BOSCH
Invented for life

Bosch IoT Suite

SaaS Data Processing Under Commission

Data Processing Under Commission Agreement

Find the German language version of this document here.

As of November 26, 2020

Version: 1.0

This agreement applies for data processing under commission for personal data to the use of software applications on the basis of Software as a Service (SaaS) by Bosch.IO GmbH, Ullsteinstr. 128, 12109 Berlin,(hereinafter: **"Provider (Data Processor)"** to the customer (hereinafter: **"Customer (Data Controller")**. (Customer and Provider hereinafter collectively referred to as **"Parties"** and individually as **"Party"**).

Preamble

The present Agreement specifies the obligations of the parties on data protection according to the order detailed in the SaaS Terms and Conditions. It is applicable to all activities connected to the SaaS Terms and Conditions and the subscriptions of Services on www.Bosch-IoT-Suite.com and in which employees of the Provider or subprocessors of the Provider may process personal data ("data") of the Customer.

§1 Subject matter, duration and specification of contract data processing

1.1 The subject matter, type and purpose of contract data processing under commission are described in the SaaS Terms and Conditions and the service description.

1.2 The processing comprises potentially the following types of data: Time recording, Personal master data, Communication data, Contractual master data, Client history, Contract accounting and payment data, Planning and regulation data, Provision of information, miscellaneous personal data.

1.3 The following categories of individuals are affected by the processing: Business management, Senior employees, Customers employees, Customers employees, Customers prospects, Customers subscribers, Customers suppliers (in particular consultants and cooperation partners subcontracted by the Customer), Customers trade representatives, Customers contact partners, Miscellaneous affected individuals

1.4 The term of the present Agreement is determined by the subscription period of the SaaS Terms and Conditions unless obligations going beyond that date result from the provisions of the present Agreement.

1.5 Any services in connection with data processing under commission under this Agreement shall be rendered exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any

relocation to a third country requires the Customers prior agreement and is permitted only if the special requirements of Art. 44 et seqq. GDPR have been satisfied.

§2 Scope of application and responsibility

2.1 The Provider processes personal data at the instruction of the Customer. This comprises activities as described in the SaaS terms and Conditions and the Service descriptions. With regard to data processing under commission, the Customer is responsible for compliance with the statutory regulations on data protection and especially for the legitimacy of data processing.

2.2 At first, the instructions will be set forth in in the SaaS terms and Conditions and the Service descriptions. The instructions may subsequently be amended, supplemented or replaced by the Customer in writing or in text form (single instruction) to the indicated persons of the Provider. Single instructions going beyond the services agreed in the contract, will be treated as a change request, and the Provider is entitled to request adequate financial compensation.

2.3 The Provider shall inform the Customer without delay if it is of the opinion that an instruction violates data protection rules. The Provider is entitled to suspend compliance with the instruction in question until it is either confirmed or changed by the Customer.

§3 Obligations of the Provider

3.1 The Provider may process personal data of data subjects only within the scope of the assignment and the documented instructions of the Customer. In the event that the Provider is obliged to process data differently as a result of national or European law, it shall inform the Customer before start of the processing, unless that law prohibits such information on important grounds of public interest.

3.2 The Provider shall set up the internal organisation of his area of responsibility in such a manner that it meets the specific requirements of data protection. The Provider shall take the technical and organisational measures described in Appendix 1 so as to ensure an adequate protection of the Customers personal data. The purpose of these measures is to ensure long-term confidentiality, integrity, availability and resilience of the systems and services in connection with the processing of personal data under commission. The Customer is informed of these technical and organisational measures. It is the Customer´s responsibility to ensure that these measures provide an adequate level of protection regarding the risks of personal data processing.

3.3 The Provider reserves the right to change the technical and organisational measures taken, but must guarantee that the level of protection agreed in the contract is not reduced.

3.4 To the best of his ability and within the scope of the services or under the contract, the Provider shall assist the Customer in dealing with requests and claims of data subjects according to chapter III of the GDPR and in respecting its obligations specified in Articles 32 to 36 GDPR. For these services, the Provider is entitled to adequate financial compensation.

