BOSCH
Invented for life

Bosch IoT Suite

Privacy leaflet

Version as of 2021.10.15

Europe:
Bosch.IO GmbH
Ullsteinstrasse 128
12109 Berlin / GERMANY
Tel. +49 30 726112-0
Fax +49 30 726112-100
support@bosch.io
https://bosch.io

Copyright notice

© Bosch.IO GmbH, 2021.
All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Table of Contents

© Bosch.IO GmbH

© Bosch.IO GmbH

Chapter 1 – About this document

This document covers protection and privacy topics for personal data related to the Bosch IoT Suite and all its components. It discusses how the Bosch IoT Suite processes personal data within the package services, as well as in interaction with your custom IoT solution including all additional services acting on its behalf.

It is provided as an information source for your solution-specific data protection and data privacy topics. This document is not intended to provide, and should not be relied on for legal advice.

© Bosch.IO GmbH

Chapter 2 – Purpose of the Bosch IoT Suite

The Bosch IoT Suite is a **set of cloud services** for the development of IoT applications.

It enables device manufacturers and administrators to securely address a wide range of IoT use cases, including: device connectivity for heterogeneous landscapes of devices, device-to-cloud and cloud-to-device communication patterns, digital twin representations of your devices, which help to synchronize the physical and the digital world, mass device management, centralized remote management of device fleets, software updates, and many more.

Some of the services can be booked individually, while others are also available as a package.

Available packages:

- Bosch IoT Asset Communication,
  comprising:
  - Bosch IoT Things
  - Bosch IoT Hub
  - Bosch IoT Edge - formerly known as Bosch IoT Suite Gateway Software

- Bosch IoT Device Management,
  comprising:
  - Bosch IoT Rollouts
  - Bosch IoT Manager
  - Bosch IoT Things
  - Bosch IoT Hub
  - Bosch IoT Edge - formerly known as Bosch IoT Suite Gateway Software

Available services in alphabetic order:

- Bosch IoT Edge - formerly known as Bosch IoT Suite Gateway Software
- Bosch IoT Gateway Software - deprecated as of September 2020
- Bosch IoT Hub
- Bosch IoT Insights
- Bosch IoT Manager - only available with the Bosch IoT Suite for Device Management package
- Bosch IoT Remote Manager
- Bosch IoT Rollouts
- Bosch IoT Things

© Bosch.IO GmbH

Chapter 3 – Bosch IoT Asset Communication

3.1 Purpose of Bosch IoT Asset Communication

Bosch IoT Asset Communication - previously known as Bosch IoT Suite for Asset Communication - is a pre-configured service package dedicated to support the scalable and secure ingestion of large volumes of sensor and asset data, and supports the remote control of your assets.

It enables device manufacturers and administrators to securely address a wide range of IoT use cases, including for device connectivity for heterogeneous landscapes of devices, device-to-cloud and cloud-to-device communication patterns, as well as digital twin representations of your devices, which help to synchronize the physical and the digital world.

This package comprises:

- Bosch IoT Things – manages the digital representation, or digital twin, of your physical devices
- Bosch IoT Hub – takes care of device connectivity on a large scale
- Bosch IoT Edge – provides edge computing capabilities - next generation of Bosch IoT Gateway Software

© Bosch.IO GmbH

Chapter 4 – Bosch IoT Device Management

4.1 Purpose of Bosch IoT Device Management

Bosch IoT Device Management is a pre-configured, highly scalable service package dedicated to the centralized remote management of device fleets in diverse IoT scenarios. It enables device manufacturers and administrators to securely address a wide range of device management and maintenance use cases, including sophisticated capabilities for remote deployment of software and firmware components.

This package comprises:

- Bosch IoT Rollouts – manages and controls software and firmware updates for IoT devices
- Bosch IoT Manager – performs centralized remote maintenance and large-scale batch management of IoT devices deployed in the field
- Bosch IoT Things – manages the digital representation, or digital twin, of your physical devices
- Bosch IoT Hub – takes care of device connectivity on a large scale
- Bosch IoT Edge – provides edge computing capabilities - next generation of Bosch IoT Gateway Software

© Bosch.IO GmbH

Chapter 5 – Bosch IoT Edge Agent

5.1 Purpose of Bosch IoT Edge Agent

Bosch IoT Edge is an integrated set of tools and services that work together to connect diverse IoT devices locally and to the cloud, set communication between devices, and develop scalable IoT applications.

