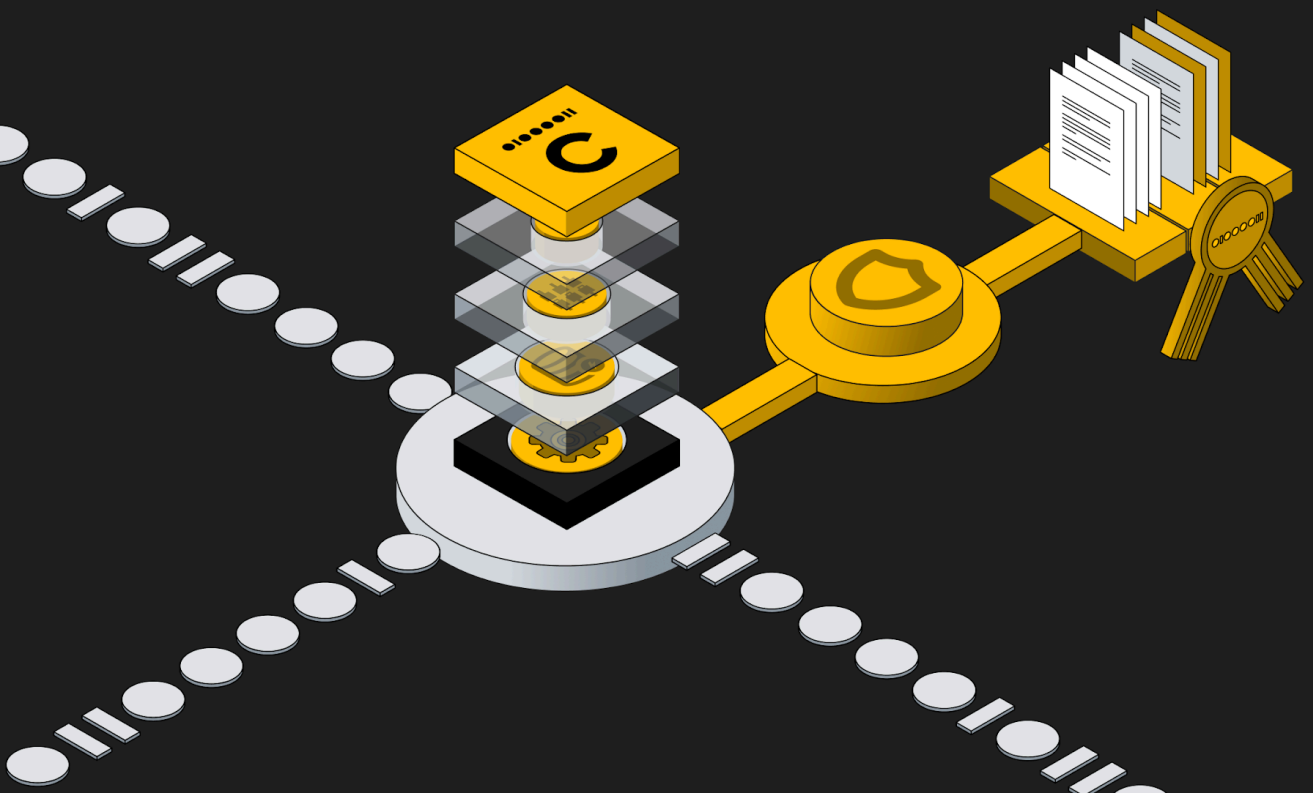
CUMULOCITY

General Technical & Organisational Security Measures

Cloud Services



Owner: Jane Porter (Data Protection Officer)
Date effective: 01/01/2025

TABLE OF CONTENTS

As of the Data Processing Agreement Effective Date Processor 's entity set out in the relevant Cloud Services Order Form as the entity delivering the Cloud Services is certified under ISO/IEC 27001 and agrees to maintain an information security program for the services that comply with the ISO/IEC 27001 standards or such other alternative standards as are substantially equivalent to ISO/IEC 27001 for the establishment, implementation, control and improvement of the Software GmbH Cloud Services Security Standards.

