Annex to the agreement to provide IoT services: BODAS Connect

1 Agreement pursuant to Art. 26 para. 1 General Data Protection Regulation (GDPR)

Preamble

The customer of the platform called CUSTOMER and Bosch Rexroth AG, called BOSCH REXROTH GERMANY, both together called the DATA PARTIES, work together in the context of IoT-Services in a cooperative effort. This also involves the processing of personal data within the meaning of Art. 4 No. 1 GDPR. In order to meet the requirements of data protection law and to ensure the greatest possible transparency for the persons concerned, the DATA PARTIES therefore agree to the following:

1.1 Definitions

Terms defined within the GDPR and used in this Agreement shall have the meaning given in the GDPR. In all other respects, the following definitions shall apply:

“**Applicable data protection law**“ is the data protection law applicable to the contractual partners in the European Union, including the GDPR and the national data protection laws to be observed in the territory of a member state of the Union (in particular the German BDSG).

“**Data subject rights**” means a request from a data subject asserting rights under Art. 15 - Art. 22 GDPR.

“Data protection incident” means a violation of the protection of personal data in accordance with the definition in Art. 4 No. 12 GDPR.

“**Responsible party**” means the DATA PARTY responsible for fulfilling data protection obligations under the applicable data protection law in accordance with the provision in clause 3.

"Bosch internal service provider" as listed in clause 4 of this agreement.

1.2 Scope of agreement

This agreement applies exclusively to activities in the context of which the DATA PARTIES jointly process personal data and regulates the rights and obligations existing in this context. The provisions of this Agreement also apply to processors that are used by the DATA PARTIES to process personal data.

The DATA PARTIES have jointly determined the measures and purposes of the data processing activities described in the Process Records, clauses 2.1 through 2.3, and are therefore jointly responsible for the processing within the meaning of the GDPR.

Apart from the jointly performed data processing activities resulting from the Process Records, clauses 2.1 through 2.3, the DATA PARTIES are considered independent controllers within the meaning of Art. 4 No. 7 GDPR and independently responsible for compliance with the applicable data protection law.

1.3 Compliance with data protection

Each DATA PARTY shall ensure compliance with applicable data protection law, and in particular, the lawfulness of processing activities carried out by it, including in the context of joint data processing.

The DATA PARTIES shall take all necessary measures to ensure that the rights of the data subjects, in particular in accordance with Articles 12 to 22 GDPR, are guaranteed at all times within the statutory periods.

The DATA-PARTIES shall ensure that appropriate technical and organizational measures within the meaning of Art. 32 GDPR as well as the security concept from clause 3 of this document and the principles of Art. 25 GDPR ("Privacy by Design" and "Privacy by Default") are complied with and document compliance independently.

1.4 Responsibilities for individual data processing activities and notification obligations

Within their joint controllership, the DATA PARTIES shall proceed on the basis of a joint responsibility. The responsibilities for individual processing activities are set out in Process Records, clauses 2.1 through 2.3.

If the DATA PARTIES discover irregularities or errors with regard to compliance with data protection regulations, the DATA PARTIES will inform each other immediately.

1.5 Compliance with the information obligations towards data subjects

The CUSTOMER is obliged to provide the data subject, free of charge, with the information required under Art. 13 and 14 GDPR in a precise, transparent, comprehensible and easily accessible form in clear and simple language.

Each DATA PARTY is obliged to provide the information required to produce the information in accordance with Articles 13 and 14 GDPR, insofar as it is responsible for individual processing activities.

The DATA PARTIES will coordinate the content of the information pursuant to Art. 13 and 14 GDPR before the data processing activity begins.

1.6 Fulfillment of the data subject rights

The data subjects can assert the rights to which they are entitled under Art. 15- 22 GDPR against both DATA PARTIES.

BOSCH REXROTH shall be responsible for the implementation of the rights of the data subjects and for any necessary communication with the data subjects.

Where a data subject makes a request to one of the DATA PARTIES in exercise of his or her rights as a data subject, the DATA PARTIES undertake to transmit this request to the other DATA PARTY without delay, irrespective of the obligation to guarantee the rights of the data subject.

Should a data subject request the deletion of his/her personal data, the DATA PARTIES will inform each other immediately. The respective other DATA PARTY may object to the deletion for justified reasons.

The DATA PARTIES support each other in implementing the rights of the persons concerned.

1.7 Accessibility of this agreement

The CUSTOMER undertakes to make the essential content of this agreement available to the data subjects in accordance with Art. 26 para. 2 GDPR.