Bosch IoT Edge makes it possible to deploy cloud or custom logic on the device so enterprises can get more value from diverse edge assets, process and act on IoT data right on the device and manage devices from the cloud.

5.2 Type of processed personal data

The following types of personal data is processed for Bosch IoT Edge Agent

- Provisioning data:
  - User credentials for the Bosch Suite IoT Hub.
  - User credentials for registries with container images
- IoT equipment data: Personal data from IoT equipment.

For all data that is provided by the IoT solution to the Edge Agent (e.g. personal data within device information) the IoT solution is responsible for data protection and data privacy.

5.3 Purpose of personal data processing

Personal data processed for the following purposes:

- Authentication:
  - Used to apply access control to the Bosch IoT Suite Hub.
  - Used for access to registries with container images
- IoT equipment data transfer to Bosch IoT Suite. Some of this data may contain personal data.

5.4 Personal data processing details and considerations

Bosch IoT Agent

- Provisioning data is used for:
  - Access to Bosch IoT Suite Hub. The provision data is stored in a file. TLS is used for secure transfer.
  - Access to registries with container images. Basic authentication with TLS transfer is used for authorization. Data transfer type depends of registry implementation. Edge Agent supports https with self signed certificates and basic authentication.
- Edge Agent allows connecting a diverse set of IoT devices, gateways or micro controllers and processing and managing data:
  - Personal data send from IoT devices, gateways or micro controllers is transferred by Edge Agent to Bosch IoT Suite without unnecessary processing and data modification. TLS is used for secure transfer.
  - Edge Agent does not store personal data. In case of missing connection to Bosch IoT Suite Hub, messages (which may contain personal information) are buffered.

System logs may contain personal information.

© Bosch.IO GmbH

- Cloud agent system logs are stored in plain text. The number of log files can be configured via a environment property; the default value is five. When the limit is reached the oldest log file is deleted. Log files can also be deleted with the OS commands. Access to logs can be done via the log API and the file system.
- The containers management engine's system logs are stored on demand - they can either be dumped in the standard process's output stream or be persisted. There are three persistent options - in a specified file on the file system, handled by the Linux system logger on the target platform, both at the same time. The log data is provided in plain text. Depending on the persistence configuration, the result files can be deleted accordingly if needed as there is no size limit policy applied by the container management engine itself. If a Linux system logger is used, then all its configurations apply.
- Cloud agent RTOS logs are not stored.

© Bosch.IO GmbH

Chapter 6 – Bosch IoT Edge Services

6.1 Purpose of Bosch IoT Edge

Bosch IoT Edge is an integrated set of tools and services that work together to connect diverse IoT devices locally and to the cloud, set communication between devices, and develop scalable IoT applications.

Bosch IoT Edge makes it possible to deploy cloud or custom logic on the device so enterprises can get more value from diverse edge assets, process and act on IoT data right on the device and manage devices from the cloud.

6.2 Type of processed personal data

The following types of personal data is processed for Bosch IoT Edge Services

- User credentials: Administrative and user access to the gateway
- Azure connection strings: Access from the Edge Services to the Azure Cloud
- Home Connect user credentials: Access from the Edge Services to the Home Connect cloud
- Sensor and device data: Personal data from IoT equipment

For all data that is provided by the IoT solution to the Edge Agent (e.g. personal data within device information) the IoT solution is responsible for data protection and data privacy.

6.3 Purpose of personal data processing

Personal data processed for the following purposes:

Bosch IoT Edge Services

- Access control: Used to apply access control on entities managed by Edge Services.
- Azure connectivity: Used to send device data to the Azure cloud.
- Home Connect connectivity: Used to monitor and control Home Connect devices locally on the Edge Software.
- System operation: Personal data from IoT equipment used for system operation.

6.4 Personal data processing details and considerations

System logs may contain personal information.

- Cloud agent system logs are stored in plain text. The number of log files can be configured via a environment property; the default value is five. When the limit is reached the oldest log file is deleted. Log files can also be deleted with the OS commands. Access to logs can be done via the log API and the file system.
- The containers management engine's system logs are stored on demand - they can either be dumped in the standard process's output stream or be persisted. There are three persistent options - in a specified file on the file system, handled by the Linux system logger on the target platform, both at the same time. The log data is provided in plain text. Depending on the persistence configuration, the result files can be deleted accordingly if needed as there is no size limit policy applied by the container management engine itself. If a Linux system logger is used, then all its configurations apply.
- Cloud agent RTOS logs are not stored.

