Data privacy information Telekom Deutschland GmbH („Telekom“) for Magenta SmartHome App

Telekom Deutschland GmbH attaches great importance to protecting your personal data. We always inform you what personal data we collect, how your data is used, and how you can influence the process.

What data is recorded, how is it used, and how long is it stored?
When registering:
To register for the app, you will have to enter your e-mail address and passphrase of your Qivicon account. Alternatively, you have the possibility of using your Telekom Login to register. You can find more information about registering at QIVICON at www.qivicon.com/datenschutz. With regard to the Telekom Login, you can find further information at www.telekom.de/datenschutzhinweise. This data is required for contract performance (Art. 6 (1) b GDPR) and is stored on our servers until end of contract.

When using the app:
The following data are collected by us and saved until the contract ends or until they are automatically deleted:

- The Magenta SmartHome App saves the configuration data for your Magenta SmartHome System (sensors, actuators, Smart Home gateway) on the Smart Home gateway in your home (Art. 6 para. 1 b GDPR). This includes:
  - Current sensor and actuator statuses
  - Configuration data for switching groups/automations
  - Default temperatures
  - The personal timing program (heating)
  - Events (e.g. window open, low battery)
  - Notifications of events
- The mobile phone number data entered by you is saved on the Smart Home gateway for the SMS functionality (Art. 6 para. 1 a DSGVO). (see also Contacts/Address Book)
- For the use of service offers from a cooperation partner (e.g. the provision of an emergency assistance service by an insurance company), it may be necessary to provide and disclose data that is required exclusively for the provision of this service (Art. 6 para. 1 b GDPR).

  - Configuration of the service offer from a cooperation partner
  Configuration is possible via the service provider's own configuration pages within the Magenta SmartHome App. The data you enter there is processed directly by the cooperation partner as soon as these configuration pages are closed. This data is neither stored in the Magenta SmartHome App nor forwarded to Telekom Deutschland GmbH. The assignment of the cooperation partner's data with data of your SmartHome system is conducted via an identifier, a so-called hash value. This identifier is only related to the data you enter in the configuration pages, but not to your Telekom contract data. The data privacy policy of the cooperation partner applies to the data entered in the configuration pages.

  - Use of the service offer from a cooperation partner If the forwarding of messages from your Magenta SmartHome system to the cooperation partner is necessary for the provision of services by the cooperation partner, the transmission is encrypted and contains the identifier described under IV) a) and the information necessary for the provision of the service.
  The data protection provisions of the cooperation partner apply for the forwarded data.
- If you cancel Magenta SmartHome with Deutsche Telekom, the data on the QIVICON platform will not be deleted automatically. You can initiate the deletion directly via QIVICON Support, which registers your QIVICON account. For details, please refer to the data privacy policy of QIVICON (Art. 6 para. 1 b GDPR). When you use the app, our servers temporarily record the IP address of your device and other technical characteristics, such as the requested content (Art. 6 para. 1 b GDPR).
  In this app, you have the option to dictate the text in addition to the keyboard input. Voice input (Google) or dictation (Apple) is a functionality provided by the operating system of our app. When used, the speech is processed by a third party (e.g. Apple or Google) as the responsible party and the result is delivered to our app and output in the input field. You can find details on the functionality and how you can enable or disable use from the respective operating system manufacturer.

Connection with other systems/devices:
Using Magenta SmartHome with a voice control system (e.g. Amazon Echo, Google Assistant, Sonos One) allows voice control of your Magenta SmartHome. Within this process, the voice commands are analyzed, evaluated and executed by the respective third party. For partners, in this case Telekom, the respective third party provides an interface that allows us to provide our own functions. This allows us to specifically connect and use your systems with the voice control of the respective third party. When using a voice control system, the voice is processed by a third party (e.g. Amazon or Google) as the responsible party. The data protection provisions of the respective third party apply.

This functionality is only provided if you explicitly activate Magenta SmartHome in your account of the respective third party and link your SmartHome account with this service there (Art. 6 para. 1 a GDPR). Only through this link is it possible for certain commands to be evaluated by the respective third party and sent to your Smart Home gateway for execution.

