Bosch Smart Home GmbH

Privacy statement

Bosch Smart Home App

Effective date: 02-05-2024

Contents

1. Bosch respects your privacy....2
2. Controller....2
3. Collection, processing and usage of personal data....2
   3.1 Principles....2
   3.2 Processing purposes and legal bases....12
   3.3 Log files....14
   3.4 Data transfer....14
   3.5 Integration of components provided by other providers....17
      3.5.1 Connection to systems, apps and services of other providers ("Smart Home Cloud")....17
      3.5.2 Voice control....18
      3.5.3 Link to Apple HomeKit....19
      3.5.4 Activating the Matter Bridge....20
   3.6 Functionalities....20
   3.7 Duration of storage, retention periods....20
   3.8 Provision of personal data....21
4. Security....21
5. User rights....22
   5.1 Right to information and access:....22
   5.2 Right to correction and deletion:....22
   5.3 Restriction of data processing:....22
   5.4 Objection to data processing:....22
   5.5 Objection to data processing based on the legal basis of "justified interest":....22
   5.6 Withdrawal of consent:....23
   5.7 Data portability:....23
   5.8 Right of complaint with supervisory authority:....23
6. Responsibility as a user....23

7. Changes to the Data Protection Notice.....24
8. Contact.....24

1. Bosch respects your privacy

The Robert Bosch Smart Home GmbH (hereinafter **"Robert Bosch Smart Home GmbH"** or **"We"** or **"Us"**) welcomes you to our internet pages and mobile applications (together also referred to as **"Online Offers"**). We thank you for your interest in our company and our products.

The protection of your privacy throughout the course of processing personal data as well as the security of all business data is an important concern to us. We process personal data that was gathered during your visit of our Online Offers confidentially and only in accordance with statutory regulations. Data protection and information security are included in our corporate policy.

Children

Our services and offers (in particular website, store, newsletter, apps) are not aimed at children under the age of 16.

2. Controller

The Robert Bosch Smart Home GmbH is the controller responsible for the processing of your data; exceptions are outlined in this data protection notice.

Our contact details are as follows:

Robert Bosch Smart Home GmbH
Schockenriedstr. 17
70565 Stuttgart-Vaihingen
GERMANY
service@bosch-smarthome.com

3. Collection, processing and usage of personal data

3.1 Principles

The Bosch Smart Home App and connected devices (e.g. Smart Home Controller) with their functionalities serve to offer you more comfort in your home. For the execution of the contract, i.e. for the provision of related services (e.g. app functionalities, control of the Smart Home Controller), it is unavoidable that we collect data that can be related to you or another natural person.

Personal data is all information that refers to an identified or identifiable natural person, such as names, addresses, telephone numbers, e-mail addresses, contract, booking and billing data that are an expression of a person's identity. Some of the data we process is not personal data. With regard to this

information, we have neither an interest in identifying a natural person, nor do we have the necessary knowledge or the legally permissible means to establish a personal reference. We may use such non-personal data to improve our products, for example.

We only collect, process and use personal data if we have a legal basis for this or if you have given us your consent in this regard, e.g. as part of a registration. Several legal bases can coexist and allow the processing of personal data.

Processed data includes:

Contract information (e.g. when purchasing from the online shop)

This personal data that is necessary to establish, execute and terminate the contractual relationship with you. This includes in particular name and registration information.

Usage-related and technical information

This is information that is not personal or for which we are unable to establish any personal reference. These are required to enable the operation and use of the Bosch Smart Home System (in particular Smart Home Controller and Smart Home App). In concrete terms, these are:

- Characteristics for identification as user (SHC identification, IP address)
- Information on the beginning, end and scope of use of the Smart Home System
- Device IDs
- Device ID for event notification
- Settings of the app regarding the use of offered services
- Technical information to synchronize and provide current time and updates of your system via our servers
- System data e.g. connected devices and accessories, serial numbers, Smart Home Controller specifications, software versions of the individual components
- System status data, e.g. sensor readings, system time, timer program points, error messages
- History data of the Smart Home System
- Type of terminal used, e.g. smartphone or tablet PC, manufacturer, OS version of the terminal, device ID
- Application usage data e.g. frequency of use, registered crashes, application errors
- Smart Home system data.

Registration via the central SingleKey ID

Login with SingleKey ID, Joint Controllership

You can log in to our services using SingleKey ID.

SingleKey ID was devised by Robert Bosch GmbH for the Bosch Group to provide users with a comprehensive login option on Bosch websites, shops, apps and services. Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany, is responsible for providing SingleKey ID.