© Bosch.IO GmbH

Bosch IoT Edge Services

- Access control for Edge Services is used for:
  - Login in Web Admin Console
  - Telnet login to Edge Services Runtime
  - Credentials for access to onvif cameras.

    Passwords are not stored as plain text. Support for HTTPS is implemented for secure credentials transfer.

- Azure Connectivity is used for:
  - Connect the Edge Services with Azure cloud.
  - Send telemetry data for the connected devices.
  - Receive and execute commands from the Azure cloud.

    Connection string is stored in configuration in the internal DB service.

- Home Connect Connectivity is used for:
  - Represent the Home Connect devices locally on the Edge Services.
  - Monitor and control Home Connect devices.

    User and password are stored in configuration in the internal DB service.

- Edge Services allows connecting a diverse set of IoT devices and processing and managing device data:
  - IoT devices exchanges data with Protocol drivers. Communication is via IoT device specific protocols.
  - Protocol driver exchanges data with Device Access module. The Device Access module aims to abstract away the differences between various supported protocols. The Device Access module defines two APIs that enable control over devices in a network based on their functionality instead of the protocol which is used to maintain a connection with them.
  - Protocol drivers and Device Access module may exchange with data Internal or external applications.

    System logs may contain personal information. Access to logs can be done via the log API, Web Admin Console or the device file system. System logs are stored in plain text. The number of log files can be configured via a system property; the default value is five. When the limit is reached the oldest log file is deleted. Log files can also be deleted with the OS commands.

    Backups may contain personal information. Access to backups can be done via device file system. The system does not create backups by default. Backup files can be deleted with the OS commands.

© Bosch.IO GmbH

Chapter 7 – Bosch IoT Gateway Software

7.1 Purpose of Bosch IoT Gateway Software

Bosch IoT Gateway Software allows connecting a diverse set of IoT edge devices, to process and manage device data locally for quick intelligent decisions at the edge, or move normalized data for further cloud analytics. It is hereinafter referred to as "Gateway Software".

7.2 Type of processed personal data

The following types of personal data is processed

- User credentials: Administrative and user access to the gateway
- Sensor and device data: Personal data from IoT equipment

For all data that is provided by the IoT solution to the Gateway Software (e.g. personal data within the device information) the IoT solution is responsible for data protection and data privacy.

7.3 Purpose of personal data processing

Personal data processed for the following purposes:

- Access control: Used to apply access control on entities managed by the Gateway Software.
- System operation: Personal data from IoT equipment used for system operation.

7.4 Personal data processing details and considerations

- Access control for Gateway Software is used for:
    - Login in Web Admin Console
    - Telnet login to Gateway Runtime

Passwords are not stored as plain text. Support for HTTPS is implemented for secure credentials transfer.

- Gateway Software allows connecting a diverse set of IoT devices and processing and managing device data:
    - IoT devices exchange data with Protocol drivers. Communication is via IoT device specific protocols.
    - Protocol driver exchanges data with Device Access module. The Device Access module aims to abstract away the differences between various supported protocols. The Device Access module defines two APIs that enable control over devices in a network based on their functionality instead of the protocol which is used to maintain a connection with them.
    - Device Access module may exchange data Internal or external applications.

© Bosch.IO GmbH

Chapter 8 – Bosch IoT Hub

8.1 Purpose of Bosch IoT Hub

Bosch IoT Hub - a cloud service of Bosch IoT Suite - allows to connect devices through various protocols to applications in the IoT in an easy, secure and reliable manner. As a result, IoT applications are able to retrieve telemetry data from devices (either with or without guaranteed delivery) and send command & control messages to the devices. It is hereinafter referred to as "IoT Hub".

8.2 Type of processed personal data

IoT Hub processes the following types of personal data:

- Identifier of the IoT Hub service instance. The identifier is generated by the Bosch IoT Suite Portal and persisted as part of the subscription process of a customer.
- IP addresses of customers making use of IoT Hub provided interfaces

For all data that is provided by the IoT solution to the IoT Hub (e.g. personal data within device information) the IoT solution is responsible for data protection and data privacy.

8.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Billing of subscriptions for the IoT Hub
    - The service instance identifier is linked to the customer in the Bosch IoT Suite Portal. The billing process that is triggered by the Bosch IoT Suite Portal makes use of the identifier.
- Logging and tracing of interactions with the IoT Hub
    - To support service improvement, prevention of misuse, management of incidents and for security reasons all listed personal data is collected in logging information (see *Type of processed personal data*).