3.5 The Provider warrants that its employees involved in the processing of the Customers personal data and other individuals working for the Provider are prohibited from processing such personal data outside the scope of the Customers instructions. The Provider further ensures that the individuals authorised to process personal data have signed an

agreement of confidentiality or are subject to an adequate confidentiality clause. This obligation of confidentiality and secrecy shall remain in effect even beyond completion of an assignment.

3.6 The Provider shall inform the Customer without delay as soon as it becomes aware of any violation of the protection of the Customers personal data. The Provider shall take the necessary measures to safeguard personal data and to alleviate possible disadvantageous consequences for the data subject and shall consult with the Customer in that respect without delay.

3.7 The Provider is obliged to appoint a competent and reliable Data Protection Officer according to Art. 37 GDPR to the extent and as long as the statutory prerequisites for such an obligatory appointment are in force. The Customer shall be informed of the contact data of this individual for the purpose of making direct contact. If the Provider is not obliged to appoint a Data Protection Officer, it shall give the Customer the name of the contact for any questions in relation to data protection that may arise in connection with the Agreement. Contact information is available at https://www.bosch.io/lp/privacy-statement.html.

3.8 The Provider shall ensure that its obligations according to Art. 32 (1) lit. d) GDPR are complied with and put in place a process for regular examination of the effectiveness of the technical and organisational measures to ensure the safety of processing.

3.9 The Customer is responsible for correction and erasure of personal data. The same is valid for the restriction of the processing of personal data under commission (blocking).

3.10 The personal data shall be erased at the date of completion of the respective Contract. It is up to the Customer to prepare backup copies of its personal data and to move such personal data before the end of the contract. The Provider is not obliged to hand over personal data to which the Customer has direct access.

3.11 The Provider undertakes to maintain a record of data processing activities according to Art. 30 (2) GDPR.

§4 Obligations of the Customer

4.1 It is the Customers responsibility to provide the Provider with the personal data in due time so as to enable the latter to provide the services according to the Contract. The Customer is responsible for the quality of the personal data. The Customer shall inform the Provider immediately and completely in the event that it should identify any errors or irregularities with regard to data protection rules or in the performance of the Provider when checking the work results.

4.2 In the event that claims should be made by a data subject in connection with Art. 82 GDPR, the Customer and the Provider undertake to assist each other in the defence against such claims.
The Customer shall provide the Provider with contact details for any data protection enquiries arising in connection with the Agreement named in the Account Data.

§5 Enquiries from data subjects

If a data subject contacts the Provider demanding correction, erasure, restriction of processing or information about the personal data, the Provider shall refer the data subject

to the Customer if allocation to the Customer is possible on the basis of the information provided by the data subject.

§6 Ways of verification

6.1 If so requested, the Provider shall submit suitable proof to the Customer that the obligations set forth in Art. 28 GDPR and in the present Agreement are complied with. For the purpose of proving compliance with the agreed obligations, the Provider may provide the Customer with certificates and third-party test results (e.g. according to Art. 42 GDPR or ISO 27001) or with test reports from the internal Data Protection Officer or any individual to whom this task has been assigned by the Data Protection Officer.

6.2 In the event that spot checks by the Customer or an auditor appointed by the Customer should turn out to be necessary in individual cases, request shall be made in text form. The Provider is entitled to make approval of such checks dependent on signing an adequate declaration of secrecy by the Customer or the auditor assigned by the Customer. If the auditor appointed by the Customer should be a competitor of the Provider, the Provider is entitled to object. Such objection shall be declared to the Customer in text form.

6.3 In the event that an audit should be carried out by the data protection supervisory agency or another state authority, chapter 6.2 shall apply accordingly. Signing a confidentiality obligation is not required if the supervisory authority is subject to professional or statutory confidentiality any breach of which shall be penalised in accordance with the German Criminal Code.

6.4 The Provider is entitled to request adequate compensation for carrying out such an audit as per chapter 6.2 or 6.3, unless the reason for such an audit is the strong suspicion that a data protection breach has taken place within the scope of responsibility of the Provider. In such a case, details of the suspicion must be submitted by the Customer together with the notification of the examination.