Robert Bosch GmbH processes your data for the purposes of "Registration and login with SingleKey ID" and "Overview and management of data and applications with SingleKey ID" in joint responsibility with us. For more information, see: https://singlekey-id.com/data-protection-notice/.

After a one-time registration, you can use SingleKey ID to log in. To do this, you will be forwarded to a login screen at Robert Bosch GmbH. After successful authentication, Robert Bosch GmbH provides us with the necessary personal data (e.g., e-mail address, telephone number, first name, last name, language, country). Your password will not be sent to us.

You can terminate your SingleKey ID user agreement at any time on the SingleKey ID website by deleting your SingleKey ID: https://singlekey-id.com/myprofile/.

Please note that by deleting your SingleKey ID you will lose access to all Bosch websites, shops, apps and services that you used to log in to with your SingleKey ID.

Information to be provided to data subjects in accordance with Art. 13 GDPR – Joint controllers

As the party responsible for SingleKey ID, Robert Bosch GmbH exercises joint responsibility, together with third parties responsible for the application(s) you use, for the processing of your data in accordance with the provisions of the General Data Protection Regulation and national data protection laws. In accordance with Art. 26 of the GDPR (Joint controllers), we have agreed in writing to exercise joint responsibility for data processing. In particular, we have determined and agreed upon the responsibilities and liabilities of the parties involved. For detailed information on individual processing operations, please refer to the data protection notice of Robert Bosch GmbH and the information sheet on data processing available at Data Protection Policy.

Notifications on your smartphone (push notifications)

Android user:

We use the Google Firebase Cloud Messaging service, which is operated by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, in order to send you notifications from your Smart Home system to your mobile end device (push notifications). To this end, a "Google Firebase Cloud Messaging

registration token" is generated during installation and configuration of our app which clearly identifies app installation on your device. The use of Google Firebase Cloud Messaging requires the forwarding of your personal data, where applicable, to states (e.g. USA) in which there may be a lower level of data protection then in the EU.

You can find more information about Google Firebase Cloud Messaging at

https://firebase.google.com/products/cloud-messaging/

and in the Google privacy statement at

https://policies.google.com/privacy?hl=en

iOS users:

We use the Apple Push Notification service, which is operated by Apple Inc. One Apple Park Way, Cupertino, California, USA, 95014, to send you notifications from your Smart Home system (push notification). If you use our app via a mobile end device which can receive push notifications, you can configure the receipt of "push notifications". Here, a pseudonymised device token ID, a unique connection number generated from the device ID, is allocated to your mobile end device. This allows us to address push notifications to you. You can edit notification through push notifications at any time in the app settings under "Settings" > "Push notifications". The use of Apple Push Notification requires the forwarding of your personal data, where applicable, to states (e.g. USA) in which there may be a lower level of data protection then in the EU.

Please see the Apple Inc. data protection conditions https://www.apple.com/legal/privacy/en-ww/ for more information regarding data protection.

You can find more information about the terms of use for the Apple Push Notification service on the Apple Inc. website: https://www.apple.com/legal/internet-services/terms/site.html

Use of analytics tools/customisation

We use Google Analytics Firebase (hereinafter referred to as Google Firebase) for analyses. The provider of Google Analytics Firebase is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. The use of Google Firebase requires the forwarding of your personal data, where applicable, to states (e.g. USA) in which there may be a lower level of data protection then in the EU. Google automatically deletes the data which is communicated to Google Firebase and linked with your user ID after 14 months.

On the one hand, Google Firebase is used for statistics purposes, i.e. without inference of your personal data, in order to keep our service promises and in particular to ensure the best possible availability of services. Furthermore, we use the Google Firebase services in order to send you messages (push notifications) from your Smart Home system.

If you consent to it, we also use Google Firebase to analyse your usage behaviour. To this end, Google Firebase stores some information regarding use processes, operating system, device model or region. You can find a detailed overview of the data collected by Google Firebase and more information about Google Firebase at: https://support.google.com/firebase/answer/6318039?hl=en. You can change your consent through the settings in the app at any time.

We learn how, when or in what manner you use the app and your Smart Home system, for example, through analysis of the information. We thus gain valuable insights for improving our products and services. Based on your usage behaviour, you can receive smart tips or recommendations (in-app messaging) for products, for example, in order to be able to make even better use of your Smart Home system as a result.

We also use the Firebase "Crashlytics" function to stabilise and improve our apps. This function collects data about your device and your use of our apps (device ID and the timestamp when the respective app was launched and when an error occurred). When using Firebase Crashlytics, we process this data in such a way that we are unable to assign it. In its Firebase privacy policy, Google guarantees that this data is not merged with any other data, meaning that no conclusions can be drawn about you personally.

