ControlUp GDPR Whitepaper

Last updated: July 2022

Table of Contents

About ControlUp 3
The GDPR in a nutshell 3
What is ControlUp's take on the GDPR 3
Processing Customer Data 4
Sub-processor Information 4
Data Types 5
Data Storage and Cross-Border Data Transfers 6
Data Privacy Officer 9
Security 9

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 certification or license required or available for GDPR.

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 four types of data collected by ControlUp which are processed through the pipelines and stored in different databases:

- User registration information which the customer sends upon registration to ControlUp services (usually IT administrators and Help desk personnel). This data type is stored in Active Directory databases, located in AWS Frankfurt, AWS North Virginia, and AWS Ireland.
- User general settings and configurations of the Real-Time application. This data type is stored in PostgreSQL databases, located in AWS Ireland for European customers and in AWS North Virginia for other customers.
- System incidents 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.
- Customer data telemetry (ControlUp Insights) which includes all the performance metrics and system information. This data type is stored in ControlUp Insights databases, located in AWS Frankfurt for European customers, and in AWS North Virginia for other customers.

Data Storage and Cross-Border Data Transfers

Currently, ControlUp stores collected data across multiple regions:

- 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 user registration information.
  - ControlUp Real-Time DX user general settings and configurations.
  - ControlUp Insights customer data telemetry for customers outside EMEA.
- 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 user registration information.
  - ControlUp Real-Time user general settings and configuration.
  - ControlUp Real-Time DX System incidents.
- 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.

- Azure East US (N. Virginia) – This site stores end-user data, as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp Edge DX user registration information for customers outside EMEA.
  - ControlUp Edge DX user general settings and configurations for customers outside EMEA.
  - ControlUp Edge DX customer data telemetry for customers outside EMEA.
- Azure Europe (Frankfurt) – This site stores end-user data, as detailed in our Privacy Policy and DPA, of the following data types:
  - ControlUp Edge DX user registration information for customers in EMEA.
  - ControlUp Edge DX user general settings and configurations for customers in EMEA.
  - ControlUp Edge DX customer data telemetry for EMEA customers.

ControlUp has taken a step ahead of the GDPR and keeps all the European customers' data telemetry (Insights and Edge DX customer data telemetry) in Frankfurt, Germany.

ControlUp is in the process of completing the move of all European customers' registration, configuration, and incident data to Frankfurt, Germany. The ETA for completion of this process is Q3, 2023.

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 Officer

ControlUp has appointed a Security and Compliance 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.