8.4 Personal data processing details and considerations

- Logging information is deleted automatically after a maximum of 14 days, if not sooner. Access to the logs is restricted to the operators of the IoT Hub.
- For access control, the IoT Hub creates credentials for the IoT Hub Device Registry and messaging component. These credentials only identify a user in combination with the service instance identifier
- To fulfill its service the IoT Hub engages service providers to perform functions and process data. Data processing services from the following service providers are used:
    - Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany
    - Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States
    - MongoDB Ltd.,3 Shelbourne Building, Crampton Avenue, Ballsbridge, Dublin 4, Ireland
    - Red Hat Limited, 6700 Cork Airport Business Park, Kinsale Road, Cork, Ireland
    - Confluent, Inc., 899 West Evelyn Avenue, Mountain View, CA 94041
- The IoT Hub stores data in the following locations:
    - Data centers of Robert Bosch GmbH in Stuttgart, Germany
    - Data centers of Amazon Web Services, Inc. in Frankfurt, Germany

© Bosch.IO GmbH

- The IoT solution can access and remove all data which was transmitted by the IoT solution to the IoT Hub using the IoT Hub APIs.
- The IoT solution should consider implementing an audit logging for its changes to access control definitions which potentially affect personal data.

© Bosch.IO GmbH

Chapter 9 – Bosch IoT Insights

9.1 Purpose of Bosch IoT Insights

Bosch IoT Insights - a cloud service of Bosch IoT Suite - is a fully managed cloud service that collects, processes, and stores your IoT data for further analysis. IoT data management provides the basis for optimizing devices and functions and developing new services and solutions.

9.2 Type of processed personal data

The following types of personal data is processed:

- User ID: The user ID is an identifier which uniquely identifies a person and is provided by an identity provider.
- Subscriber information: The subscriber user ID and the email address of a subscriber of the Bosch IoT Insights service.
- Notification receivers: Email addresses and phone numbers where to send notifications about specified data patterns.
- Invitation receivers: User can invite other persons by sending invitation emails to their email address.
- IP address: The internet IP address of IT equipment.

For all data that is provided by your IoT solution to the Bosch IoT Insights service (e.g. personal data within device information) your solution is responsible for data protection and data privacy.

9.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Access control: The *user ID* is used to apply access control on entities managed by the Bosch IoT Insights service. Therefore the user IDs are included by the IoT solution into the access control definitions during the creation and the management of entities. The user ID is submitted to the Bosch IoT Insights service during the authentication of API requests by the IoT solution or by the identity provider.
- Service subscription:
    - The subscriber's *user ID* is captured and stored during the subscription process.
      It is used later for the following purposes:
        - It is used for authenticating this user as someone who is allowed to manage the Bosch IoT Insights service subscription.
        - It can be retrieved via authorized API calls at the solution store.
    - The subscriber's *email address* is captured and stored during the subscription process.
      It can be used for the following purposes:
        - Notifications about maintenance, interruption or general information related to the Bosch IoT Insights service.
        - Invitation to Bosch IoT Insights service related surveys.
- Email or text notifications:
    - Users can configure email addresses and phone numbers to receive data notification messages (email or text messages).
    - These email addresses and phone numbers are used for the single purpose of notification messages when data patterns configured by the users have been identified during data processing.
    - The configuration is stored until a user is removing the notification rule.

© Bosch.IO GmbH

- Email invitations:
    - Existing users can invite third persons to join Bosch IoT Insights solutions by proving their email addresses. Invitations emails are later sent to these addresses.
    - Bosch IoT Insights' access protection stores these email addresses together with an access code, until the invitation is accepted, but never longer than 14 days since submitting the invitation email.
    - It is the responsibility of your IoT solution to align with privacy regulations using this functionality. Bosch IoT Insights supports by full transparency and comprehensive management functionality for invitations in-flight in the user management view for IoT solution managers.
- Logging:
    - To support service improvement, prevention of misuse, and management of incidents and problems, all listed personal data (see *Type of processed personal data*) is collected in logging information.

