ControlUp Privacy Whitepaper

Last updated: April 2026

Table of Contents

Contents

Table of Contents 2
About ControlUp 3
The GDPR in a nutshell 3
What is ControlUp's take on the GDPR 3
Processing Customer Data 4
AI Processing and Data Protection 4
What is ControlUp doing to comply? 5
Data Processing Agreement 5
Sub-processor Information 5
Compliance 6
Privacy by design 6
Data Types 6
Data Storage and Cross-Border Data Transfers 8
Data Retention 11
Data Deletion 12
Data Privacy Management 12
Data Subject Rights 12
Data Breach Notification 12
Logging & Monitoring 13
Disclaimer 13

About ControlUp

ControlUp is transforming the way IT professionals manage systems, troubleshoot issues, and help deliver great user experience. More than 2,000 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 SaaS Agreement 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.

AI Processing and Data Protection

ControlUp incorporates artificial intelligence (AI) capabilities within its platform to enhance IT operations, monitoring, and troubleshooting processes.

AI functionality operates under strict data protection and governance controls aligned with GDPR principles:

- **Inference-Only Processing** – AI models are used solely for inference. Customer data is not used for training, fine-tuning or improving underlying models.
- **No Cross-Tenant Data Access** – Customer data is logically segregated and AI processing occurs within the boundaries of the customer's tenant.
- **Data Minimization** – AI processes only the minimum system and performance telemetry required.
- **No Expansion of Data Scope** – AI capabilities do not introduce new categories of personal data beyond those already processed by the platform.
- **Human Oversight** – AI outputs are advisory in nature. Action-based recommendations require human review and authorization.

ControlUp maintains appropriate technical and organizational measures to ensure that AI processing complies with applicable data protection laws and does not alter the role of ControlUp as a data processor acting on customer instructions.

For additional details regarding AI governance, security controls, and data handling practices, please refer to the ControlUp AI Security Whitepaper.

What is ControlUp doing 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.

Compliance

ControlUp maintains compliance with recognized industry frameworks, including ISO 27001, ISO 27701, and SOC 2 Type II, which support its alignment with GDPR requirements.

Privacy by design

Implementation of privacy by design and by default principles across product development and data processing activities.

Data Types

ControlUp follows the principle of data minimization and collects only the data necessary to provide its services. Customers may configure data collection settings according to their requirements.

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, is separated 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 for VDI & DaaS:
   - 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 Real-Time DX System incidents data.
- 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 Audit data.

2. ControlUp for Desktops (CU4D):

- 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:
  - CU4D user registration information.
  - CU4D configuration data.
  - CU4D 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 in the following sub regions:

US East (Virginia), Central US (Iowa), Canada Central (Toronto), UAE North (Dubai) and Central India (Pune).

3. ControlUp ONE:

- 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 ONE user registration information.
  - ControlUp ONE customer data telemetry.
  - ControlUp ONE audit log data.

  The sites are located in 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 ONE user registration information.
  - ControlUp ONE customer data telemetry.
  - ControlUp ONE 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) and, where applicable, the EU-U.S. Data Privacy Framework (DPF) to ensure appropriate safeguards are in place when processing and transferring data into or out of the European Union. These safeguards include a comprehensive set of technical and organizational security measures.

ControlUp invests significant efforts to implement and maintain robust information security controls, reduce risk exposure, and ensure the availability and stability of its computing infrastructure.

Data Retention

ControlUp offers two types of licenses:

- Essential - provides one month of data retention.
- Advanced - provides 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 Deletion

Upon termination of the service, customer data is deleted or returned in accordance with applicable contractual agreements, using secure deletion methods aligned with industry standards.

Data Privacy Management

ControlUp has appointed a DPO 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.

Data Subject Rights

ControlUp supports its customers in fulfilling data subject rights requests under GDPR, including access, rectification, erasure, restriction and data portability. As a data processor, ControlUp acts on documented instructions from the data controller and provides reasonable assistance to enable timely response to such requests in accordance with applicable legal requirements.

Data Breach Notification

ControlUp maintains a formal incident response program and notifies customers without undue delay, and no later than 72 hours after becoming aware of a personal data breach, in accordance with GDPR requirements. Notifications include relevant details to support the customer's regulatory obligations.

Logging & Monitoring

ControlUp implements logging and monitoring mechanisms to detect unauthorized access and ensure accountability, while maintaining compliance with data protection and privacy requirements.

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.