CUMULOCITY

Personal Data Processing and Compliance – FAQ

This FAQ provides information on how we manage the processing of personal data, protect your privacy, and ensure compliance with applicable data protection regulations, including GDPR and other relevant standards.

How does Cumulocity GmbH ensure data protection compliance in its products and services?

All products offered by **Cumulocity GmbH** have been analyzed for compliance with data protection principles concerning their functionality in processing personal data. For future enhancements, a **data protection compliance check** has been integrated into the product release cycle.

How are accountability and governance requirements addressed?

Cumulocity GmbH has established a **Data Protection Management System (DPMS)** that defines clear processes for key data protection aspects, including:

- Handling **Data Subject Requests**
- Managing **Data Breaches**
- Reviewing **Data Processing Agreements (DPA)**
- Conducting **Data Privacy Impact Assessments (DPIA)**
- Performing **Transfer Impact Assessments (TIA)**
- Assessing **Data Breach Risks**

As part of **Cumulocity GmbH's ISO 9001 certification**, these DPMS processes are subject to regular external audits.

Additionally, we have implemented a **Global Data Protection Policy**, applicable to all employees. This policy ensures legally compliant handling of personal data and protects the rights of individuals whose data is processed by **Cumulocity GmbH** and its subsidiaries.

How does Cumulocity GmbH process personal data on behalf of customers?

When **Cumulocity GmbH** processes personal data on behalf of its customers (data controllers), or when access to such data is required for service provision, a **Data Processing Agreement (DPA)** is established. This covers:

- **Customer Instructions:** Cumulocity GmbH processes personal data strictly as instructed by the customer and in compliance with relevant data protection laws.
- **Use of Sub-processors:** To ensure high service availability, **Cumulocity GmbH** engages affiliates and carefully selected external service providers, all of whom act as sub-processors.
- **Data Transfers:** For data transfers from the **EEA to non-adequate jurisdictions**, **EU Standard Contractual Clauses** are implemented to maintain compliance with data protection regulations.
- **Handling Data Subject Requests:** Customers, as data controllers, may be required to respond to data subject requests. **Cumulocity GmbH** supports customers with appropriate technical and organizational measures to facilitate compliance.
- **Data Breach Notification:** In the event of a data breach, **Cumulocity GmbH** notifies affected customers without undue delay, ensuring compliance with regulatory obligations.
- **Technical and Organizational Measures (TOMs):** We implement robust **security measures**, which are continuously reviewed and updated as necessary to protect personal data.

How does Cumulocity GmbH handle data breaches?

A **Data Breach Handling Process** is documented within our DPMS. In case of a security breach leading to unauthorized access, loss, or alteration of personal data:

1. The incident is reported to the **Data Protection Team**.
2. The team assesses the breach's scope, impact, and root cause.
3. If necessary, the **Data Protection Officer (DPO)** determines whether to notify regulatory authorities and affected individuals.

How does Cumulocity GmbH handle data subject requests?

We have a **Data Subject Request Handling Process** in place. Upon receiving a **Data Subject Request (DSR)**:

1. The request is forwarded to the **Data Protection Team**.
2. Identity verification is conducted.
3. Relevant business teams are consulted to check for the requested data.
4. A response is provided to the data subject within statutory deadlines.

If identity verification is insufficient, **Cumulocity GmbH** may request additional proof, such as a passport or ID card.

Does Cumulocity GmbH conduct privacy risk assessments (DPIA)?

Yes, we perform **Data Protection Impact Assessments (DPIAs)** when processing activities pose a high risk to data subjects' rights and freedoms. Our **DPIA process** evaluates:

- **Necessity and proportionality** of data processing
- **Potential risks** to data subjects
- **Mitigation measures** to reduce identified risks

If risks remain high, the **processing activity cannot proceed** without additional safeguards.

Does Cumulocity GmbH have a Data Protection Officer (DPO)?

Yes, **Cumulocity GmbH** has appointed a **Corporate Data Protection Officer (CDPO)** responsible for monitoring compliance with data protection laws and advising on personal data processing. The **Data Protection Team** supports the **CDPO** in fulfilling these responsibilities.

Are employees trained in data protection?

Yes, **Cumulocity GmbH** provides **mandatory data protection training** for all employees. This training covers:

- **Legal requirements** for handling personal data
- **Technical and organizational security measures**
- **Compliance with global data protection policies**

Non-compliance with training requirements is monitored and may lead to disciplinary action.

How does Cumulocity GmbH comply with evolving data protection laws?

Given the **dynamic nature of data protection laws**, we:

- Regularly **review and update** our **DPMS** and **Technical and Organizational Measures (TOMs)**.
- Adapt internal processes to **new regulatory requirements**.
- Conduct **external audits** as part of our **ISO 9001 certification** to ensure continued compliance.

For further details, refer to:

- **Cumulocity GmbH Privacy Notice**: https://cumulocity.com/docs/legal-notices/privacy-notice
- **Technical and Organizational Measures (TOMs)**: https://www.cumulocity.com/legal/toms-subprocessors/