§7 Sub-Processors (additional contract data processors)

7.1 The Customer agrees to the Provider involving subprocessors. Before involving or replacing subprocessors, the Provider shall inform the Customer in text form with four weeks' notice. The Customer may object to such a change. Any objection must be lodged within 14 days, and all reasons must be specified explicitly. If no objection is lodged within this time limit, consent to the involvement or replacement is deemed to have been given. If there is an important reason which cannot be eliminated by the Provider by adjusting the assignment, the Customer is granted an extraordinary right of termination. No separate information will be provided regarding the subprocessors and their partial services than given at https://bosch-iot-suite.com/legal/data-processing-under-commission/ upon signature of the Agreement. If the Provider assigns any subprocessors, it is up to the Provider to convey its obligations regarding data protection under the present Agreement to the subprocessor.

7.2 Upon written request of the Customer, the Provider shall provide information regarding the data protection obligations of its subprocessors at any time.

7.3 The provisions of this chapter 7 shall also apply if a subprocessor in a third country is involved – observing the principles of Chapter 5 of the GDPR. The Provider agrees to

cooperate to the required extend in meeting the prerequisites as set in Chapter 5 of the GDPR.

§8 Liability

8.1 The limitations of liability under the SaaS Terms and Conditions are applicable.

8.2 The Customer shall indemnify the Provider against any claims lodged by third parties against the Providers as a result of the processing of personal data according to the instructions of the Customer unless the claim of such third party is based on processing the personal data by the Customer in violation of instructions.

§9 Obligations of information, written form clause, choice of law

9.1 In the event that the Customers personal data processed by the Provider should be placed at risk as a result of seizure or confiscation, insolvency or settlement proceedings or by other events or measures of a third party, the Provider shall inform the Customer without delay. In this connection, the Provider shall inform all third parties without delay that the control and ownership of the personal data exclusively lies with the Customer as “controller”, as defined in the GDPR.

9.2 Any amendments and additions to the present Agreement and its constituent elements – including any assurances granted by the Provider – shall be made in the form of a written agreement which may also be in electronic form and include an explicit reference that it is an amendment or addition to this Agreement. This shall also apply to the waiver of the requirements of this format.

9.3 In the event of contradictions, the regulations in this data protection Agreement shall take precedence over the regulations of the Contract. If individual regulations of the present Agreement should become invalid, the validity of the agreement as such shall not be affected.

9.4 To the extent permissible by law, the exclusive place of jurisdiction shall be Stuttgart, Germany.

Bosch.IO GmbH

Data Processing Under Commission Agreement – Appendix 1: Technical and Organizational Measures

As of November 26, 2020

Version: 1.0

This agreement applies for data processing under commission for personal data to the use of software applications on the basis of Software as a Service (SaaS) by Bosch.IO GmbH, Ullsteinstr. 128, 12109 Berlin,(hereinafter: **“Provider (Data Processor)”** to the customer (hereinafter: **“Customer (Data Controller”**). (Customer and Provider hereinafter collectively referred to as **“Parties”** and individually as **“Party”**). The following technical and organizational measures are implemented by the Provider and agreed with the Customer.

§1 Measures for the pseudonymization and encryption of personal data

1.1 Pseudonymisierung

Pseudonymization means processing personal data in such a manner that these data can no longer be allocated to a specific data subject without additional information, provided such additional information is kept separately and is subject to technical and organizational measures ensuring that the personal data cannot be allocated to an identified or identifiable natural person.

Measures in connection with the pseudonymization of personal data:

- Selection of a suitable pseudonymization process according to the state of the art
- Mandatory pseudonymization is a central element of the data protection concept of the company
- Pseudonymization of data in accordance with the risk-based approach as per the different data categories requiring protection
- The use of software permitting a safe management of pseudonymised data
- Safe storage of cryptographic keys used for pseudonymization or control lists (if necessary, encrypted storage of control lists)
- Authorization concept for access to cryptographic keys or control lists permitting personalization

1.2 Encryption

Encrypting personal data is a common way to protect it against being read by unauthorized persons. In particular, encryption is suitable to protect data against outside influences such as hacking and espionage. Encrypting means a process by which clearly legible information is converted to a sequence of characters which cannot be read or interpreted.