When linking, all data regarding names and IDs of your scenes, devices and rooms is transferred to and saved by the respective third party in order to be able to use them in voice commands. No other data, such as account or personal data from your Magenta SmartHome, will be saved or transmitted to the respective third party. Please note that voice control by other persons may also occur, as different voices are not recognized.

Usage surveys / feedback from customers with Get Feedback:
This app uses the service provided by SurveyMonkey Europe UC, 2 Shelbourne Buildings, 2nd Floor, Shelbourne Road, Ballsbridge, Dublin 4, Ireland (Notice: SurveyMonkey has taken over the previous Usabilla company and its tool of the same name) for customer surveys. App ratings and your feedback can be surveyed (Art. 6 (1) a GDPR). Our customers' opinions and improvement suggestions crucially help us improve our app. Only anonymous information is processed and there is no way of tracing the sender. Personal data or personally identifiable data is not transferred at any time. We store and analyze the data for a period of 24 months.

Two different methods can be used to conduct the surveys:

I. The feedback button in the app menu. You can use this button or the sub-item in the menu at any time to provide us with your feedback. No data is transferred unless you use this function.

II. An active feedback survey can also be displayed in the app. You can reject this survey or cancel it at any time. Answers are only sent once you have completed the survey.

Miscellaneous:
You can find more information about how the Smart Home gateway and the QIVICON platform exchange data and how you can view, change or delete personal data at QIVICON at www.qivicon.com.
Additional personal data, such as your name, address or e-mail address, will not be collected unless you provide this information voluntarily.

Authorizations
For the app to work on your device, it needs access to various functions and data on the device. You need to grant certain authorizations to do so (Art. 6 (1) a GDPR).

The authorizations are programmed differently by the various manufacturers. Individual authorizations may, e.g. be combined in authorization categories, and you can only grant consent to the authorization category as a whole.

Please remember that if you withhold consent for one or a number of authorizations, you may not have access to the full range of functions offered by our app.

If you have granted authorizations, we will only use them to the extent described below:

Location data
The app requires information about your current location for the following purpose:

- For use of the weather service.
  The location data is used by the Magenta SmartHome app to retrieve weather information from the weather service provider. In addition, the data is used to send information about weather events (e.g. severe weather) for this location to your smartphone via push notification. For this purpose, the current location data of your smartphone can be used if desired. For this, the location function must be turned on once for this process. Alternatively, you can enter the city or zip code manually.
- For use of the 'Coming Home' function
  The 'Coming Home' function can be used to automate arrival at home. You can set a radius around your Smart Home gateway of between 100 m and 1,000 m. If you enter this 'Home Zone', the app automatically switches your Smart Home into the 'At Home' state. This means that you do not have to change the status manually. For this, the location detection of your smartphone must be permanently activated. The location is then used to compare your position with the selected radius and automatically set the status of your Smart Home. For this purpose, it is necessary to determine the location even if the Magenta SmartHome App is in the background or closed. The Magenta SmartHome App transmits and saves the location on the Smart Home gateway. The location is also saved in the Magenta SmartHome App, but the entered data can be viewed, changed or deleted at any time in the Magenta SmartHome App. Furthermore, no data, such as movement data, is passed on to the Smart Home gateway, nor is it stored. This data is processed exclusively on the operating system of your smartphone.
  Users can define their location in the "Settings / Location" menu. The current location is only recorded when using the Magenta SmartHome app if you have expressly consented to this. This is done either when the app is installed or later via the smartphone settings. Both functions can also be deactivated in the Magenta SmartHome App. The general consent can be revoked at any time for the future in the settings of your smartphone.

Contacts / Address book
The app requires access to the contacts and the address book for the following purpose.

In addition to push notifications, the Magenta SmartHome App, if so configured by you, sends SMS messages to up to three Telekom Deutschland GmbH mobile numbers when an alarm is triggered.