1.8 Obligations to report data protection breaches

BOSCH REXROTH shall be responsible for the notification and notification obligations resulting from Art. 33, 34 GDPR to the supervisory authority and the data subjects by a violation of the protection of personal data.

The DATA PARTIES shall inform each other within 24 hours of becoming aware of any violations of the protection of personal data processed under this Agreement.

The DATA PARTIES shall assist each other in clarifying the facts of the case and, where necessary, notifying the supervisory authority and the persons concerned.

1.9 Data protection impact assessment

If necessary, the DATA PARTIES shall assist each other in conducting a data protection impact assessment pursuant to Art. 35 GDPR.

1.10 Data processing under commission

The DATA PARTIES shall conclude a contract in accordance with Art. 28 GDPR when using processors within the scope of this agreement and obtain the written consent of the other DATA PARTY before concluding the contract.

The DATA PARTIES shall inform each other in due time of any intended change with regard to the use or replacement of subcontracted processors and shall only use subcontractors that meet the requirements of data protection law and the provisions of this Agreement.

The DATA PARTIES shall draw up a list of processors within the scope of this Agreement in accordance with Annex 4.3.

1.11 International data transfers

In case one DATA PARTY is located outside the EU/EEA and in a country for which an adequate level of data protection is not recognized, the DATA PARTIES shall conclude standard contractual clauses for the transfer of personal data to third countries or any other appropriate agreement ensuring the protection of personal data.

1.12 Liability

Without prejudice to the provisions of Art. 82 GDPR and without prejudice to the provisions of this Agreement, the DATA PARTIES shall be jointly and severally liable to the data subjects in their external relations for any damage caused by processing which does not comply with the GDPR.

1.13 Miscellaneous

An invalid or unenforceable provision of this agreement shall not affect the remaining provisions of this agreement. In such a case, the invalid or unenforceable provision shall automatically be replaced by a valid and enforceable provision that comes closest to the purpose of the original.

2 Recording of data processing activities in the context of projects under joint responsibility (Art. 26 GDPR)

2.1 Master data

2.1.1 Basic information

Name of the data processing: Collect master data

Controller for this processing will be the CUSTOMER

The contact person is the customer-side purchaser/buyer on the Rexroth Marketplace unless otherwise agreed.

Description:

- Collecting employee data for login
- Assignment of users to CUSTOMER
- Collecting of machine data on device portal and data management portal

Data flow:

Employee of CUSTOMER provides relevant information (e.g. Name, given name, email address, telephone number) to Bosch registration portal and receives credentials. These data are stored at Bosch internal service provider (one-time).

After successful login at the device portal or the data portal, the respective portal stores the information of the managed devices. The input data of the managed devices, the modifications of that data respectively, are stored in log-files (incl. user-ID of the CUSTOMER employee who has issued the modifications). These data are stored at the Bosch internal service providers.

What are the purposes of the data processing?

- Licensing and registration
- Management of IoT devices incl. management of Software updates on these devices

2.1.2 Data subjects and affected data types

Which data subjects are affected by the data processing?

Employees of CUSTOMER

Which data types are affected by the data processing?

- Personal details (incl. photos)
- Log- and protocol data

2.1.3 How is personal data processed?

- The server infrastructure is used by Bosch internal service providers to process the data.
- In the context of data processing, no personal data is transferred to or processed by a country outside the EU.

2.1.4 Additional provisions in other jurisdictions

- Russian Federation
    - No processing of personal data for Russian citizens as Russian citizens must not enter personal data like real names as login credentials.

2.2 Device Management

2.2.1 Basic Information

Name of the data processing: Device Management

Controller of the data processing will be the BOSCH REXROTH AG

The contact person for the controller is the DC-MH/PJ-IOT department.

Description

The processing is used to manage IoT devices

Data flow:

Information of IoT devices (e.g. serial number, MAC address, software version, geoposition, data of the SIM card and further customer specific data) is stored on servers. On the next customer login, the device portal provides information on newly available.

updates for the respective IoT devices based on an automatic cross-check of stored IoT data (like serial number, SW version etc.) and the newly input data on generally available SW for this kind of device. The system shows the status of the IoT devices to the customer. Respective data are not permanently stored. These actions are provided by Bosch internal service providers.

What are the purposes of the data processing?

- Management of IoT devices
- Identification of SW updates for the stored/managed devices

- Information about necessary updates on next login of customer employees

2.2.2 Data subjects and affected data types

Which data subjects are affected by the data processing?

- Employees
- Customer employees

Which data types are affected by the data processing?