9.4 Personal data processing details and considerations

- Logging information is deleted automatically after a maximum of 180 days, if not sooner. Access to the logs is restricted to the operators of the Bosch IoT Insights service.
- To fulfill its tasks, the Bosch IoT Insights service engages service providers to perform functions and process data.
  The following service providers are used:
    - Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany
- The Bosch IoT Insights services stores data in the following locations:
    - Data centers of Robert Bosch GmbH in Stuttgart, Germany
- The IoT solution has access to all data ever transmitted to or collected by Bosch IoT Insights. The IoT solution can request deletion or modification of data stored inside the Bosch IoT Insights service at any time.
- The IoT solution can use sophisticated functionality of the Bosch IoT Insights service to define fine-grained access control on all entities managed in the Bosch IoT Insights service. The Bosch IoT Insights service does only allow access to any of these entities according to these access control definitions.
- The IoT solution should consider implementing an audit logging for its changes to access control definitions which potentially affect personal or sensitive data.

© Bosch.IO GmbH

Chapter 10 – Bosch IoT Manager

10.1 Purpose of Bosch IoT Manager

Bosch IoT Manager - a cloud service of Bosch IoT Suite - provides IoT developers and operators with an indispensable set of device management functionalities needed in IoT solutions. These include mass device management, rule-based automation, monitoring, diagnostics and troubleshooting of various connected devices communicating via different protocols. It has inbuilt support for sending commands to edge devices and gateways modeled as digital twins.

10.2 Type of processed personal data

The following types of personal data is processed:

- User ID: The user ID is an identifier that uniquely identifies a person and is provided by an Identity Provider.

For all data that is provided by the IoT Solution to the Bosch IoT Manager Service (e.g. personal data within the device information) the IoT Solution is responsible for data protection and data privacy.

10.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Access control:
    - The User ID is used to apply access control on entities managed by the Bosch IoT Manager Service. Therefore the User IDs are included by the IoT Solution into the access control definitions during the creation and the management of entities. The User ID is submitted to the Bosch IoT Manager Service during the authentication of API requests by the IoT Solution or by the Identity Provider.
- Logging:
    - To support service improvement, prevention of misuse and management of incidents and problems all listed personal data (see *Type of processed personal data*) is collected in logging information.

10.4 Personal data processing details and considerations

Logging information is deleted automatically after 60 days by default and shorter periods for deletion can be configured if necessary. Access to the logs is restricted to the operators of the Bosch IoT Manager Service.

- For access control, the Bosch IoT Manager Service uses the User ID provided by Identity Providers. All supported Identity Providers use pseudonymized IDs and not direct personal data like email address. Thus, the User IDs processed by the Bosch IoT Manager Service are pseudonymized personal data that can only be revealed as personal data in combination with the information that is known to the Identity Provider.
- To fulfill its service the Bosch IoT Manager Service engages service providers to perform functions and process data. The following service providers are used:
    - Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany
    - Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States
- The Bosch IoT Manager Service stores data in the following locations:
    - Data centers of Robert Bosch GmbH in Stuttgart, Germany
    - Data centers of Amazon Web Services, Inc. in Frankfurt, Germany

© Bosch.IO GmbH

- The IoT Solution can delete, modify and access all data that was transmitted by the IoT Solution to the Bosch IoT Manager Service using the Bosch IoT Manager APIs.
- The IoT Solution can use a sophisticated functionality of the Bosch IoT Manager Service to define fine-grained access control on all entities managed in the Bosch IoT Manager Service. The Bosch IoT Manager Service does only allow access to any of these entities according to these access control definitions.

The IoT Solution should consider implementing an audit logging for its changes to access control definitions that potentially affect personal data.

© Bosch.IO GmbH

Chapter 11 – Bosch IoT Remote Manager

11.1 Purpose of Bosch IoT Remote Manager

Bosch IoT Remote Manager - a cloud service of Bosch IoT Suite - provides you with a proven and feature-rich solution to address device management throughout the device life cycle. It supports multiple device management protocols out-of-the-box and various classes of gateways and devices. The Bosch IoT Remote Manager can be used as a fully managed cloud service in different cloud environments or deployed on premise.

11.2 Type of processed personal data

The following types of personal data is processed:

- User ID: The user ID is an identifier that uniquely identifies a person and is provided by an Identity Provider.
- Subscriber information: The subscriber user ID of a subscriber of the Remote Manager Service.

For all data that is provided by the IoT Solution to the Bosch IoT Remote Manager service (e.g. personal data within the device information) the IoT Solution is responsible for data protection and data privacy.

