

Privacy Policy Sennheiser Smart Control (hereinafter called "App")
(Version March 4th, 2024)

Prior to download, installation and use, please carefully read the following notes and information on how and for what purpose your data is collected and processed.

Further information can be obtained by reading the privacy policy of the platform/app store from which you download the app. Under the heading of "Data Protection", "Privacy Policy" or a similar heading addressing the topic of data protection, this will inform you about which data is directly collected there and how it is processed. As the provider of the app, Sennheiser has no influence on data processing by the platform providers.

The responsible party for the processing of personal data is the publisher and operator of the app indicated on the platform/in the app store.

Further information on your data protection rights (right to information pursuant to Art. 15 GDPR, right to rectification pursuant to Art. 16 GDPR, right to erasure pursuant to Art. 17 GDPR, right to restriction of processing pursuant to Art. 18 GDPR, right to data portability pursuant to Art. 20 GDPR, right to object pursuant to Art. 21 GDPR, right to lodge a complaint with a supervisory authority pursuant to Art. 77 GDPR) as well as the contact details of our data protection officer can be found in our privacy policy at <https://www.sennheiser-hearing.com/privacy>.

The processing of your personal data complies, according to your country, with local law requirements, including the Swiss Federal Data Protection Act ("FDPA"), the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") and including the Cyber Security Law of People's Republic of China (PRC) and the Personal Information Protection Law of PRC.

If you have any questions regarding the processing of your data, please contact us directly:

Sonova Consumer Hearing GmbH, Am Labor 1, 30900 Wedemark, Germany, send us an email to privacy@sonova.com or contact our customer support team <https://www.sennheiser-hearing.com/contact>.

Notes on data collection and processing and on firmware updates

The following information is required to establish a connection to a device: Bluetooth address (for Android), access rights to location information of the device (for Android), BLE UUID (for iOS). This data is required for the operation of the product on your device and is not transferred to us or companies commissioned by us and is not processed.

The use of the app on Android devices mandatorily requires the activation of location services to enable the functioning of the app and the operation of your Sennheiser product. The connection to your Sennheiser product is established using Bluetooth Low Energy Scan (BLE Scan) technology, which requires access to the location services of your device. If you do not enable location services, the app cannot connect to your

Sennheiser product. Sennheiser does not process location information for any other purpose.

Using the “Sennheiser Smart Control” app, you can update the product’s firmware free of charge via an Internet connection.

It is possible to register for push notifications (optional opt-in) in the event of newly provided firmware of a Sennheiser product connected to the app. If this function is used, then a PNS handle (Platform Notification Service) corresponding to the operating system (Android or iOS) is installed on the device. This PNS handle does not contain any personal data. This setting can be revoked at any time.

Updating the firmware requires your consent. If the device on which the app is installed is connected to the Internet, the following data is transferred to our servers and processed there in order to provide and transfer appropriate firmware updates: hardware identifier, hardware revision number, firmware version of the product, operating system type (Android, iOS) and version, version of the app. The data is only used for the purpose of providing and transferring firmware updates (legal basis Art. 6 para. 1 lit. b GDPR) and is not stored permanently.

If you do not want this data to be transferred and processed, do not establish an Internet connection.

Installation and use:

Sonova Consumer Hearing GmbH as the publisher of the app itself does not collect or process any personal usage data. Therefore, there is also no transfer of personal data by Sonova Consumer Hearing GmbH to third parties.

Certain usage data and crash reports are processed using Google Firebase (a service of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland), subject to your consent. Such processing is necessary to provide a continuously improved app and is only done in anonymous form to determine statistical characteristics regarding app usage, app distribution and identification of error causes, as well as for the purpose of providing and maintaining the app and improving the features of the app. At no time can a reference be made to a specific person. In particular, the following information is processed:

Frequency, type, and duration of app use

Settings made on the device such as equalizer, Active Noise Cancellation (ANC) mode or other device-specific settings.

Type of device used with the app

Operating system and version number

Number of firmware updates performed

Error reports in case of app crash

supplementary only when used with products of the Sennheiser wireless Bluetooth headset series:

Operating time, number of usage cycles

Duration of use of the various ANC programs and number of switchovers
Accumulated charging time and number of charging cycles
Total duration in phone mode and number of times it was switched to phone mode
Accumulated connection time of two devices and number of connections of an additional device
Duration of audio playback and number of times playback was started
Crashes

The Google Firebase Analytics and Crashlytics services used by the app automatically collect anonymized data. A complete overview of all possible collectable events can be viewed via the following link:

<https://support.google.com/firebase/answer/6317485> .

The events relevant to our app are limited only to the first chapter ‘Automatically collected events’, whereby in particular all mentioned events in connection with advertising (ads), in-app purchases (in-app buy), subscriptions (subscriptions) are not relevant as these functions are not supported by the app.

If Google Firebase transfers your data to third countries outside the European Economic Area (“EEA”), the standard data protection clauses issued by the European Commission apply in conjunction with appropriate technical and organizational safeguards.

By selecting the appropriate setting in the “Privacy” section of the app menu, you can consent to the processing of your anonymized data by Google Firebase or prevent it at any time by revoking your consent with future effect.

Personalized data in case of User Registration (Sennheiser account)

If you log in to the Smart Control app using your SCH user account or create a user account in the app, the following data is processed automatically to provide you with personalized settings and features (Art. 6 para. 1 lit. b GDPR):

user-created profiles and settings such as: EQ presets, sound zones & sound personalization profile

This data is stored to ensure the functionality of the features on multiple devices and after reinstallation. You can prevent the storage of this data in the app settings at any time, but then you will no longer be able to access the data from other devices and benefit from personalized settings. In this case, your personalized profiles and settings remain stored only locally on your device and are not accessible to us. The data stored locally on the device will be deleted when you delete or uninstall the app.

Deleting your user account will also delete all associated profiles and settings from our systems.

We use Microsoft Azure (provider: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA) to store data associated with the user account. In order to maintain the level of data protection granted by the European General Data Protection Regulation (GDPR), Sennheiser has concluded the standard data protection clauses or “standard contractual clauses” issued by the European Commission in

conjunction with appropriate technical and organizational safeguards with the provider. If your country of origin entered during registration belongs to the European Economic Area (“EEA”), your data will be stored in data centers within the EEA. For users from China, Azure services is provided by 21Vianet Group, Inc. For users from other regions, data center locations will be determined in accordance with relevant data localization requirements.

Feedback on the app

You will have the opportunity to give your feedback on the app in order to help us improve our products and service. A pop-up will appear asking you to rate your satisfaction, and you will have the option of giving your feedback or refusing giving it. The data processing, based on our consent (Art. 6 para. 1 lit. a GDPR), will only take place if you respond, and involves the collection of the following data:

product feedback (self-reported by the user)

model name

unique Sennheiser Smart Control app installation ID

IP address

To collect those data, we use a tool provided by the third-party Qualtrics LLC (USA). The pop-up will only appear once when using the app.

Using MOMENTUM Sport devices

Sennheiser Momentum Sport has the capability to transmit Heart Rate, Body Temperature, and, where applicable, system ID, through the BLE standard protocol and corresponding service, from sensors located in the user's ear-canal. This data is not stored on the Sennheiser Momentum Sport’s device but is consistently broadcasted to any connected device capable of receiving such information. It is important to clarify that Sonova Consumer Hearing GmbH neither accesses nor stores any of this personal data. However, it is incumbent upon manufacturers of non- Sonova Consumer Hearing GmbH products to determine whether any processing of personal data occurs, for which they assume sole responsibility, acting as independent data controllers.

Sent from [Outlook for Android](#)