1. Confidentiality (ART 32 PARA. 1 LIT B GDPR)

1. **Access Control of Processing Areas**: Processor shall implement suitable measures to prevent unauthorized persons from gaining access to the data processing equipment where the personal data is processed. This is accomplished through the following measures:
    a. Access to premises is controlled by security guards, access cards and (electronic) door locks.
    b. Access privileges to premises is only granted to those employees and contractors who have a legitimate business need for such access. When an employee or contractor no longer has a business need for the access privileges assigned, the access privileges are promptly revoked.
    c. The data centers where personal data is hosted are secured by appropriate security measures. Data centers operated by Processor are located in the highest security zone according to the Physical Access Policy. Data centers of service providers guarantee adequate safeguards to grant access to premises only to authorized staff.
    d. The Cloud Services Infrastructure as a Service sub-processor (IaaS Supplier), identified in the Cloud Services Order Form, maintains physical access control over the Cloud Services data processing equipment. Independent external audits review the respective physical security mechanisms of the IaaS Supplier regarding ISO/IEC 27001 compliance.
    e. Visitors are registered, required to wear a visitor badge, and must be accompanied by Processor’s staff throughout their visit.

2. **Access Control to Data Processing Systems**: Processor shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished through the following measures:
    a. Depending upon the particular Cloud Services subscribed: authentication via passwords and/or multi-factor authentication, documented authorization processes, documented change management processes and logging of access on several levels.
    b. Access to Controller data and systems is controlled in accordance with Processor’s Access Control Policy aligned with the ISO/IEC 27001 Standard.
    c. Staff members of Processor are issued their own login credentials. Passwords must be in line with industry best practices and comply with the Processor’s Login and Password Policy (e.g., length and complexity).
    d. Automatic time-out of workstations if left idle, authentication is required to reopen.
    e. Staff policies in respect of each staff access rights to personal data (if any), informing staff about their obligations and the consequences of any violations

of such obligations to ensure that staff will only access personal data and resources required to perform their job duties and training of staff on applicable privacy duties and liabilities.

f. Use of state-of-the-art encryption technologies for data in transit and data at rest.

3. **Access Control to use Specific Areas of the Data Processing System**: Processor shall commit that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied, modified, or removed without authorization. This is accomplished through the following measures:
    a. Staff members of Processor are assigned with access based on the principle of least privilege. Access controls to be applied include a documented change management process and multi-factor authentication and encryption. This access is controlled in alignment with the Processor's Cloud Access Control Policy, Clear Desk and Clear Screen Policy, Encryption Policy and Customer Cloud Data Privacy Policy.
    b. Data transfer requirements of the Processor's Cloud Communication Security Policy are aligned with the ISO/IEC 27001 Standard.
    c. Use of state-of-the-art encryption technologies for data in transit and data at rest.

4. **Separation of Processing for Different Purposes:** Processor shall implement suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished through the following steps:
    a. Processing of tenant content is directly encapsulated in the cloud application accessed via the Cloud Service. Access control to the tenant application is the responsibility of the Controller. Controller tenant content is directly encapsulated in the logically segregated tenant database.

5. **Pseudonymization**: To achieve the purposes of the commissioned data processing, it is impossible to pseudonymize personal data. If pseudonymization is required by the Controller, the data must be processed within the Cloud Service in a pseudonymized format.

6. **Encryption:** All relevant data is transmitted and stored in line with highest standards defined in Encryption Policy, using state-of-the-art encryption algorithms.

2. Integrity (ART 32 PARA. 1 LIT B GDPR)

1. **Input Control:** Processor shall implement suitable measures to monitor whether and by whom personal data has been entered, modified or removed from data processing systems. This is accomplished through the following measures:

a. The source of personal data is under the control of the Controller, and personal data input into the Cloud Service is managed by secured file transfer (i.e., via web services or entered into the application) from the Controller. Note - specific Cloud Services may permit Controller to use unencrypted file transfer protocols. In such cases, the Controller is solely responsible for its decision to use such unencrypted file transfer protocols.
b. Only authorized personnel can access the production cloud infrastructure of Controller data processing for the sole purpose of management and maintenance functions. All personnel have a unique user ID and use strong passwords according to the Login and Password Policy, and all such activities are monitored and logged. Authentication of the authorized personnel; individual user IDs that, once assigned, cannot be re-assigned to another person.

2. **Transmission Control**: Processor implements suitable measures to prevent personal data from being read, copied, altered, or deleted by unauthorized parties during transmission. This is accomplished through the following measures:
    a. For all production cloud environments, IaaS provider security mechanisms provide private, isolated areas for Processor Cloud where respective Cloud resources are launched in a defined virtual network. All scoped data is stored in a virtual cloud environment and is transmitted through HTTPS with up-to-date encryption ciphers.
    b. Controller tenant data-at-rest for Cloud Services is encrypted. Except as otherwise specified for the Cloud Services (including within the ordering document or the applicable service specifications), transfers of data outside the Cloud Service environment are encrypted.
    c. Data transfer requirements of the Processor's Cloud Communication Security Policy protect the transfer of Controller tenant data through the use of all types of communication facilities.
    d. Use of appropriate firewall and encryption technologies for data in transit.
    e. Data transmissions are logged and monitored.