Measures in connection with the encryption of personal data:

- Encryption of confidential data during transport and over data networks
- Encryption of confidential data when stored on IT end devices and on mobile data carriers
- Carry out a risk analysis when cryptographic measures are not feasible
- Instructions for using coordinated and approved cryptographic techniques, algorithms, applications, and standards
- Generating key material for productive systems at a public key certification authority
- Secrecy of the private keys of a certificate
- Protection against unauthorized access or spying on secret keys as well as the private key of public key cryptography
- Deletion or destruction of keys no longer needed in a secure way

§2 Measures to ensure confidentiality

Among others, measures regarding the implementation of the mandate of confidentiality are those which are part of admission and access control or access inspection. The technical and organizational measures should ensure adequate safety of personal data including protection against unauthorized or illegitimate processing and against unintentional destruction or unintentional damages.

2.1 Physical access control

2.1.1 Physical access to business rooms of Data processor

This means measures preventing unauthorized individuals to enter buildings of Data processor in which personal data are processed. Further measures (like video surveillance, door status monitoring of entrance, exits and escape doors, ...) may be implemented depending on the particular risk classification of the location.

- Definition of authorized people
- Access control System with personalized badge reader, magnetic card or Chip card including access code, personally given keys
- Definition of access rules of external people
- Installation of different security zones including separate access authorizations
- Documentation about granting and revocation of access authorizations
- Intrusion detection system with transmission of alarm signal to a permanent guarded security control center or to the police office
- Restrictive key allocation
- Visitors stays only accompanied by associates of the Data processor
- Obligation to carry identity cards

2.1.2 Physical access to data centers of Data processor

Additional implemented measures to prevent unauthorized individuals to enter data centers of Data processor in which personal data are processed. Depending on the risk classification of the respective Bosch server room, further security measures (such as video surveillance) may be implemented.

- Logging of access to server rooms (automatically by access control system or by designed lists)
- Door status monitoring for server room
- Automatic door pull-in device for entrance and exit in server rooms
- Stays of external companies / technicians in server rooms only under the constant supervision of employees of the contractor

2.1.3 Logical access control

This means measures to prevent unauthorized individuals using the data processing systems and processes.

- Defaults for setting passwords:
  - Minimum length
  - Usage of characters, special characters and numbers
  - No use of trivial passwords
  - Regular change of the password
  - Prohibition of password transfer
  - Rules for storage and transfer in data processing systems
- Defaults of the password management applications to use
- Locking the screen in case of inactivity by time
- Blocking of workstation and/or user accounts after multiple incorrect loggings
- Regular access authorizations for user access to the network of:
  - Employees
  - Externals
- Regular conditional access checks for administrators of:
  - Network and network services
  - Server
  - Risk identified applications
- Isolation of internal networks by setting up firewall systems
- Usage of on Virtual Private Networks (VPN) with

    - User/password as authentification criteria
    - Token as authentification criteria
- Restrictive settings for blocking USB ports
- Use of a central management software for smartphones (for example, for deleting data on the smartphone)

2.1.4 Data access control

This means measures ensuring that individuals authorized to use the data processing systems can only access data within the scope of their access authorization. Measures must be taken that personal data cannot be read, copied, changed or erased without authorization during processing, use and after storage.

- Usage of individualized and user related authorization information
- Differentiated authorization concept based on data and application level (roles)
- Logging of granted authorizations
- Usage of signatures and certificates to prove of author or authentication
- Privacy compliant disposal of data, data carriers and print outs based on the security concept

2.2 Separation control This means measures to ensure that data collected for different purposes are processed separately.

- Logical/technical data separation or internal multi-client capability
- User profiles
- Access authorizations

§3 Measures to ensure integrity

On the one hand, measures for implementing the requirement of integrity are those which are also part of input control, on the other hand, however, those which generally contribute to the protection against unauthorized or illegitimate processing, destruction or unintentional damaging.