You can find more information about Google Firebase at:

- https://firebase.google.com/
- https://www.firebase.com/terms/privacy-policy.html

Usage of retargeting tools

For the purpose of optimizing our online marketing we use so-called retargeting technologies. This is to design a more interesting Online Offer for you, which is tailored to your needs. To do so, we use the tools listed below.

The usage profiles compiled with the assistance of advertisement cookies or third party advertisement cookies, so-called web beacons (invisible graphics which are also called pixels or counting pixels) or comparable technologies that are not combined with personal data.

The tools are used by the providers to show our users in our Online Offers and in third party offers interest-based advertisements and to control the frequency in which users see certain advertisements. The provider of the respective tool is responsible for the data processing in connection with the tools. The tool providers eventually transfer information to third parties for abovementioned reasons.

When using retargeting tools, we might transfer personal data to recipients located outside the EEA into so-called third countries. With each tool you can find information on the tool provider as well as information on how to object to the data collection by this tool.

Be advised that with regard to tools which use opt out cookies, the opt out function is related to that individual device or browser. In case you use several terminal devices or browsers you must opt out on every device and with every browser used.

Beyond this, you can avoid the forming of usage profiles by generally deactivating cookie usage; for this please refer to the section Deactivate and delete cookies.

Further information on interest-based advertising may be found on the consumer portal http://www.meine-cookies.org. The following link to the portal additionally enables you to view the activation status of certain tools provided by different providers and to object to the collection and processing of your data by these tools: http://www.meine-cookies.org/cookies_verwalten/praeferenzmanager-beta.html.

The option to object to certain tools especially issued by U.S. based providers can be found at the following link: http://www.networkadvertising.org/choices/.

Specifically, we use the following tools:

Name:	Facebook Pixel
Provider:	Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland Together with Facebook, we are responsible for the processing of your personal data within the context of the processing of your personal data on our online offering using Facebook Pixel. In order to define the respective responsibilities for the fulfilment of obligations in accordance with the GDPR for joint processing, we have concluded a shared responsibility agreement with Facebook. You can see the key points of the agreement at any time under the following link: https://www.facebook.com/legal/controller_addendum In particular, this governs what security measures Facebook must take into consideration (https://www.facebook.com/legal/terms/data_security_terms) and how the rights of data subjects can be asserted vis-à-vis Facebook.
Function:	Facebook processes your personal data on the basis of your consent through Facebook Pixel for the generation of campaign reports, conversion tracking, click events and targeted advertising outside our website (retargeting) on the basis of HTTP headers (including IP address, device and browser properties, URL, referrer URL, your person), Pixel-specific data (including Pixel ID and Facebook cookie), click behaviour, optional values (such as conversions, page type), form field names (such as **"email"**, **"address"**, **"quantity"** for purchasing a product or a service) We

	do not receive any personal data concerning you from Facebook, but rather receive anonymised campaign reports about the website target audience and ad performance. You can stop getting interest-based ads from Facebook by changing your advertising preferences on the Facebook website. Alternatively, you can deactivate the use of third-party cookies by visiting the Digital Advertising Alliance opt-out page at http://optout.aboutads.info/?c=2&lang=EN or the http://www.youronlinechoices.com website.
	You can find more information at: https://www.facebook.com/policy

Name:	Google Ads Remarketing Tag
Provider:	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
Function:	Google processes your personal data on the basis of your consent through "Google Ads Remarketing Tag" Pixel for the generation of campaign reports, conversion tracking, click events and targeted advertising outside our website (retargeting) on the basis of URL, referrer URL or inclusion on remarketing lists defined through us, for example. Using the above information, it is also possible for you to be associated with your Google account and included in remarketing lists. We do not receive any personal data concerning you from Google, but rather receive anonymised campaign reports about the target audience and ad performance. You can stop getting interest-based ads from Google by changing your advertising preferences on the Google website at https://www.google.com/settings/ads/onweb#display_optout. Alternatively, you can deactivate the use of third-party cookies by visiting the Network Advertising Initiative opt-out page at http://www.networkadvertising.org/managing/opt_out.asp or managing the use of device identification in the device settings. You can find instructions at https://support.google.com/ads/answer/1660762#mob.
	You can find more information at: https://policies.google.com/privacy