3. Availability and Resilience (ART 32 PARA. 1 LIT B GDPR)

1. **Availability Control**: Processor shall implement suitable measures to ensure that personal data is protected from accidental or unauthorized alteration, loss or destruction. This is accomplished through the following efforts:
    a. Any changes to the production environments are fully monitored. Processor performs regular tenant backups to be able to restore virtual machine images and tenant data.
    b. Control of availability for Cloud Services is ensured under the Cloud Services Information Security Continuity Management and Operations Backup and Restore Controls aligned with the ISO/IEC 27001 Standard.
    c. Processor's IaaS Supplier services are protected from utility service outages in alignment with the ISO/IEC 27001 standard as validated and certified by an independent auditor, and the identification of the person who carried them out is recorded.

d. Backup up of Controller data and protection of log files are controlled in alignment with the ISO/IEC 27001 Standard (Refer to Annex A 12 for additional details). Policies are in place to control the retention of backup copies.
e. Any detected security incident is recorded, alongside the followed data recovery procedures.

2. **Resilience**: Firewalls protect external access to all cloud production networks and systems, and Intrusion Detection Prevention Systems are used to limit/filter network traffic. Cloud Services Disaster recovery is tested and reviewed annually.

4. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing (ART. 32 PARA. 1 LIT. D GDPR)

1. **Data Protection Management:** The Processor has implemented a Data Protection Management System which contains documented data protection processes such as handling data breaches, maintaining records of processing activities, and supporting the Controller in processing data subject requests. The Data Protection Management System is subject to regular review and audit.

2. **Incident Response Management:** The Processor has clearly defined IT Security Incident Handling and Data Breach Handling processes in the scope of the Quality Management and Data Protection Management System aligned with the ISO/IEC 27001 Standard. Security Incidents are tracked with the Processor's incident management tool. The incident response program of the IaaS Supplier (detection, investigation, and response to incidents) has been developed in alignment with ISO 27001 standards, and system utilities are appropriately restricted and monitored.

3. **Data Protection by Default (Art. 25 para. 2 GDPR)**: The Processor has data protection policies and controls that prohibit Cloud Services staff from accessing tenant data unless explicitly authorized and granted by the Controller tenant administrator. Controller tenant content is directly encapsulated in the logically segregated tenant database. Personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. The default configurations of Cloud Services are designed to process only personal data required to deliver the service.

4. **Job Control**: Processor implements suitable measures to ensure that the personal data is processed in accordance with the Controller's instructions. Processor shall ensure that if sub-processors' security measures apply for providing support services, the Processor obtains written description of those measures. Additionally, the Processor shall regularly monitor sub-processors' compliance with these measures. This is accomplished through the following efforts:
    a. The control of personal data remains with the Controller. As between Controller and Processor, Controller will at all times remain the Controller for the purposes of the Cloud Services, the Cloud Services Agreement, and the Data Processing Agreement. Controller is responsible for compliance with its obligations as Controller under data protection laws, in particular for justification of any transmission of personal data to Processor (including providing any required notices and obtaining any required consents), and for its decisions and actions concerning the processing of and use of the data.
    b. Processor will process personal data solely for the provision of the Cloud Services and will not otherwise (i) process or use personal data for purposes other than those outlined in the Cloud Services Agreement or as instructed by Controller, or (ii) disclose such personal data to third parties other than sub-processors for the purposes mentioned above or as required by law.
    c. Access to Controller data and systems are controlled following Cloud Services Access Control Policy and Operations Security Controls aligned with the ISO 27001 Standard.

5. **Job Control–System Administrators:** Processor shall further implement suitable measures to monitor its cloud service system administrators and to ensure that they act per instructions received and comply with respective ISO/IEC 27001 controls. This is accomplished through the following measures:
    a. Individual appointment of system administrators;
    b. Regular review of system administrators to assess compliance with assigned role; Keeping an updated list with system administrators' identification details;.
    c. Evaluation of sub-processors' technical and organizational measures prior to their engagement and regular monitoring sub-processors' compliance with these measures.

Additional country specific measures

The following measures apply to the extent the Controller is located in the respective country:

I. Belgium

A. It is agreed that each Processor subscribes this DPA for its own purposes and its own data processing, without being bound jointly or severally ("solidairement ou indivisiblement") with the others.