When using the SMS function, the responsibility for the use of the mobile numbers lies exclusively with you if you enter the numbers in the Magenta SmartHome app. You are thus also responsible for the consent or possible revocation of the respective persons for the use of their mobile phone numbers. You can delete the numbers entered at any time.

Since dispatch only works for Telekom Deutschland GmbH mobile numbers, regular checks are carried out to determine whether the numbers entered belong to the Telekom Deutschland GmbH number range. If it is determined that the mobile number is no longer a Telekom Deutschland GmbH mobile number, no more SMS will be sent to the number in question and it will be deleted automatically. You should therefore ensure that the SMS recipients tell you when they change mobile phone provider, so that you are always informed which of your specified numbers actually receives an SMS.

To avoid abuse, the number of SMS that can be sent per month is limited to 1,000. If this limit is reached, we will send you a push notification informing you that the maximum number of SMS for the respective month has been reached and no more SMS can be sent. In addition, we will inform you about this in the Magenta SmartHome app.

To make it easier to select the contacts to be informed, the Magenta SmartHome App provides you with the option of searching for the relevant people in the contact data and selecting them. For this to be possible, the app requires permission to access the contact data. The Magenta SmartHome App does not change any contact data, nor does it access the contacts automatically.

Further information on the SMS function can be found in the FAQs

Wi-Fi connection information
The app needs access to the Wi-Fi status for the following purposes:

To be able to inform you automatically if an Internet connection is available and to be able to alert you that you can switch to "offline" control if the Internet connection is not established or cannot be established. To do this, it is necessary to be able to query the state of the network and search for Wi-Fi connections/home networks.

This ensures that you are able to control and use your Magenta SmartHome devices in your own home network even when no Internet connection is available.

Information on Bluetooth connection
The app requires access to the Bluetooth connection for the following purposes:

Consent to access the Bluetooth connection is only required in connection with the use of a smartwatch. Currently, the Apple Watch series is supported. In combination with an Apple Watch, you can switch the status of your home control between “At Home” and “Away” or control scenes (favorites) that you have set up yourself. In addition, the Apple Watch notifies you about alarms and warnings.

Access to the Bluetooth interface is necessary in order to transfer this data to the smartwatch and the control information from the Apple Watch to the smartphone.

Camera, microphone, USB, photos, videos, message content, etc.
The app requires access to the memory for the following purpose:

Access to the memory is only required if you want to save camera recordings from the cloud to your SmartHome App and actively select the save function in the app. The SmartHome App does not otherwise access the memory of your smartphone.

The app requires access to the microphone for the following purpose: When using Magenta SmartHome, you have the option of using the integrated voice function to dictate voice inputs to switch devices or scenes.

Ignore battery power optimization
The app requires access to the battery saving mode for the following purpose:

Access is necessary because when the energy saving mode is activated, the app functions are restricted and the energy consumption is minimized. If this access is not granted, this also means that push notifications are no longer sent or processed. You would therefore no longer be informed about important events such as alarm notifications

Other authorizations
The app requires access to "Control vibration alarm", "Disable sleep mode" and "Retrieve data from the Internet" for the following purpose:

- Control vibration alarm: To give you the option of being alerted to push notifications and alerts through vibration as well.
- Disable sleep mode/Foreground service: To "wake up" the smartphone from sleep mode and to be able to inform you at any time in case of an alarm.
- Retrieve data from the Internet: Internet access is required to be able to control the Magenta SmartHome functions remotely.
- Wi-Fi Multicast: To be able to find the gateway (Homebase/Speedport) via UPnP in the network.
- Run at startup: To counteract occasional loss of the set geofence, it is also reset when the app is started.
- View network connections: Is required to determine whether a network connection exists in order to provide the service reliably.
- Full network access: Is necessary not only to have access to the SmartHome devices and services outside the home, but also to enable local access to the gateway and to be able to control the home when there is no Internet connection.
- Receive boot completed: Is needed to restore important services after a reboot of the phone, e.g. Geofence.
- Request ignore battery optimization. To significantly increase the reliability for push notification delivery, the app should be excluded from the power saving options of the mobile device

