DATA PROTECTION APPENDIX

When performing services defined in the service agreement, we are acting as a processor in terms of Art. 28 GDPR and process personal data on behalf of our customers.

1. Scope of processing

1.1. The processing on behalf of the customer shall include the following products or services:
A1 Digital IoT Platform powered by Cumulocity IoT.

1.2. The following categories of data may be processed on a regular basis:

- ☒ Master Data
- ☒ Personal Identifiers
- ☒ Sensitive Data
- ☒ Personalized Marketing and Sales Data
- ☒ Roles and Associations
- ☒ Customer Inventory
- ☒ Customer Interaction
- ☒ Traffic Data
- ☒ Geolocation Data
- ☒ Content Data
- ☒ Financial Data
- ☒ Login Data

1.3. Categories of data subjects concerned by the processing of personal data:

- ☒ Client of the customer – natural Person
- ☒ Client of the customer - legal Person
- ☒ Employee of the customer
- ☒ Authorized user of Enterprise Customer
- ☒ Vulnerable natural persons/Children
- ☒ Supplier, Business partner, Prospect or other contract partner of the customer

2. List of appointed subprocessors

Name	Adresse	Type of processing	Place of processing
Software AG	Uhlandstraße 12, 64297 Darmstadt, Germany	Support	Germany
Akenes SA (Exoscale)	Boulevard de Grancy 19A 1006 – Lausanne Switzerland	Hosting	Austria or Germany or Switzerland

3. Technical and Organisational Measures

As processor, we apply security measures to ensure an appropriate level of protection in accordance with Art. 28 para. 3 lit. c, 32 GDPR and Art. 5 para. 1, para. 2 GDPR. Technical and organisational measures ensure an appropriate level of protection with respect to risk for confidentiality, integrity, availability and resilience of the systems.
Unless otherwise specified in the performance agreement, it is the responsibility of the processor to ensure the appropriate level of protection for the respective processing, in particular by a combination of the technical and organisational measures. The processor shall apply security measures based on current practice, implementation costs and the type, scope and purpose of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons. The processor shall be permitted to implement alternative measures, if the safety level of such measures is not lower than measures listed below.

A. CONFIDENTIALITY (ARTICLE 32 PARAGRAPH 1 POINT B GDPR)

- **Physical Access Control:** Protection against unauthorised access to data processing systems, e.g. by magnetic or chip cards, keys, electric door openers, factory security or gatekeepers, alarm systems, video systems.

- **Electronic Access control:** Protection against unauthorized system use by e.g. (secure) passwords, automatic blocking mechanisms, two-factor authentication, encryption of data carriers.

- **Internal Access control:** No unauthorised reading, copying, modification or removal within the system through, e.g. authorization concepts and demand-oriented access rights, logging of accesses.

- **Separation control:** Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing.

- **Pseudonymisation:** If possible for the respective data processing, the primary identification features of the personal data are removed in the respective data processing and stored separately.

- **Classification scheme for data:** Due to legal obligations or self-assessment (secret/confidential/internal/public).

B. INTEGRITY (ARTICLE 32 PARAGRAPH 1 POINT B GDPR)

- **Data Transfer Control**: No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- **Data Entry Control**: Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

C. AVAILABILITY AND RESILIENCE (ARTICLE 32 PARAGRAPH 1 POINT B GDPR)

- **Availability Control**: Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning;

- **Rapid recovery**

D. PROCEDURES FOR REGULAR TESTING, ASSESSMENT AND EVALUATION (ARTICLE 32 PARAGRAPH 1 POINT D GDPR; ARTICLE 25 PARAGRAPH 1 GDPR)

- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
- No third party data processing as per Article 28 GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.