11.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Access control:
    - The User ID is used to apply access control on entities managed by the Bosch IoT Remote Manager service. Therefore the User IDs are included by the IoT Solution into the access control definitions during the creation and the management of entities. The User ID is submitted to the Bosch IoT Remote Manager service during the authentication of API requests by the IoT Solution or by the Identity Provider.
- Service subscription:
    - The subscriber's user ID is captured and stored during the subscription process. It is used for authenticating this user as someone who is allowed to manage the Bosch IoT Remote Manager service subscription.
- Logging:
    - To support service improvement, prevention of misuse and management of incidents and problems all listed personal data (see *Type of processed personal data*) is collected in logging information.

11.4 Personal data processing details and considerations

Logging information is deleted automatically after 60 days by default and shorter periods for deletion can be configured if necessary. Access to the logs is restricted to the operators of the Remote Manager Service.

- For access control, the Bosch IoT Remote Manager service uses the User ID provided by Identity Providers. All supported Identity Providers use pseudonymized IDs and not a direct personal data like email address. Thus, the User IDs processed by the Remote Manager are pseudonymized personal data that can only be revealed as personal data in combination with the information that is known to the Identity Provider.
- To fulfill its service the Bosch IoT Remote Manager service engages service providers to perform functions and process data.
  The following service providers are used:

© Bosch.IO GmbH

  - Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany
  - Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States
- The Bosch IoT Remote Manager service stores data in the following locations:
  - Data centers of Robert Bosch GmbH in Stuttgart, Germany
  - Data centers of Amazon Web Services, Inc. in Frankfurt, Germany
- The IoT Solution can delete, modify and access all data that was transmitted by the IoT Solution to the Bosch IoT Remote Manager service using the Bosch IoT Remote Manager service APIs.
- The IoT Solution can use a sophisticated functionality of the Bosch IoT Remote Manager service to define fine-grained access control on all entities managed in the Bosch IoT Remote Manager service. The Bosch IoT Remote Manager service does only allow access to any of these entities according to these access control definitions.

The IoT solution should consider implementing an audit logging for its changes to access control definitions that potentially affect personal data.

© Bosch.IO GmbH

Chapter 12 – Bosch IoT Rollouts

12.1 Purpose of Bosch IoT Rollouts

Bosch IoT Rollouts - a cloud service of Bosch IoT Suite - provides a secure and reliable means of handling software rollout processes involving a large number of devices. It is hereinafter referred to as "the Rollouts-Service". This domain-independent back-end solution supports the rollout of software updates to constrained edge devices as well as to more powerful controllers and gateways.

12.2 Type of processed personal data

The following types of personal data is processed:

- Tenant ID
- Authentication credentials (E-Mail Address, password): The E-Mail address is used to uniquely identify a person in the Rollouts-Service and is provided by an Identity Provider. It is also used for authorization purposes.
- IP-Address (from the customer of Rollouts) including the IP addresses of devices.

For all data that is provided by the IoT Solution to the Rollouts-Service (e.g. personal data within device information) the IoT Solution is responsible for data protection and data privacy

12.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Authorization:
    - The E-Mail address is used to authorize a user to access specific functionalities in the Rollouts-Service. Therefore the E-Mail address and the specific roles are defined in a user management view in the Rollouts-Service.
- Logging:
    - To support service improvement, prevention of misuse and management of incidents and problems, all listed personal data (see *Type of processed personal data*) is collected in logging information.
- Audit Log
    - For all business entities the E-Mail address of the user, the date and the time is stored for creation and update of the entity.

12.4 Personal data processing details and considerations

- To fulfill its service the Rollouts-Service engages service providers to perform functions and process data.
- The Rollouts-Service stores data in the following locations:
    - Data centers of Robert Bosch GmbH in Stuttgart, Germany
    - Data centers of Amazon Web Services, Inc. in Frankfurt, Germany
- The IoT Solution can delete, modify and access all data which was transmitted by the IoT Solution to the Rollouts-Service using the Rollouts-Service APIs.
- The IoT Solution should consider implementing an audit logging for its changes to access control definitions which potentially affect personal data.

© Bosch.IO GmbH

Chapter 13 – Bosch IoT Things

13.1 Purpose of Bosch IoT Things

Bosch IoT Things - a cloud service of Bosch IoT Suite - enables applications to manage digital twins for their IoT device assets in a simple, convenient, robust, and secure way. Based on the digital twin approach, applications can manage asset data, are notified automatically on all relevant changes of their IoT devices, and share device data and functionality across the layers of their application or with 3rd-party applications. It is hereinafter referred to as "Things-Service".

