DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into as of this ____ day of ____, 2022 forms part of our End User License Agreement (available at https://www.controlup.com/privacy-policy/controlup-eula/) (the "**Agreement**"). You acknowledge that you, on your own behalf as an individual and on behalf of [_____] incorporated under _____ law, with its principal offices located at _____ ("**Organization**") (collectively, **"You", "Your", "Customer", or "Data Controller"**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with **ControlUp** as defined below (**"ControlUp "**, **"Us"**, **"We", "Our", "Service Provider" or "Data Processor"**) to reflect the parties' agreement with regard to the Processing of Personal Data (as such terms are defined below) of European individuals. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

WHEREAS, ControlUp shall provide services of performance monitoring, troubleshooting, analytics and management of multiple types of IT infrastructures (collectively, the "**Services**") for Customer, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, we may process Personal Data on your behalf, in the capacity of a "**Data Processor**"; and the Parties wish to set forth the arrangements concerning the processing of Personal Data within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA. References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated. Words used in the singular include the plural and vice versa, as the context may require. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.2 Definitions:

(a) **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and ControlUp, but has not signed its own agreement with ControlUp and is not a "**Customer**" as defined under the Agreement.

(c) **"Controller" or "Data Controller"** means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include yourself, the Organization and/or the Organization's Authorized Affiliates.

(d) **"Member State"** means a country that belongs to the European Union and/or the European Economic Area. "Union" means the European Union.

(e) "**ControlUp Group**" means ControlUp and its Affiliates engaged in the Processing of Personal Data.

(f) **"Data Protection Laws and Regulations"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their Member States and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

(g) **"Data Subject"** means the identified or identifiable person to whom the Personal Data relates.

(h) "**ControlUp"** means the relevant ControlUp entity of the following ControlUp legal entities: ControlUp Technologies Ltd., and/or ControlUp Inc. and/or ControlUp GmbH.

(i) "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(j) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(k) **"Process(ing)"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(l) **"Processor" or "Data Processor"** means the entity which Processes Personal Data on behalf of the Controller.

(m) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via https://support.controlup.com/docs/controlup-architecture-security-concepts?highlight=archit , or as otherwise made reasonably available by ControlUp.

(n) **"Sub-processor"** means any Processor engaged by ControlUp.

(o) "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Customer is the Data Controller, (ii) ControlUp is the Data Processor and that (iii) ControlUp or members of the ControlUp Group may engage Sub-processors pursuant to the requirements set forth in Section 5 "**Sub-processors**" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and comply at all times with the obligations applicable to data controllers (including, without limitation, Article 24 of the GDPR). For the avoidance of doubt, Customer's instructions for the Processing of

Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data. Without limitation, Customer shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal bases in order to collect, Process and transfer to Data Processor the Personal Data and to authorize the Processing by Data Processor of the Personal Data which is authorized in this DPA. Customer shall defend, hold harmless and indemnify ControlUp, its Affiliates and subsidiaries (including without limitation their directors, officers, agents, subcontractors and/or employees) from and against any liability of any kind related to any breach, violation or infringement by Customer and/or its authorized users of any Data Protection Laws and Regulations and/or this DPA and/or this Section.

2.3 Data Processor's Processing of Personal Data.

2.3.1 Subject to the Agreement, Data Processor shall Process Personal Data in accordance with Customer's documented instructions as necessary for the performance of the Services and for the performance of the Agreement and this DPA, unless required to otherwise by Union or Member State law or any other applicable law to which Data Processor is subject, in which case, Data Processor shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The duration of the Processing, the nature and purposes of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

2.3.2 To the extent that Data Processor cannot comply with a request (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind) from Customer and/or its authorized users relating to Processing of Personal Data or where Data Processor considers such a request to be unlawful, Data Processor (i) shall inform Customer, providing relevant details of the problem, (ii) Data Processor may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Data Processor all the amounts owed to Data Processor or due before the date of termination. Customer will have no further claims against Data Processor (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).

2.3.3 ControlUp will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of ControlUp, to the extent that such is a result of Customer's instructions.

2.3.4 If Customer provides ControlUp or any of the entities of the ControlUp Group with instructions, requests, suggestions, comments or feedback (whether orally or in writing) with respect to the Services, Customer acknowledges that any and all rights, including intellectual property rights, therein shall belong exclusively to ControlUp and that such shall be considered ControlUp's intellectual property without restrictions or limitations of any kind, and Customer hereby irrevocably and fully transfers and assigns to ControlUp any and all intellectual property rights therein and waives any and all moral rights that Customer may have in respect thereto.