B. By express deviation from Article 1325 of the Belgian Civil Code, this DPA may be validly executed separately by each signatory and shall be properly evidenced by the production of any original or non original copy thereof together with the signature pages (or copies thereof) of the other relevant parties. The Parties waive any and all evidentiary and/or other requirements as to the execution of this DPA other than those enunciated in this section for Belgium.

II. Luxembourg

A. It is agreed that each Processor subscribes this DPA for its own purposes and its own data processing, without being bound jointly or severally ("solidairement ou indivisiblement") with the others.
B. Done in [two] originals, each Party acknowledgement receipt of one duly signed original.

III. Australia

The following amendments apply only in respect of the processing of personal data by the Processor on behalf of a Controller which has an Australian link in respect of that personal data within the meaning of the Privacy Act 1988 (Cth) ("**Australian Data**"), irrespective of whether the country where the subprocessor is located has been designated by the European Commission as ensuring an adequate level of protection pursuant to Article 45 (1) General Data Protection Regulation:

A. In this DPA, references to
    1. a "Member State" includes Australia;
    2. the "General Data Protection Regulation", "GDPR", "applicable data protection laws" ("**EU Privacy Laws**"), and any provisions, sections, Chapters or Articles of those of those EU Privacy Laws, in the Agreement shall be replaced with the term "Privacy Act 1988 (Cth) and any applicable state and territory-based privacy laws, and all related laws and regulations" ("**Australian Privacy Laws**");
    3. "personal data" shall be read as including personal information within the meaning of Australian Privacy Laws;
    4. the "supervisory authority" shall be read as references to the competent regulatory authority pursuant to Australian Privacy Laws; and
    5. "special categories of data" and "sensitive data" shall be read as including sensitive information within the meaning of Australian Privacy Laws;
B. The Processor will take reasonable steps to protect Australian Data it processes from misuse, interference and loss and from unauthorized access, modification or disclosure;
C. The Processor will notify the Controller without undue delay of: (i) any known or reasonable ground to believe of non-compliance with statutory provisions dealing with the protection of Australian Data by the Processor or its employees, and (ii) any known or reasonable ground to believe of non-compliance with the provisions of this DPA. The Processor shall further

notify the Controller, without undue delay, if it holds that an instruction violates applicable laws. Upon providing such notification, the Processor shall not be obliged to follow the instruction, unless and until the Controller has confirmed or changed it. The Processor shall notify the Controller of data subjects' complaints and requests (e.g., regarding the rectification, deletion and blocking of data) and orders by courts and competent regulators and any other exposures or threats in relation to data protection compliance identified by the Processor and shall provide reasonable assistance to the Controller to respond to such complaints or requests in a timely manner. Notwithstanding (i) and (ii) above, the Processor will provide the Controller immediately with a data breach notice if the Processor has reasonable grounds to believe there has been any security incident that is likely to have impact on the availability, integrity and / or confidentiality of the Australian Data processed by the Processor (e.g., discovery of unintended data deletion, discovery of data being accessible to resources that were not or no longer authorized, discovery of unintended disclosure or data potentially having become compromised by a hacking attack or other external security threat). The data breach notice must contain as a minimum the scope of the Australia Data affected, the scope and number of data subjects affected, the time when the data breach took place, the circumstances, and the effects of the data breach, and the measures taken to eliminate the consequences of the breach and further information the Controller may require to comply with Australian Privacy Laws;

D. Australian Data must be destroyed or permanently de-identified after it is no longer required for a purpose permitted by this DPA. The Processor must obtain written confirmation from the Controller that Australian Data is no longer required prior to destroying or de-identifying that Australian Data.
E. Australian Data may only be processed for direct marketing where the data subject has expressly consented to such processing, or as otherwise agreed by the Controller in writing;
F. Identifiers of data subjects that have been assigned by or on behalf of any Australian government organisation must not be used or disclosed unless required or authorised by Australian law; and
G. Sensitive data may only be processed as authorised by the data subject, unless the Controller otherwise agrees in writing.

