ControlUp GDPR Statement

Last updated: January 2022

Table of Content

ControlUp GDPR Statement

About ControlUp

ControlUp is transforming the way IT professionals manage systems, troubleshoot issues, and help to deliver a great user experience. More than 1,000 organizations around the worldrely on ControlUp to save time, money, and precious human resources to ensure business continuity.

ControlUp Compliance with GDPR

ControlUp is committed to General Data Protection Regulation (GDPR) compliance. Our engineering, product, security and compliance teams have been working 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 the terms are defined in the ControlUp EULA and Privacy Policy. In this instance, ControlUp acts as the 'processor' - acting on controller instructions - while the customer is the 'controller' who determines the purposes of the processing.

Data Processing Agreement

ControlUp has published a Data Processing Agreement (DPA) that incorporates the appropriate definitions required by the GDPR.

This DPA was created under the supervision of EU privacy experts and is designed to comply with the GDPR and to reflect the specific details of the data processing activities associated with ControlUp's products and services.

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 Storage and Cross-Border Data Transfers

Currently, ControlUp stores collected data across two regions:

- AWS Eastern US (Virginia) – This site currently stores end-user data as detailed in our Privacy Policy and DPA.
- AWS Europe (Frankfurt) – This site is dedicated for the storage of our European customer's end-user data.
- Azure Eastern US (Virginia) – This site is used for storing our Edge DX product's collected data from our American customers.
- Azure Europe (Frankfurt) – This site is used for storing our Edge DX product's collected data from our European customers.

The data collected by ControlUp includes statistics of customer's infrastructure performance metrics[1], updates and system information about hosts, machines, users' sessions and processes.

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 (SCCs) to ensure safeguards are met and complied with when data is transferred across, and into or out of, other countries including the European Union.

[1] Performance metric details of endpoints connected to customer's IT infrastructure such as: IP Location, Geolocation, Wi-Fi SSID, host name, etc.

Data Retention

ControlUp product licenses are based on the retention period of the data.

Currently there are three tiers:

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

Data retention could be configured to store data for shorter periods as per customer requirements.

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 your data is protected. To do so, we have implemented a comprehensive information security program that is guided by a defense in depth philosophy that includes privacy by design and privacy by default practices.

ControlUp follows the best international industry standards and we have also developed our own best practices to stay ahead of the increasing number of threats facing all service providers

today. ControlUp maintains appropriate technical and organizational measures to secure your data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access, as described in the ControlUp Security White Paper.