Name:	Amazon Advertising Pixel
Provider:	Amazon Europe Core SARL, Société à responsabilité limitée, 38

	avenue John F. Kennedy, L-1855 Luxembourg
Function:	Amazon processes your personal data on the basis of your consent through Amazon Advertising Pixel for the generation of campaign reports, conversion tracking, click events and targeted advertising outside our website (retargeting). We do not receive any personal data concerning you from Amazon, but rather receive anonymised campaign reports about the website target audience and ad performance. You can stop getting interest-based ads from Amazon by changing your advertising preferences on the Amazon website at https://advertising.amazon.com/legal/ad-preferences?ref=a20m_us_fnav_l_adprf or by visiting the Digital Advertising Alliance opt-out page at http://optout.aboutads.info/?c=2&lang=EN or the http://www.youronlinechoices.com website.
	You can find more information at: https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

Name:	Trade Desk Pixel
Provider:	The Trade Desk Inc., 42 N Chestnut St, Ventura, California, CA – 9300, USA
Function:	The Trade Desk is an advertising technology platform for managing digital marketing campaigns, and processes your personal data on the basis of your consent. To do this, the browsing behaviour of users of our website is analysed using cookies. The Trade Desk collects and processes personal data about users, devices and advertisements, and where these are displayed. This includes, for example, clear cookie identifiers, advertisement identifiers for mobile devices, IP addresses and other information about browsers and devices, such as type, version and settings. You can object or withdraw your consent at any time in the cookie settings of the Consent Management Tool used.
	You can find more information at: https://www.thetradedesk.com/de/privacy

Name:	Media Intelligence Network
Provider:	Amnet GmbH, Alsterufer 3, 20354 Hamburg, Germany

Function:	Media Intelligence Network is a data management platform for the use of retargeting, and processes your personal data on the basis of your consent. Retargeting is a tracking process used in online marketing where your visit to our website is flagged and then, when you visit other websites, advertisements for the products you previously viewed on our website are inserted. The cookie placed by Media Intelligence Network serves to recognise the end device you used. Based on your prior visit to our website, this records your interest in specific products and is used for targeted advertising on other websites. Using the cookie, Media Intelligence Network can establish the so-called conversion rate. This determines the number of persons who have decided to make a purchase after clicking on an advertisement for a promoted offer. You can object or withdraw your consent at any time in the cookie settings of the Consent Management Tool used.
	https://www.mediaintelligence.de/privacy-policyeng.do?appLocale=en

Processing of the advertising identifier / advertising ID

With your consent, we use the so-called "advertising identifier" (IDFA) for devices with the iOS operating system and the so-called advertising ID for those with Android for advertising purposes. These are non-permanent identification numbers for a specific device which are provided by iOS or Android. The data collected through this is not linked with other device-specific information. We use the identification numbers in order to provide you with personalised advertising and to be able to analyse your usage. If you activate the "No ad tracking" option in the iOS settings under "Privacy" – "Apple Advertising" or the "Deactivate interest-based advertising" option on Android under "Google Settings" – "Advertising", then we are only able to take the following measures: Measurement of your interaction with banners by counting the number of times a banner is shown without being clicked on ("frequency capping"), click rate, determination of unique usage ("unique user") and security measures, fraud prevention and troubleshooting. You can delete the IDFA or the advertising ID at any time in the device settings ("Reset Ad ID"); a new identification number will then be generated which is not merged with the previously collected data. We would like to note that you may not be able to use all of the functions of our app if you restrict the use of the respective identification number.

Integration of additional Smart Home products into your Bosch Smart Home System

If you integrate additional Bosch Smart Home products (e.g.'360° Indoor Camera','Eyes Outdoor Camera','Home Connect') into your Bosch Smart Home System, it is usually necessary that you register with the product and/or service provider and accept the additional terms and conditions. It may also be necessary to allow connection to the Bosch Smart Home System in the additional product so that data can be exchanged. Please note that the data exchanged may be personal information.

3.2 Processing purposes and legal bases

We; as well as the service providers commissioned by us process your personal data for the following processing purposes:

Provision of these *service (app and online storage)*

(Legal basis: Fulfillment of contractual obligations).

Customer administration

(Legal basis: Fulfillment of a contractual obligations).

Resolving service disruptions as well as for security reasons

(Legal bases: Fulfillment of contractual obligations or fulfillment of our legal obligations within the scope of data security, and justified interest in resolving service disruptions as well as in ensuring the protection of our offers).

Customer surveys

Product or customer surveys performed via email and/or phone in case you have expressly consented to this

(Legal basis: Consent).

Safeguarding and defending our rights

(Legal basis: Justified interest on our part for safeguarding and defending our rights).