Will my usage habits be evaluated, e.g. for advertising purposes or tracking?
Explanations and definitions:
We want you to enjoy using our app and take advantage of our products and services. We have an economic interest in ensuring this is the case. We analyze your usage habits on the basis of anonymized or pseudonymized data so that you can find the products that interest you and so that we can make our app user-friendly. We or companies commissioned by us to process data create usage profiles to the extent permitted by law. This information cannot be traced back to you directly. The following information is intended to provide you with general information on the various purposes of processing data. You can change your data privacy settings to consent to

the use of the tool, or reject their use accordingly. Tools that are strictly necessary to provide the app cannot be rejected (see explanation at 1. above).

Tag management (strictly necessary)
Tag management is used to manage tracking tools in apps. A tag is set for each page to do this. Based on the tag, the system can determine which tracking tools should be used for this page. Tag management can be used to specifically control tracking so that the tools are only used where appropriate.

Market research/Reach measurement (opt-in)
Reach measurement aims to statistically determine an app's use intensity and the number of users as well as obtaining comparable figures for all the connected services. Market research is designed to learn more about the target groups that use services or applications and view advertisements. Individual users are not identified at any time. Your identity is always protected.

Strictly necessary tools
These tools are strictly necessary to enable you to navigate the pages and use essential functions. They enable basic functions, such as order processing in the online shop and access to secured areas of the app. They also serve the purpose of performing an anonymous analysis of usage patterns, which we use to continuously develop and improve our app for you. The legal basis for these tools is Art. 6 (1) b GDPR respectively for third Countries Art. 49 (1) b GDPR respectively for third Countries Art. 49 (1) b GDPR.

Company	Purpose	Storage period	Country of processing
Telekom	Login	For the session or 6 months (remain registered)	Germany
Telekom	Push notifications	7 days	Germany
MoEngage	In-app notifications	24 months	USA

Optional usage of tools
These tools are activated when you use additional functions, e.g. the chat. The possible functions are explained in section 1 of this data privacy information. The legal basis for these tools is Art. 6 (1) a GDPR respectively for third Countries Art. 49 (1) a GDPR.

Company	Purpose	Storage period	Country of processing
Survey Monkey (formerly Usabilla)	Usage surveys	24 months	Ireland
MoEngage	Push messages	24 months	USA

Analysis tools
These tools help us to improve our understanding of how our apps are used.

Analysis tools allow for the collection of usage and identification data by the original provider or third party providers and their compilation into pseudonymous usage profiles. We use analysis tools, e.g. to determine the number of individual users of an app, to collect technical data if the app has crashed, and to analyze the app's usage patterns and user interactions on the basis of anonymous and pseudonymous information. This information cannot be traced back to a person. The legal basis for these tools is Art. 6 (1) a GDPR respectively for third Countries Art. 49 (1) a GDPR.

Company	Purpose	Storage period	Country of processing
Adjust	Customized design	28 days	Germany
MoEngage	Customized design	24 months	USA
Telekom	Demand-driven design to improve the usage experience	24 months	Germany

You can change the settings in the app under "Settings" > "Privacy

Marketing tools
These tools are used to show you promotional contents, e.g. in the form of push notifications.

Marketing tools make it possible to show interesting advertising contents and measure the effectiveness of the campaigns. This is done exclusively within this app and not with other advertising partners (third-party providers). It is therefore not possible to draw conclusions about a person. By using marketing tools, you help us to issue content that is relevant to you, such as an offer for a smoke detector or door/window contact that allows you to use further functions in the app. The legal basis for these tools is Art. 6 (1a) GDPR or, in the case of third countries, Art. 49 (1a) GDPR.

Company	Purpose	Storage period	Country of processing
MoEngage	In-app notifications, Push notification	28 days	USA

You can change the settings in the app under "Settings" > "Privacy"

Services by other companies (independent third-party providers)
Some pages of our app feature services from third-party providers, who bear the sole responsibility for their services. This involves the use of tools to capture data while the app is used and transmission of the data to the respective third-party provider. Some of the data may be transmitted for Deutsche Telekom's own purposes. The legal basis for these tools is Art. 6 (1) a GDPR respectively for third countries Art. 49 (1) a GDPR. The scope, purpose and legal basis on which further processing is carried out for the third party's own purposes can be found in the third party's data privacy information. Information about these independent third party providers can be found in the following.