3. RIGHTS OF DATA SUBJECTS. If Data Processor receives a request from receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, right to be informed, erasure (“right to be forgotten”), restriction of Processing, data portability, right to object, or its right not to be subject to automated individual decision making, including profiling (“Data Subject Request”), Data Processor shall, to the extent legally permitted, promptly notify and forward such Data Subject Request to Customer. Considering the nature of the Processing, Data Processor shall use commercially reasonable efforts to assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Data Processor’s provision of such assistance.

4. CONTROLUP PERSONNEL

4.1 Confidentiality**.** Data Processor shall grant access to the Personal Data to persons under its authority (including, without limitation, its personnel) only on a need to know basis and ensure that such persons engaged in the Processing of Personal Data have committed themselves to confidentiality.

4.2 Data Processor may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable Data Protection Laws and Regulations (in such a case, Data Processor shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a “need-to-know” basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s),accountant(s), investors or potential acquirers.

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 List of Current Sub-processors and Notification of New Sub-processors.

5.1.1 Data Processor current list of Sub-processors is included in Schedule 2 ("**Sub-processor List**") and is hereby approved by Data Controller. The Sub-processor List as of the date of execution of this DPA, or as of the date of publication (as applicable), is hereby, or shall be (as applicable), authorized by Customer. In any event, the Sub-processor List shall be deemed authorized by Customer unless it provides a written reasonable objection for reasons related to the GDPR within ten (10) business days following the publication of the Sub-processor List. Customer may reasonably object for reasons related to the GDPR to Data Processor's use of an existing Sub-processor by providing a written objection to privacy@controlup.com. In the event Customer reasonably objects to an existing Sub-processor, as permitted in the preceding sentences, and the parties do not find a solution in good faith to the issue in question, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Customer will have no further claims against Data Processor due to (i) past use of approved Sub-processors prior to the date of objection or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.1.2 At least 7 days before ControlUp engages any new sub-processor, ControlUp will update the Customer by providing a notification of any new Sub-processor(s) in connection with the provision of the Services.

5.2 **Objection Right for New Sub-processors.** Customer may reasonably object to Data Processor's use of a new Sub-processor for reasons related to the GDPR by notifying Data Processor promptly in writing within ten (10) business days after receipt of Data Processor's notice in accordance with the mechanism set out in Section 5.2 and such written objection shall include the reasons related to the GDPR for objecting to Data Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within ten (10) business days following Data Processor's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Data Processor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to new Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Until a decision is made regarding the new Sub-processor, Data Processor may temporarily suspend the Processing of the affected Personal Data. Customer will have no further claims against Data Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.3 **Agreements with Sub-processors**. In accordance with Articles 28.7 and 28.8 of the GDPR, if and when the European Commission lays down the standard contractual clauses referred to in such Article, the Parties may revise this DPA in good faith to adjust it to such standard contractual clauses.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** Taking into account the state of the art, Data Processor shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Documentation which are hereby approved by Customer. Upon the Customer's request, Data Processor will use commercially reasonable efforts to assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing, the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing and the information available to Data Processor.

6.2 **Security Assessments and Audits.** ControlUp audits its compliance against data protection and information security standards on a regular basis. Such audits are conducted by ControlUp's Security Department or by third party auditors engaged by ControlUp. In addition, and upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Data Processor shall make available to Customer that is not a competitor of Data Processor (or Customer's independent, third-party auditor that is not a competitor of Data Processor) a copy of Data Processor's then most recent third-party audits or certifications, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Data Processor's prior written approval and, upon Data Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Data Processor in the context of the audit and/or the certification). At Customer's cost and expense, Data Processor shall allow for and contribute to audits, including inspections, conducted by the controller

or another auditor mandated by Customer (who is not a direct or indirect competitor of Data Processor), provided that the Parties shall agree on the scope, timing and conditions of such audits and inspections. Notwithstanding anything to the contrary, such audits and/or inspections shall not contain any information, including without limitation, personal data that does not belong to Customer.

6.3 **Personal Data Incident Management and Notification**. To the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Data Processor or its Sub-processors of which Data Processor becomes aware (a "Personal Data Incident"). Where, and in so far as, it is not possible to provide the Personal Data Incident at the same time, the Personal Data Incident may be provided in phases without undue further delay. Data Processor shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Data Processor deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Data Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users. In any event, Customer will be the party responsible for notifying supervisory authorities and/or concerned data subjects (where required by Data Protection Laws and Regulations).