Your request to the Robert Bosch Smart Home GmbH

(Legal basis: Fulfillment of contractual obligations or implementation of pre-contractual measures; justified interest on our part on the consideration and clarification of request directed by our customers.)

Contact based on your call to the customer hotline of the Robert Bosch Smart Home GmbH

Provided that the transmission of personal data and technical data is voluntary, encrypted.

(Legal basis: Justified interest on our part on the elimination of faults and the safety of our offers)

Notifications on your smartphone (push notifications)

Notifications from the Smart Home system

(Legal basis: fulfilment of contractual obligations)

Use of analysis tools

For ensuring the availability of the service and keeping the service promise

(Legal basis: fulfilment of contractual obligations)

Smart tips or recommendations (in-app messaging) for products for app optimisation and improvement of the offerings

(Legal basis: consent)

Location information

For consideration of location-related factors influencing your system or the products used (e.g. sunrise/sunset in shutter control)

(Legal basis: consent)

3.3 Log files

Each time you use the internet, your browser is transmitting certain information which we store in so-called log files.

We save log files for a short period of time to determine service disruptions and for security reasons (e.g., to investigate attack attempts).

3.4 Data transfer

Data processed by Bosch as joint controller

The Bosch Group is made up from numerous companies and is active in the field of household appliances, tools or building technology, for example. These companies are located in Europe (EU and EEA). In order to design the products, services and (online) offers available to you in line with your interests, we employ the following methods:

Analytics

- We want to understand and come to know our customers/prospective customers better. We want to incorporate our insights into our decisions.
- Products, services and offers should work well together and be improved continuously.

Customised marketing

- We want to align our marketing and sales activities better to your interests and needs using analytics.
- The insights we have obtained will be incorporated in our decisions, for example regarding new or improved products, services and offers.

If you use products, services and offers of various companies of the Bosch Group, the respective companies are the primary controllers for the processing of personal data. Please refer to the individual privacy policies to learn more about what happens with your personal data.

For the purpose of designing the products, apps and offers in line with your interests, Bosch Group companies may also use personal data for common purposes. Therefore, we provide you with the following information according to art. 26 (2), clause 2 of the GDPR in this regard:

Who are the companies in this joint controllership?

The following companies of the Bosch Group work together as joint controllers (participating companies):

- Robert Bosch Smart Home GmbH, Schockenriedstr. 17, 70565 Stuttgart-Vaihingen, Germany
- grow platform GmbH, Grönerstraße 9, 71636 Ludwigsburg, Germany
- Bosch Healthcare Solutions GmbH, Stuttgarter Str. 130, 71332 Waiblingen, Germany
- Robert Bosch GmbH, Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Germany

This is why the companies in Bosch Group work together

The companies providing products, services and offers around the field of home and household wish to provide you with a comprehensive offer. In this context, processing your personal data for analysis and customised marketing is of particular importance.

The companies involved have made joint stipulations regarding the joint processing of such data. In a joint agreement, the following material aspects are determined:

Processing:

Use of user data for the purpose of analysis, identification and use of relevant user interactions across legal entities by means of Google Analytics.

Compliance with obligations by: All participating companies

Processing:

- Analysis of relevant cross-company user data (e.g. conversion path data, page views, number of visitors and visits, downloads, reference websites) and provision of relevant information to parties with restricted access ("custom view") by means of Google Analytics.
- Use, preparation and exchange of pseudonymised user data for cross-company analytics and reports (e.g. multi-channel interactions, performance measurements)
- Allocation and bundling of user data in unique digital identities (user) within the Bosch Group and its companies (inside/outside of the EU), (e.g. creating profiles, information on the interaction of the user with and between products, services and offers).

Compliance with obligations by: All participating companies

Processing:

Use of data for the analysis of your interaction with products, services and offers for further processing for marketing purposes by means of Google Analytics and Marketing Pixel

Compliance with obligations by: All participating companies

Processing:

- Analysis and development of marketing-relevant target groups; provisions of the user data relevant for the purpose of carrying out marketing activities to parties with restricted access ("custom view") be means of Google Analytics
- Exchange and use of marketing-relevant target groups for the performance of marketing activities by means of implemented Marketing Pixels and retargeting. The marketing activities can be performed by individual participating companies but also by several companies for cross-company marketing purposes.