3.1 Transfer control

This means measures to ensure that personal data cannot be read, copied, changed or erased without authorization during electronic transmission, transport or storage on data carriers, and that it can be verified and determined at which locations a transfer of personal data by data transmission installations is intended.

- Encryption of data and data carries in regard of their protection requirement with file or hard disk encryption on hard of software base
- Encrypted transmission protocol, especially on public transmission (i.e. ssl, tls)
- Usage of virtual private networks (VPN)
- Usage of logged transportation boxes
- Privacy compliant disposal of data, data carries and print outs based on the security concept
- Electronic signature
- Careful selection of transport staff

3.2 Input control

This means measures to ensure that it can be checked and determined afterwards whether and by whom personal data in data processing systems and applications have been entered, changed or erased.

- Legal form of contracts for the data processing of personal data with subprocessors, including appropriate regulations for control mechanisms
- Procuring self-disclosures from service providers with regard to their implementing the data protection law
- Written confirmation of oral instructions
- Recording and documentation of actions carried out on systems (such as log files)
- Use of logging and logging analysis systems
- Determining authorized persons preparing data carriers and editing data

§4 Measures to ensure availability and resilience

4.1 Availability control

This means measures ensuring that personal data are protected against incidental destruction or loss. These measures must be designed in a way to ensure permanent availability.

- Central purchasing of software and hardware
- Usage of centrally approved and released standard software from secure sources
- Regular back-up-process or mirror hard disks, e.g. RAID-procedure
- Decommissioning of hardware (especially of servers) takes place after testing the data carriers used therein and, if necessary, after backup of the relevant data sets.
- Uninterrupted electricity supply in server rooms
- Separate storage of data sets which were collected for different purposes or which belong to different protection requirement categories
- Multilayer antivirus and firewall architecture
- Emergency planning (emergency plan for security and data protection violations including specific handling instructions)
- Early alert system for fire, water and high temperature in server rooms
- Fire doors
- IT supervision by qualified employees who are trained continuously
- Regular testing of data recovery in accordance with the data protection concept

4.2 Order control

This means measures to ensure that personal data processed by a subprocessor of the contract data processor are processed only in accordance with the processor's instructions and requirements.

- Define criteria for selecting subprocessors (references, certifications, seals of quality)
- Detailed written regulations (contract/agreement) of the assignment relationship and formalization of the entire sequence of the assignment including the use of subprocessors, clear regulations regarding competencies and responsibilities
- Ensuring that contract data processing is controlled and documented
- Contractual agreement with subprocessors to commit both internal and external staff to data secrecy

4.3 Resilience

This includes for example measures, that must already be taken before the contract data processor starts to process the data. In addition, continuous monitoring of the systems is required.

- Load-Balancing
- Penetration tests
- Regular stress tests of the data processing systems

- Define the stress limit for the respective data processing system above the necessary minimum
- Regular training of the staff deployed (both management and other internal or external employees) to act in accordance with the requirements of integrity and confidentiality of data processing (at least once a year)

§5 Availability

In order to ensure recoverability, sufficient safeguards as well as plans for measures are required with which running operations can be recovered in case of disaster scenarios (if necessary, also the basis of the safeguards).

- Back-up concept
- Double IT infrastructure for processes with high availability requirements
- Backup data centre

§6 Procedures for periodical review, assessment and evaluation

Bosch.IO holds the certificates for ISO 9001 and ISO 20000. In addition a regular review, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing shall be carried out in the framework of the implementation of at least one of the following audits:

- Internal audits by the relevant authorities (e.g. auditors, data protection officers, information security officers, process controls through quality management
- External audits by auditors, certification authorities with the following proofs:
    - ISO 27001

Bosch.IO GmbH

- Data Processing Under Commission Agreement – Sub-Processors

Bosch IoT Suite

https://bosch-iot-suite.com/
https://www.bosch-digital.com/

Imprint

Name and address
Bosch.IO GmbH
Ullsteinstrasse 128
12109 Berlin
GERMANY

Board of management
Dr. Andreas Nauerz, Stephan Lampel

Telephone number
+49 30 726112-0

E-mail address
info@bosch.io

Registrations
District Court Charlottenburg, HRB 148411 B

VAT ID No
DE 203273734