Google
We use Google Maps on some of our pages (e.g. the Shop Finder) to display maps, location information and for route planning purposes. Google Maps is operated by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. When you visit one of these pages, the embedded Google Maps function will transmit your IP address directly to Google servers and stored there. You can obtain information and opt out at any time from data processing by Google at http://www.google.de/intl/de/policies/privacy.

Where can I find the information that is important to me?
This **data privacy information** provides an overview of the items which apply to Deutsche Telekom processing your data in this app.

Further information, including information on data protection in general and in specific products, is available at https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection and https://www.telekom.com/en/deutsche-telekom/privacy-policy-1744.

Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy at Deutsche Telekom?
Responsible for data is Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn. If you have any queries, please contact our Customer Services department or the Group Data Privacy Officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany datenschutz@telekom.de.

What rights do I have?
You have the right

a) To request **information** on the categories of personal data concerned, the purposes of the processing, any recipients of the data, and the envisaged storage period (Art.15GDPR);

b) To request that incorrect or incomplete data be **rectified** or supplemented (Article16GDPR);

c) To **withdraw** consent at any time with effect for the future (Art.7(3)GDPR);

d) To **object** to the processing of data on the grounds of legitimate interests, for reasons relating to your particular situation (Article 21(1)GDPR);

e) To request the **deletion** of data in certain cases under Art. 17 GDPR – especially if the data is no longer necessary in relation to the purposes for which it was collected or is unlawfully processed, or you withdraw your consent according to (c) above or object according to (d) above;

f) To demand, under certain circumstances, the **restriction** of data where erasure is not possible or the erasure obligation is disputed (Art.18GDPR);

g) To **data portability,** i.e. you can receive the data that you provided to us in a commonly used and machine-readable format such as CSV, and can, where necessary, transfer the data to others (Art.20GDPR);

h) To **file a complaint** with the competent **supervisory authority** regarding data processing (for telecommunications contracts: the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)); for any other matters: State Commissioner for Data Protection and Freedom of Information, North Rhine-Westphalia (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen

Who does Deutsche Telekom pass my data on to?
To **processors**, i.e. companies we engage to process data within the legally defined scope, Article 28 GDPR (service providers, agents). In this case, Deutsche Telekom also remains responsible for protecting your data. We engage companies particularly in the following areas: IT, sales, marketing, finance, consulting, customer services, HR, logistics, and printing.

To **cooperation partners** who, on their own responsibility, provide services for you or in conjunction with your Deutsche Telekom contract. This is the case if you order services of these partners from us, if you consent to the involvement of the partner, or if we involve the partner on the basis of legal permission.

Owing to legal obligations: In certain cases, we are legally obliged to transfer certain data to a state authority that requests it. Example: Upon presentation of a court order, we are obliged under Section 101 of the German Copyright Act (UrhG) to provide the owners of copyrights/ancillary copyrights with information about customers who have allegedly offered copyrighted works via Internet file sharing services.

Where is my data processed?
Your data will be processed in Germany and other European countries. If, in exceptional cases, your data is processed in countries outside the European Union (in so-called third countries), this will take place

a) if you have expressly consented to this (Article 49 (1) a GDPR). In most countries outside the EU, the level of data protection does not meet EU standards. This concerns in particular comprehensive monitoring and control rights of state authorities, e.g. in the USA, which disproportionately interfere with the data protection of European citizens,

b) or to the extent necessary for our service provision to you (Article 49 (1) b GDPR),

c) or to the extent required by law (Article 49 (1) c GDPR).

Furthermore, your data will only be processed in third countries if certain measures ensure a suitable level of data protection (e.g. the EU Commission's adequacy decision or suitable guarantees, Art. 44 et seq. GDPR).

This privacy information was last updated 05/10/2023