Compliance with obligations by: All participating companies

Your rights as a data subject

The participating companies have mutually agreed on their competence and responsibilities. Regarding your rights as a data subject arising from the GDPR, the following applies:

- If the participating companies are deemed joint controllers, they shall make available the information regarding transparency of the processing according to the legal requirements. In this regard, the companies exchange the required information among one another.
- The companies shall inform each other immediately if you assert your rights as a data subject. The companies shall provide each other with the required information.
- As a data subject, you can assert your rights as a data subject towards any of the parties. Your request will be forwarded to the responsible participating company internally.

Data transfer to other controllers

Your personal data is principally forwarded to other controllers only when required for the fulfillment of a contract, in the case where we or the third party have a legitimate interest in the transfer, or when your consent has been given. Particulars on the legal bases can be found in the Section "3.2 Processing purposes and legal bases". Third parties may also be other companies of the Bosch group. When data is transferred to third parties based on a justified interest, this is explained in this data protection notice.

Additionally, data may be transferred to other controllers when we are obliged to do so due to statutory regulations or enforceable administrative or judicial orders.

Use of service providers

We involve external service providers with tasks such as sales and marketing services, contract management, payment handling, programming, data hosting and hotline services. All service providers are obliged to maintain confidentiality and to comply to the statutory provisions. Service providers may also be companies within or outside of the Bosch group which may be located within or outside the EU or the European Economic Area (EEA). In such a case, we will ensure an adequate level of data protection by means of agreements.

3.5 Integration of components provided by other providers

3.5.1 Connection to systems, apps and services of other providers ("Smart Home Cloud")

With Bosch Smart Home you have control over your data. If you wish, you can share your device data with partner companies (hereinafter referred to as partners) and control your Bosch Smart Home products via their systems, apps or services.

This requires that you grant access to your Bosch Smart Home System and the generated data to the respective partner. These data may be personal data.

If you want to allow the partner to access and control the system, activate the function "Mirror system in cloud" in the Bosch app. The data generated by your system or products will then be mirrored in the Bosch Smart Home Cloud. You can then allow specific partners to access and control your system and products. This is done in the following way: You open the partner's site and agree to link and control your smart home products and transfer data. If you control your smart home product through partner sites, we may need to transmit data that may be personally identifiable (e.g. room or device names).

If you have given your consent, access and control remains possible until its deactivation. If you want to end a partner’s access, you can withdraw data authorisation using "Change authorisations" on the Bosch Smart Home Cloud website. If you no longer want to use mirroring of your data on the Bosch Smart Home Cloud in general, then you can deactivate this in the Bosch Smart Home app. Your mirrored data will then be erased. If you want to give a partner access to your system again, you can activate the "Bosch Smart Home Cloud" function again in the Bosch Smart Home app.

Please note:

If you want to withdraw authorisation for a specific partner, proceed as follows: You withdraw the partner’s authorisation through this app and thus remove the link between the partner account and SingleKey ID so that it can no longer control your Bosch products and services.

Furthermore, you should withdraw the partner’s authorisation on the Bosch Smart Home Cloud website. ("More" > "Partners" > "Smart Home Cloud" > "Manage permissions"). You thus ensure that not only is the account link removed, but also the authorisation is withdrawn.

If you remove the system in the Cloud through the Bosch Smart Home System app, your mirrored data will be erased. However, the authorisations which you have granted to partners remain so that you can continue to use them in the future. If you do not want this, then you can first withdraw the partners’ authorisations separately.

Insofar as you grant authorizations to a partner, you instruct us to make your data available to this partner. By activating the cloud and granting consent on the partner site, you make it clear that you agree to the transfer or exchange of your data with the partner and, if applicable, to control your Bosch Smart Home System. You or the partner are responsible for the associated data processing by the partner. The data processing carried out by the partner is subject to its terms of use and data protection regulations. Bosch has no influence on these. You will find more detailed information on data processing in the partner's terms of use and data protection regulations.

3.5.2 Voice control

Use of Amazon Alexa

You have the option of controlling your Smart Home products via Amazon Alexa voice commands. To do so, you have to connect your Smart Home products to Amazon Alexa. If you control your Smart Home product via Alexa, you may have to transmit personal data via Amazon to your Smart Home product and vice-versa.

If you give voice commands to Amazon Alexa in order to control Smart Home products or retrieve information from your Smart Home product, voice data are transmitted to Amazon and used by Amazon to perform the service. These data may be personal data. By connecting your Amazon Alexa and Bosch accounts and by activating skills, you make it plain that the Smart Home product installed on your system is to be controlled via Amazon Alexa and that information is to be output via Amazon Alexa and you instruct us to exchange data with Amazon Alexa in this context. You and Amazon are responsible for the data processing that is entailed. The data processing performed by Amazon is subject to Amazon's usage and privacy protection terms. Bosch has no influence on them. Please refer to Amazon's usage and privacy protection terms with regard to Alexa for more information on data processing by Amazon.