7. RETURN AND DELETION OF PERSONAL DATA.

7.1 Subject to the Agreement, Data Processor shall, at the choice of Customer, delete or return the Personal Data to Customer after the end of the provision of the Services relating to processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, Data Processor may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations. If the Customer requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for Data Processor's clients.

8. AUTHORIZED AFFILIATES

8.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Data Processor. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

8.2 **Communication.** The Customer shall remain responsible for coordinating all communication with Data Processor under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9. TRANSFERS OF DATA

9.1 **Transfers to countries that offer adequate level of data protection**: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "**EEA**") to countries that offer adequate level of data

protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

9.2 **Transfers to other countries**: If the Processing of Personal Data includes transfers from the EEA to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the Parties shall comply with Chapter V of the GDPR, including, if necessary, executing the standard data protection clauses adopted by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission or comply with any of the other mechanisms provided for in the GDPR for transferring Personal Data to such Other Countries. To the extent that Customer and Data Processor will use the Standard Contractual Clauses as a mechanism to transfer Customer Personal Data, the rights and obligations of the parties shall be performed in accordance with, and subject to, this DPA.

10. **TERMINATION.** This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.3, 2.3.4 and 12 shall survive the termination or expiration of this DPA for any reason. This DPA cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this DPA shall automatically terminate.

11. RELATIONSHIP WITH AGREEMENT. In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement. Notwithstanding anything to the contrary in the Agreement, this DPA and/or any other agreement between the parties and to the maximum extent permitted : (A) Us and Our Affiliates' entire, total and aggregate liability, related to personal data or information, privacy, or for breach of, this DPA and/or Data Protection Laws and Regulations, including,

without limitation, if any, any indemnification obligation under Agreement or applicable law regarding data protection or privacy shall be limited to the amounts paid to us under the Agreement within twelve (12) months preceding the even that gave rise to the claim. This limitation of liability is cumulative and not per incident; (B) In no event will we and/or our affiliates or their third-party providers, be liable under, or otherwise in connection with this DPA for: (i) any indirect, exemplary, special, consequential, incidental or punitive damages; (ii) any loss of profits, business, or anticipated savings; (iii) any loss of, or damage to data, reputation, revenue or goodwill; and/or (iv) the cost of procuring any substitute goods or services; and (C) The foregoing exclusions and limitations on liability set forth in this Section shall apply: (i) even if we, our Affiliates or third-party providers, have been advised, or should have been aware, of the possibility of losses or damages; (ii) even if any remedy in this DPA fails of its essential purpose; and (iii) regardless of the form, theory or basis of liability (such as, but not limited to, breach of contract or tort).

12. **AMENDMENTS**. This DPA may be amended at any time by a written instrument duly signed by each of the Parties.

13. **LEGAL EFFECT.** This DPA shall only become legally

binding between Customer and Data Processor when the formalities steps set out in the Section "INSTRUCTIONS ON HOW TO EXECUTE THIS DPA" below have been fully completed. Data Processor may assign this DPA or its rights or obligations hereunder to any Affiliate thereof, or to a successor or any Affiliate thereof, in connection with a merger, consolidation or acquisition of all or substantially all of its shares, assets or business relating to this DPA or the Agreement. Any Data Processor obligation hereunder may be performed (in whole or in part), and any Data Processor right (including invoice and payment rights) or remedy may be exercised (in whole or in part), by an Affiliate of Data Processor.

14. SIGNATURE

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the signing person on behalf of Customer, represent and warrant that you have, or you were granted, full authority to bind the Organization and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Organization and/or its Authorized Affiliates, you shall not supply or provide Personal Data to ControlUp.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that ControlUp processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

This DPA has been pre-signed on behalf of ControlUp.

Instructions on how to execute this DPA.

1. To complete this DPA, you must complete the missing information; and
2. Send the completed and signed DPA to us by email, indicating the Customer's legal name and address, to privacy@controlup.com.

List of Schedules

- SCHEDULE 1 - DETAILS OF THE PROCESSING
- SCHEDULE 2 - SUB-PROCESSOR LIST

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER:

Signature:
Customer Legal Name:
Print Name:
Title:
Date:

CONTROLUP TECHNOLOGIES LTD.