13.2 Type of processed personal data

The following types of personal data is processed:

- User ID: The user ID is an identifier which uniquely identifies a person and is provided by an Identity Provider.
- Subscriber information: The subscriber user ID and the email address of a subscriber of the Things-Service.
- IP address: The internet IP address of IT equipment.

For all data that is provided by the IoT solution to the Things-Service (e.g. personal data within the device information) the IoT solution is responsible for data protection and data privacy.

13.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Access control: The *user ID* is used to apply access control on entities managed by the Things-Service. Therefore the user IDs are included by the IoT solution into the access control definitions during the creation and the management of entities. The user ID is submitted to the Things-Service during the authentication of API requests by the IoT solution or by the identity provider.
- Service subscription:
    - The subscriber's *user ID* is captured and stored during the subscription process.
      It is used later for the following purposes:
        - It is used for authenticating this user as someone who is allowed to manage the Things-Service subscription.
        - It can be retrieved via authorized API calls at the solution store.
    - The subscriber's *email address* is captured and stored during the subscription process.
      It can be used for the following purposes:
        - Notifications about maintenance, interruption or general information related to the Things-Service.
        - Invitation to Things-Service related surveys.
- Logging:
    - To support service improvement, prevention of misuse and management of incidents and problems, all listed personal data (see *Type of processed personal data*) is collected in logging information.

© Bosch.IO GmbH

13.4 Personal data processing details and considerations

- Logging information is deleted automatically after a maximum of 60 days, if not sooner. Access to the logs is restricted to the operators of the Things-Service.
- For access control the Thing-Service uses the user ID provided by identity providers. All supported identity providers use pseudonymized IDs but not direct personal data like email address. Thus, the user IDs processed by the Things-Service are pseudonymized personal data, which can only be revealed as personal data in combination with the information that is known to the identity provider.
- To fulfill its service the Things-Service engages service providers to perform functions and process data. The following service providers are used:
    - Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany
    - Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States
    - Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338, Luxembourg
    - Microsoft Ireland Operations Ltd., Carmanhall Road, Sandyford Ind Est, Dublin 18, Dublin, Ireland
    - MongoDB Ltd., 3 Shelbourne Building, Crampton Avenue, Ballsbridge, Dublin 4, Ireland
- The Things-Services stores data in the following locations:
    - Data centers of Robert Bosch GmbH in Stuttgart, Germany
    - Data centers of Amazon Web Services EMEA SARL in Frankfurt, Germany
    - Data centers of Microsoft Ireland Operations Ltd. in Netherlands
    - For Beta offerings additionally: data centers of Amazon Web Services, Inc. in the United States of America or data centers of Amazon Web Services EMEA SARL in Ireland and in Germany
- The IoT solution can delete, modify and access all data which was transmitted by the IoT solution to the Things-Service using the Things-Service APIs.
- The IoT solution can use sophisticated functionality of the Things-Service to define fine-grained access control on all entities managed in the Things-Service. The Things-Service does only allow access to any of these entities according to these access control definitions.
- The IoT solution should consider implementing an audit logging for its changes to access control definitions which potentially affect personal data.

© Bosch.IO GmbH

Chapter 14 – Support plans

14.1 Purpose of the support plans

Bosch.IO GmbH, Berlin and Bosch.IO EooD, Sofia offer four different support plans for the Bosch IoT Suite services: Basic, Bronze, Silver, and Gold. The support plans can be ordered via the Bosch IoT Suite portal. A customized Platinum support plan is also available.

14.2 Type of processed personal data

The following types of personal data is processed:

- Name
- Company
- Email address
- Phone number (for Silver support plans and higher)

14.3 Purpose of personal data processing

Personal data is processed for the following purposes:

- Your name is used to address you accordingly during our support process.
- Your company name is used to associate your support requests with the support plans of your company.
- The email address is captured and stored during the support process.
  It can be used for notifications on support request updates.
- Your phone number is used for the support on critical support requests.

14.4 Personal data processing details and considerations

- Support requests are stored in the ticket system for 365 days.
- Billing data is stored as long as the contract is active.

© Bosch.IO GmbH

Chapter 15 – Contact us

Your feedback helps us to continuously improve our products and components. Please send any questions, comments or suggestions for improvement to **support@bosch.io**.

Bosch IoT Suite

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

© Bosch.IO GmbH