Bosch IoT Insights

Privacy Leaflet

Version as of 2020.06.08

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

Table of Contents

Chapter 1 – About this document

This document covers protection and privacy topics for personal data related to Bosch IoT Insights. It discusses how the Bosch IoT Insights service processes personal data within the service, 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.

Chapter 1 – About this document

Chapter 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.

Chapter 2 – Type of processed personal data

Chapter 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.

- 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.

Chapter 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:

    o Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany

- The Bosch IoT Insights services stores data in the following locations:

    o 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.

Chapter 5 – 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**.

Member of the Bosch IoT Suite

https://developer.bosch-iot-suite.com/service/insights/