQL databases, located in AWS in Frankfurt for European customers, and in AWS in North Virginia for other customers.

4. System incidents information, such as event logs and errors

including user-configured and "out of the box" incident triggers. This data type is stored in MSSQL databases located in AWS Ireland.

5. System auditing information separates into two pipelines:
   - Legacy audit log information is stored in Graylog in AWS Ireland and US.
   - New DEX audit log information is stored in secured databases in the selectable region in Azure in EU or US.

Data Storage and Cross-Border Data Transfers

Currently, ControlUp stores collected data across multiple regions:

1. ControlUp Real-Time DX, ControlUp Solve and ControlUp Insights:
   - AWS East US (N. Virginia) – This site stores end user data, as detailed in our Privacy Policy and DPA, of the following data types:
     - ControlUp Real-Time DX legacy user registration information.
     - ControlUp Real-Time DX general settings and configuration data.
     - ControlUp Insights customer data telemetry for customers outside EMEA.
     - ControlUp Real-Time DX Audit data.
   - AWS Europe (Ireland) – This site stores end-user data, as detailed in our Privacy Policy and DPA, of the

following data types:

- ControlUp Real-Time DX legacy user registration information.
- ControlUp Real-Time DX configuration and setting data.
- ControlUp Real-Time DX System incidents data.
- ControlUp Real-Time DX Audit data.

- AWS Europe (Frankfurt) – This site stores end user data, as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp Insights customer data telemetry for customers in EMEA.

2. ControlUp Edge DX:

- Azure Europe – these sites store end user data, for customers in EEA based on the customer sub region selection as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp Edge DX user registration information.
  - ControlUp Edge DX configuration data.
  - ControlUp Edge DX customer data telemetry.

  The sites are located in the following sub regions: Germany North (Berlin), West Europe (Amsterdam), Sweden Central (Galve), France Central (Paris) and Switzerland North (Zurich).
- Azure Global - these sites store end user data, for all non-EEA customers data based on the customer sub region selection as detailed in our Privacy Policy and

DPA, of the following data types:

- ControlUp Edge DX user registration information.
- ControlUp Edge DX user configuration data.
- ControlUp Edge DX customer data telemetry.

The sites are located in the following sub regions: US East (Virginia), Central US (Iowa), Canada Central (Toronto), UAE North (Dubai) and Central India (Pune).

3. ControlUp DEX:

- Azure Europe – for customers in EEA based on the customer sub region selection as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp DEX user registration information.
  - ControlUp DEX customer data telemetry.
  - ControlUp DEX audit log data.

  The sites are located in the Europe (Amsterdam) region.
- Azure Global - these sites store end user data, for all non-EEA customers data based on the customer sub region selection as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp DEX user registration information.
  - ControlUp DEX customer data telemetry.
  - ControlUp DEX audit log data.

  The sites are located in the following sub regions: US East (Virginia), Canada and Australia.

For more information about AWS data centers:
https://aws.amazon.com/compliance/data-center/

For more information about Azure data centers:
https://azure.microsoft.com/en-us/global-infrastructure

ControlUp relies on standard contractual clauses (GDPR SCCs) to ensure safeguards are enforced when processing and transferring data into or out of the European Union.

The safeguards are a set of strict and broad technical and organizational security measures.

ControlUp invests tremendous efforts to best apply adequate information security measures, to reduce exposure to risks, and to provide availability and stability to its computing infrastructures.

Data Retention

ControlUp Insights is a license based on the retention period of customer data.

Currently there are three tiers:

- Pro - one day of data retention.
- Enterprise - one month of data retention.
- Platinum and Ultimate - one year of data retention.

Data retention periods can be configured according to customer requirements to store customer data for shorter periods.

Retention periods of other data types are determined according to the relevancy of the data to the service ControlUp supplies to the customer, and in accordance with the law.

Data Privacy Management

ControlUp has appointed a Security GRC Manager who works with key internal and external stakeholders to manage our privacy program and answer questions that our prospects, customers, and partners may have about our ongoing compliance efforts.

Security

ControlUp is committed to ensuring that the security and privacy of customer data is protected. To achieve this, we follow our comprehensive data security program, which is guided by an in-depth defense philosophy which includes both privacy by design and privacy by default practices.

ControlUp follows the best international industry standards as well as our own best practices developed in-house, to stay ahead of the increasing number of threats facing all service providers today. ControlUp maintains appropriate technical and organizational measures to secure customer data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access, as described in the ControlUp Security White Paper.

Disclaimer:

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their

processing of personal data.