Signature:
Legal Name:
Print Name:
Title:
Date:

CONTROLUP INC.

Signature:
Legal Name:
Print Name:
Title:
Date:

CONTROLUP GmbH.

Signature:
Legal Name:
Print Name:
Title:
Date:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Service(s) to Customer and improving the Services and the Software.
2. Setting up an account/account(s) for Customer.
3. Setting up profile(s) for users authorized by Customers.
4. For Customer to be able to use the Services.
5. Performing the Agreement, this DPA and/or other contracts executed by the Parties.
6. Providing support and technical maintenance, if agreed in the Agreement.
7. Enforcing the Agreement, this DPA and/or defending Data Processor's rights.
8. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation; and
9. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
10. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Data Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Types of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

1. In all available operation modes of the Software; Standalone Mode, On-Prem Mode, as well as Hybrid Cloud Mode, we collect User registration information as entered by the user during ControlUp user account creation. Such information includes: Name, email, phone number, company name and password.
2. When Licensee operates the software in an Hybrid Cloud Mode performance related information of Licensee's monitored End Points and Hosts are sent to Our Servers securely as detailed in Section 3 below.
3. Data types sent to Our Servers when working in an Hybrid Cloud Mode:
    3.1. Portions of the Main Console and Monitor contain functions that send data to Our Servers when working in an Enterprise Hybrid Cloud Mode.
    3.2. The Data sent contains:
        3.2.1. User registration information as entered by the user during ControlUp User Account creation. Such information includes: Name, email, phone number, company name for the service.
        3.2.2. General User Account settings and configurations. Such information includes host names, private IP, and:
            3.2.2.1. User selected ControlUp's organization upon logon.
            3.2.2.2. User configured ControlUp's stress settings.

3.2.2.3. User configured ControlUp's security policy settings.

3.2.3. User login information such as login date/time, login count, login private IP address and usage duration.

3.2.4. Generated ID's for ControlUp User Account, organization, and environment.

3.2.5. User's License Information and License usage information.

3.2.6. Static computer information displayed in ControlUp's computers view while remote computer is not connected to ControlUp console.

3.2.7. Remote desktop configuration information (No credential information is ever sent)

3.2.8. Details of system incidents as defined by one of the following. These might include the following Personal Data:

3.2.8.1. Incident triggers configured by the User.

3.2.8.2. Incident triggers configured and updated by ControlUp via ControlUp Cloud Analytics.

3.2.9. Details of IT and Controller's infrastructure performance metrics and system information as follows: Performance updates and system information about hosts, computers, Users sessions and processes.

3.2.10. Details of endpoint connected to Controller's IT infrastructure performance metrics such as: IP Location, Geolocation, Wi-Fi SSID, host name, etc.

3.2.11. Auditing information of actions executed by ControlUp users and any changes in the product configuration such as IP Location, Wi-Fi SSID, host name, etc.

The Customer and the Data Subjects shall provide the Personal Data to Data Processor by supplying the Personal Data to Data Processor's Service.

In some limited circumstances Personal Data may also come from others sources, for example, in the case of anti-money laundering research, fraud detection or as required by applicable law. For clarity, Customer shall always be deemed the "Data Controller" and ControlUp shall always be deemed the "data processor" (as such terms are defined in the GDPR).

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- *Customer's contact information*
- *Customer's users authorized by Customer to use the Services*
- *Customer's users' names, computer host names, Geolocation and IP addresses,*
- *Product Information including device information, Wi-Fi SSID, activity logs, connection data (users' processes and sessions).*

SCHEDULE 2 – SUB-PROCESSOR LIST

Sub Processor	**Location**	**Related ControlUp Services**	**Scope of services provided by the sub-processor**	**Appropriate safeguard if processing takes places in or from a third country**
Amazon Web Services	N. Virginia, United States, Ireland	○ ControlUp Solve ○ ControlUp Insight ○ ControlUp Realtime backend (in case where hybrid cloud deployment mode is used)	Cloud computing services	Standard Contractual Clauses
Amazon Web Services	Frankfurt, Germany	Dedicated for EEA customer's: ○ ControlUp Solve ○ ControlUp Insight ○ ControlUp Realtime backend (in case where hybrid cloud deployment mode is used)		
Amazon Web Services	Frankfurt, Germany	Scoutbees		
Microsoft Azure	N. Virginia, United States	ControlUp Edge DX		
Microsoft Azure	Frankfurt, Germany	ControlUp Edge DX		