- Log- and protocol data

2.2.3 How is personal data processed?

How is the personal data processed technically?

- Server infrastructure at Bosch internal service providers.
- Cloud based SaaS applications at external service providers for the supply of update packages.
- In the context of data processing, no personal data is transferred to or processed by a country outside the EU.

2.3 Data management

2.3.1 Basic information

Name of the data processing: Data management

Controller of the data processing will be the BOSCH REXROTH AG

The Contact person of the controller ist the department DC-MH/PJ-IOT

Description:

Data storage, data processing, data visualization

Data flow

Data (e.g. geo-location, process data like speed, pressure, consumption of consumables) of connected machines are stored on databases on servers. A user might scan the data on the database on the servers. The internal processor processes the data. The frontend visualizes the data. The user can download the data. Furthermore, a user can access and trigger all features of the data management via the respective REST API. Bosch internal service providers conduct and provide these services.

The data processing is used for the purpose of overview and analysis of the use and behavior of machine fleets.

2.3.2 Data subjects and affected data types

Which data subjects are affected by the data processing?

- Employees
- Customer employees

Which data types are affected by the data processing?

Log- and protocol data

2.3.3 How is personal data processed?

How is the personal data processed technically?

The server infrastructure is used by Bosch internal service providers to process the data.

In the context of data processing, no personal data is transferred to or processed by a country outside the EU.

3 Technical and organizational measures / security concept

3.1 Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)

- Physical access control
  No unauthorized access to data processing systems, e.g.: magnetic or smart cards, keys, electric door openers, plant protection or security guard, alarm systems, video systems.
- Logical access control
  No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption.
- Data access control
  No unauthorized reading, copying, changing or removing within the system, e.g.: authorization concepts and user-specific access rights, logging of access.
- Separation control
  Separate processing of data collected for various purposes, e.g. multi-client capability, sandboxing.

3.2 Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)

- Transfer control
  No unauthorized reading, copying, changing or removing during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature.
- Input control
  Determination of whether and by whom personal data was entered, changed or removed in data processing systems, e.g.: logging, document management.

3.3 Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR), e.g.

- Availability control
  Protection against accidental damage or destruction or loss, e.g.: backup strategy

(online/offline; on-site/off-site), uninterrupted power supply (UPS), virus protection, firewall, escalation ways and emergency plans

- Order control
  No data processing under commission according to Art. 28 of the GDPR without corresponding instructions from the Data controller, e.g.: explicit contract design, formalized order management, stringent selection of the service provider, obligation to convince in advance, follow-up inspections.
- Resilience
  Systems and services (e.g. storage, access, line capacities, etc.) are designed in a way that even intermittent high stresses or high constant loads of processing can be ensured.

3.4 Measures for the pseudonymization of personal data, e.g.

- Separation of customer master data and customer sales data
- Use of personnel, customer, and supplier ID instead of names

3.5 Measures for the encryption of personal data, e.g.

- Symmetrical encryption
- Asymmetrical encryption
- Hashing

3.6 Measures to quickly restore the availability of personal data to them after a physical or technical incident, e.g.

- Back-up concept
- Redundant data storage
- Double IT infrastructure
- Backup datacenter

3.7 Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR), e.g.

- Privacy management
- Incident response management
- Data protection by default (Art. 25 para. 2 of the GDPR)
- Assessment by DSO, IT audits
- External assessment, audits, certifications

4 Subcontractors of the Parties

Name, address of the subcontractor:

Robert Bosch Manufacturing Solutions GmbH
Bosch Connected Industries

Order content (scope of the assignment by the contractor): Nexeed Device Portal

Place of data processing: Wernerstraße 51, 70469 Stuttgart

Transmission of/access to personal data of the client (type of data and circle of persons concerned

Type of data:
Login data of IoT devices
Communication data (Email; Bosch global User ID (CIAM))
Other: TenantID (MandatesID), User access roles and user access rights, Device information, Device backups

Circle of affected persons:
Customers or users of services (here the user of the Device Portal)

Name, address of the subcontractor

Robert Bosch GmbH

Order content (scope of the assignment by the contractor): Bosch IoT Insights

Place of data processing: PO Box 300240,70442 Stuttgart GERMANY

Transmission of/access to personal data of the client (type of data and circle of persons concerned

Type of data:
Communication data (Email; Bosch global User ID (CIAM))
Other: Device information, Localization, Technical machine data, TenantID, User access roles and user access rights

Circle of affected persons:
Customers or users of services (here the user of the data portal)