Use of Google Assistant or Google Home

You have the option of controlling your Smart Home products via Google Assistant or Google Home voice commands. To do so, you have to connect your Smart Home products to Google Assistant or Google Home. If you control your

Smart Home product via Google Assistant or Google Home, you may have to transmit personal data via Google to your Smart Home product and vice-versa.

If you give voice commands to Google Assistant or Google Home in order to control Smart Home products or retrieve information from your Smart Home product, voice data are transmitted to Google and used by Google to perform the service. These data may be personal data. By connecting your Google Assistant or Google Home and Bosch accounts and by using Google Actions, you make it plain that the Smart Home product installed on your system is to be controlled via Google Assistant or Google Home and that information is to be output via Google Assistant or Google Home and you instruct us to exchange data with Google Assistant or Google Home in this context. You and Google are responsible for the data processing that is entailed. The data processing performed by Google is subject to Google's usage and privacy protection terms. Bosch has no influence on them. Please refer to Google Assistant's or Google Home's usage and privacy protection terms with regard to Google for more information on data processing by Google.

3.5.3 Link to Apple HomeKit

If you wish, you can connect your Bosch Smart Home products to Apple HomeKit (hereinafter referred to as Apple) and control them via Apple’s Home app, Siri voice commands or third-party apps compatible with Apple HomeKit (hereinafter referred to as third-party app).

This requires that you allow Apple access to your Smart Home System, that the generated data is made available to Apple, and that data is processed by Apple to control your system. This data may be personal.

If you want to control your Smart Home System via Apple, activate the corresponding function in the Bosch app. Then connect the Smart Home System to Apple by making the other settings in Apple’s app ‘’Home.’’

Insofar as you grant authorization to Apple, you instruct us to provide Apple with your data to control the Smart Home System. By activating Apple and granting consent in Apple’s Home app, you make it clear that you agree to the transfer or exchange of your data with Apple and, if applicable, to control your Bosch Smart Home products via an app from Apple or a third-party provider.

You, Apple or the third-party provider are responsible if data is processed by Apple. The data processing carried out by Apple or the third-party provider is subject to its terms of use and data protection regulations. Bosch has no influence on them. For more information on data processing, please refer to the terms of use and data protection regulations of Apple or the third-party provider.

The option to access and control via Apple will remain available until its deactivation. If you want to end the control via Apple and the associated data exchange, you can remove the link to Apple in the Bosch app.

3.5.4 Activating the Matter Bridge

If you can activate the "Matter Bridge" function in the settings, the following applies:

You can control selected devices that are compatible with the Bosch Smart Home system as part of a system based on the Matter standard (Matter system). This requires information from the device to be exchanged with the Matter system via the Smart Home controller. Please note that you can only control standard functions of your devices via the Matter system.

3.6 Functionalities

Consideration of location-related aspects

You have the option of better adapting your system to the local conditions. For example, allowing the detection of location data makes it possible for the local times for sunrise and sunset to be considered in controlling your shutters. You may change your consent to the determination of your location at any point in your setting. If you do not wish your location to be determined by the system, a generally determined geographic central point in the respective country is used instead.

3.7 Duration of storage, retention periods

As a general rule, we cannot allocate the data generated by your Smart Home system, that is to say, we cannot link it to a person. In particular, for us, there is no connection between you, your used devices, and the data you generate. It is not necessary to erase your data. The data is generally only retained for as long as you use your system.

Your data on the system and its use can be allocated if you

- have consented to a personal analysis for marketing purposes, for instance, or
- require our support, contact our service team, and provide data about your system.

The following applies to personal data: principally, we store personal data for as long as it is necessary to render our offers and connected services or for as long as we have a justified interest in storing the data. In all other cases we erase your personal data with the exception of data we are obliged to store for the fulfilment of legal obligations or are entitled to pursue our legal claims.

When you perform a reset, all technical characteristics for authorisation are deleted. The device is reset to factory settings and the data is erased accordingly. If you terminate the integration of partner services, for instance, the technical characteristics for authorisation are deleted. Also when you deactivate

services or functions, the processing is ended and the corresponding data is erased.

3.8 Provision of personal data

In order for us to conduct a business relationship and/or to provide services (e.g. fulfilment of contact, support queries), it may be necessary for you to provide us with your personal data. If you do not wish to do this, this may lead to us being unable to perform the corresponding service.