IV. Malaysia

Processor shall adopt the following security measures in accordance with the requirements of the Personal Data Protection Standard 2015 and Personal Data Protection Act 2010:

A. to maintain a register of all its employees involved in the processing of personal data;
B. discontinue its employees' rights after the end of service, termination, and end of contractual / agreement term, or pursuant to organizational changes;
C. control and limit the extent of its employees' right to access personal data;
D. control the outward and inward movement in respect of data storage locations;
E. update all back up / recovery systems and anti-virus software to protect personal data from incidents of invasion;
F. protect computer systems from malware threats against personal data;

G. to ensure that the transfer of personal data through removable media device and cloud computing service is only with the written authorization of senior management of the processor;
H. to record all transfer of personal data which utilizes a removable media device and cloud computing service; and
I. to maintain an accurate periodic personal data access record and to disclose the records when requested by the Malaysian Personal Data Protection Department.

V. Mexico

For controllers based in Mexico, the Federal Law on Protection of Personal Data Held by Individuals 2010 and the following additional measures apply:

A. Processor shall define the functions and obligations applicable to officers in charge of the protection of the personal data;
B. Subprocessor shall implement a suitable data protection management in its organization, including those set out below:
    1. Create and maintain inventories of: (i) personal data items collected from data subjects and; (ii) security systems and storage infrastructure used for the processing the personal data;
    2. Conduct security measures gap analysis and carry out regular security risks audits and assessments to identify and evaluate possible risks and areas of improvement;
    3. Design and implement action plans to address any issues identified in such assessments and audits;
    4. Provide appropriate training to staff involved in the data processing activities;
    5. Update Security Measures accordingly to improve such measures either as result of recommendations derived from audits or assessments or after the confirmation of any unauthorized access or disclosure of personal data.

VI. India

The Digital Personal Data Protection Act 2023 is applicable to protect personal data and is expected to come into force in 2024. Additional Measures for Controller located in India: The Processor shall ensure the same or greater level of data protection, as is adhered to by the Controller, under the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

VII. Israel

1. The Controller and Processor shall comply with applicable data protection laws, including the Protection of Privacy Law 1981 and any updates to align with the EU GDPR.
2. The Processor will provide a report to the Controller, at least once a year, with respect to the manner in which it performs its duties under the Israeli Information Security Regulations and this DPA and will notify the Controller of the occurrence of any security event in which the personal data is involved.
3. The Processor undertakes that it will and will procure that the authorized persons on its behalf will maintain all the necessary security measures required in accordance with any applicable law in connection with the personal data, including any requirement for the protection of the integrity of such personal data and protection against any unlawful disclosure, use or copy thereof.
4. The Processor undertakes to provide the Controller, upon its reasonable demand, reports concerning the security measures implemented by it and will allow the Controller and/or anyone acting on its behalf.
5. The Processor undertakes to provide from time to time and in any event no less than once a year tutorials to anyone acting on its behalf in connection with the obligations under this DPA, including the duty to maintain the personal data in strict confidence.
6. The Processor will comply with all requirements of the Controller regarding data security which are required under applicable data protection laws as shall be informed to the Processor from time to time, The Processor shall limit or prevent the possibility of connecting portable devices to the systems in which the personal data is stored.
7. The Processor shall ensure that ongoing updates are performed on the database systems in which the personal data is stored.
8. When applicable according to the Israeli Information Security Regulations, the Processor should take measures to control and document the entry into, and exit from, the locations where the systems in which the personal data is processed are situated and of the introduction and removal of equipment into and from such sites.
9. The Processor shall grant permission to access to the personal data or change its scope after reasonable measures are taken by it. Access permissions to the personal data will be determined according to job definitions.
10. Processor shall commit that the persons entitled to use its data processing system should sign applicable confidentiality undertakings according to which they will keep the information confidential and that they will use the information only for the purposes of providing the Services to the customer.
11. Processor shall implement suitable measures to make sure that it can check and establish when there was access to the personal data.
12. Processor shall revoke the authorizations of an authorized person that has finished his role. and, insofar as possible, immediately upon termination of the authorized person's role, change the passwords that the authorized person might have known.
13. The systems in which the personal data is stored shall not be connected to the internet or to any other public network without the installation of appropriate means of protection from unauthorized intrusion, or from programs capable of causing damage or disruption to the computer or computer material (including the use of accepted means of encryption). In relation to a system that can be accessed remotely using the internet or another public network, security measures additional to those set forth shall be taken whose objective is to identify the party making the connection and to verify his authorization to perform the operations remotely and its scope.

DOCUMENT HISTORY

Version	Date	User ID	Comment
1.0	Dec 9, 2024	Jane Porter	Initial draft

ABOUT Cumulocity GmbH

Founded in 2012, Cumulocity is a global leading industrial IoT platform, offering ready-to-use device management and low code application enablement for a fast return on investment. For more information, visit www.cumulocity.com