4. Security

Our employees and the companies providing services on our behalf, are obliged to confidentiality and to compliance with the applicable data protection laws.

We take all necessary technical and organizational measures to ensure an appropriate level of security and to protect your data that are administrated by us especially from the risks of unintended or unlawful destruction, manipulation, loss, change or unauthorized disclosure or unauthorized access.

5. User rights

To enforce your rights, please use the details provided in the 8. Contact section. In doing so, please ensure that an unambiguous identification of your person is possible.

5.1 Right to information and access:

You have the right to obtain confirmation from us about whether or not your personal data is being processed, and, if this is the case, access to your personal data.

5.2 Right to correction and deletion:

You have the right to obtain the rectification of inaccurate personal data concerning yourself without undue delay from us. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

This does not apply to data which is necessary for billing or accounting purposes or which is subject to a statutory retention period. If access to such data is not required, however, its processing is restricted (see the following).

5.3 Restriction of data processing:

You can demand - as far as the legal requirements are fulfilled - that we restrict the processing of your data.

5.4 Objection to data processing:

You have the right to object to data processing by us at any time. We will no longer process the personal data unless we demonstrate compliance with legal requirements to provide provable reasons for the further processing which are beyond your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

5.5 Objection to data processing based on the legal basis of "justified interest":

In addition, you have the right to object to the processing of your personal data any time, insofar as this is based on the legal basis of justified interest. We will then terminate the processing of your data, unless we demonstrate compelling legitimate grounds according to legal requirements for the processing, which override your rights.

5.6 Withdrawal of consent:

In case you consented to the processing of your data, you have the right to object this consent (8. Contact)with immediate effect. The legality of data processing prior to your revocation remains unchanged. In addition, processing may continue to be permitted on the basis of another legal bases.

5.7 Data portability:

You are entitled to receive data that you have provided to us in a structured, commonly used and machine-readable format or – if technically feasible – to demand that we transfer those data to a third party.

This does not apply if a transfer affects the rights and freedoms of another person.

5.8 Right of complaint with supervisory authority:

You have the right to lodge a complaint with a supervisory authority. You can appeal to the supervisory authority which is responsible for your place of residence or your state or to the supervisory authority responsible for us. This is:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Address: Lautenschlagerstraße 20, 70173 Stuttgart, GERMANY

Postal address: P.O. Box 10 29 32, 70025 Stuttgart, GERMANY

Phone: +49 711/615541-0

Fax: +49 711/615541-15

Email: poststelle@lfdi.bwl.de

6. Responsibility as a user

The Smart Home system and Smart Home devices are intended for use in a private domestic environment. They are intended for private use only.

You bear responsibility for the lawful use of the devices and services and for compliance with the applicable legal provisions in the place of use. Laws in your country may stipulate permitted purposes, installation locations, selection of image sections and storage duration of the video sequences in particular. At the same time, you can contribute to the privacy-friendly use of the product as follows:

- Limit it to your private area. Avoid recording your neighbours' property or public areas outside your property and/or your home. Do not expose others to monitoring pressure which is perceived personally.
- Where necessary, inform other people (e.g. people living or staying in the monitored areas) about the use of your product in an appropriate manner, for example with a notice or a camera symbol which is recognisable in good time. Obtain any consent which may be required.
- Only activate voice transmission and/or voice recording if this is permitted in your place of use and if this is required for your legitimate purpose.
- Delete clips if you no longer need them for the intended purpose.
- Regularly check the monitored areas for changes and make any changes which may be necessary.

7. Changes to the Data Protection Notice

As far as the circumstances of the data processing change, we can adjust the privacy policy. Furthermore, we reserve the right to change our security and data protection measures if this is required due to technical development. In such cases, we will amend our data protection notice accordingly. Please therefore, notice the current version of our data protection notice, as this is subject to change.

8. Contact

If you wish to contact us, for example in connection with the processing of personal data or for the exercise of your user rights, please find us at the address stated in the “2. Controller“ section.

If you want to unsubscribe from a newsletter, you can click on the corresponding unsubscribe link in the newsletter or tell us your request via the contact options mentioned in the “2. Controller“ section.

To assert your data subject requests and notification of data protection incidents please use following link: https://www.bkms-system.net/bosch-datenschutz

For suggestions and complaints regarding the processing of your personal data, we recommend contacting our data protection officer:

Datenschutzbeauftragter
Abteilung Informationssicherheit und Datenschutz (C/ISP)
Robert Bosch GmbH
Postfach 30 02 20
70442 Stuttgart
DEUTSCHLAND

or

Email: DPO@bosch.com