Data privacy information Telekom Deutschland GmbH („Telekom“) for MagentaZuhause 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, use your Telekom Login. You can find further information regarding the Telekom Login at www.telekom.de/datenschutzhinweise. These details are required for contract fulfillment (Art. 6 para. 1 b GDPR) and are saved on our servers until the contract ends.

If you cancel MagentaZuhause App with Deutsche Telekom, your Telekom Login data will not be deleted automatically. For details, please refer to the Privacy Policy of Telekom Login (Art. 6 para. 1 b GDPR)

**When using the app:**

The following data are recorded by us and are saved until your MagentaZuhause App contract ends or until you delete the data yourself.

- For the personal form of address, your name (taken from Telekom Login) is processed locally by the MagentaZuhause App. For simplified configuration of notifications in the alarm system, your e-mail address (taken from Telekom Login) is processed locally by the MagentaZuhause App.
- We save your Telekom customer number and e-mail address for contract fulfillment. We take this automatically from your Telekom Login.
- For SMS notification, the mobile phone numbers you entered are saved in the MagentaZuhause App system (Art. 6 para. 1 a DSGVO). (see also Contacts / Address Book)

When you use the app, our servers will temporarily record your device's IP address and other technical details, such as the requested content (Art. 6 (1) b GDPR)

**Use of household management:**

The MagentaZuhause App uses Telekom's central household management.

In the MagentaZuhause App, the contract partner can invite other users to join their household. The invitation is sent via e-mail. Other users use their own Telekom Login and must accept the invitation to join the household. The e-mail address are deleted automatically after 14 days at the latest.

The following data are processed within the scope of household management:

- Name of the household selected by the contract partner. Initially preset with their last name, obtained from the Telekom Login.
- Display name selected by the contract partner. Initially preset with their first name, obtained from the Telekom Login.
- The avatar (profile picture) provided optionally by the contract partner or other user.
- E-mail addresses entered by the contract partner to invite other users to join the household. The e-mail address are deleted automatically after 14 days at the latest.

**Use of smarthome functions:**

The following data are recorded by us and are saved until your MagentaZuhause App contract ends or until you delete the data yourself.

The MagentaZuhause App stores configuration and runtime data in the MagentaZuhause App system (Art. 6 (1) b GDPR). This includes:

- Current sensor and actuator statuses (e.g. window open)
- General device information (e.g. low battery)
- Configuration data for switching groups and automations
- History data (e.g. alarm events, executed automations)

If you cancel MagentaZuhause App with Deutsche Telekom, the data on the QIVICON platform will not be deleted automatically. You can initiate the deletion directly via QIVICON Support, who will register your account from QIVICON. For details, please refer to the data privacy information of QIVICON. (Art. 6 para. 1 b GDPR)

**Use of location functions:**

The MagentaZuhause App allows the recording of locations (geofences). This allows the user to make their presence at any location relevant to them (e.g. home, workplace, school, etc.) usable in the system, for example for home automation.

A geofence defines a perimeter around a specific location. Mobile devices can determine whether they are within such a geofence. The recording of precise and location-independent positioning data does not take place in this way.

The following location data is processed as part of the Presence function:

- User-set address and designation of locations (geofences), as well as their determined geo-coordinates (GPS).
- Presence at a location (geofence) detected by end devices.

**Sharing one's own location**

The MagentaZuhause App system allows participants of a household to share their locations with each other. Only the presence and absence at the locations set up by the user are shared, as the exact GPS coordinates of the individual participants are not recorded.

Each participant decides for themselves whether their device determines their own location, i.e. presence in a previously set up geofence, thus making it available for automations. Each participant decides for themselves whether their location should be shared with other participants of the household.

Each participant can prevent both the location detection and the sharing of the location at any time on their end device.

**Use of the Home Network Check:**

To make the Telekom network even better for you, the following data is collected, stored and processed by the app during the “Home Network Check” function.

**Measurements regarding the quality of the connection:**

- Measured data rate in upload and download
- Number of hops between measurement client and measurement server
- Measured package runtime
- Measured jitter
- Measured number of lost packages
- DSL line downstream / upstream (current and maximum possible value

**Context information:**

- Smartphone technical data
- Remaining smartphone battery time
- Operating system
- Type of smartphone movement
- Router firmware version
- Location
- Precision of the determined location
- Date/Time
- Connection technology (2G, 3G, 4G, 5G, Wi-Fi)
- Booked broadband of the connection
- Signal strength Wi-Fi (RSSI of the Wi-Fi hotspot) or mobile network (RSSI and signal-to-noise ratio SNR)
- Link speed of the Wi-Fi hotspot
- Encryption method of the Wi-Fi hotspot
- Frequency of the Wi-Fi hotspot
- User rating of Internet connection
- Recommendations for the users based on the result of measuring the Internet connection

**Identifiers:**

- App installation ID
- Router ID (manufacturer, series number, model name)
- Local IP address
- Test ID
- SSID of the Wi-Fi hotspot
Use of the Magenta voice assistant:
Voice data are used to control the services called up with the Smart Speaker. By voice data we mean audible recordings of your spoken sentences and written, machine-readable texts obtained from the spoken sentences.

We delete your voice data within 90 days after the service is terminated. You can also delete voice data yourself in the conversation history of the MagentaZuhause App. For the sole purpose of further developing and improving the voice service and to ensure and optimize the positive customer experience on an ongoing basis, we process this data for up to 2 years during the term of the service. After the 2 years, we delete these data.

We process your voice data automatically with the use of modern software. However, for the continuous training of the software, voice data must also be analyzed “manually” by our voice experts, e.g. by listening to voice commands and comparing them with the transcribed text. This helps to identify voice recognition errors and avoid them in future. User can accept or object to analysis by our voice experts within the MagentaZuhause App before first use and change their consent any time in the data privacy settings. You can also delete individual or all voice data within 90 days using the corresponding function in the app.

Use in the app:
The voice assistant in the app is manually set to the active state by the user via a button. The recording can be stopped and canceled at any time by closing the voice assistant. Until the recording is stopped, conversations and sounds in the environment can also be recorded. To counter this risk, we have included the following functions for you:
- You can subsequently delete the accidentally recorded voice data in the conversation history of the MagentaZuhause App.
- The recording is stopped automatically after 8 seconds if it has not recognized a voice command.
- The maximum recording length of a recognized voice command is 9 seconds.

The legal basis for processing voice data is Art. 6(1)(b) GDPR in conjunction with Art. 6(1)(f) GDPR. The recording of voice data is initiated manually by the user. As soon as there is no speaking, the recording is stopped. Furthermore, the recording can be stopped and canceled by the user at any time.

“Share” function
In the voice history and in the lists (shopping list, to-do list), you have the option to share individual contents via the sharing function of your device, i.e. to make them available to other people. In this case, the forwarded information is no longer processed by Telekom, but by the provider of the respective application. From this point on, the processing of your data is governed exclusively by the data protection provisions of the provider of the third-party application you have selected. Telekom accepts no responsibility or liability whatsoever for the legally compliant processing of your data by third-party providers!

Ask Magenta
You can use the “Ask Magenta” function to retrieve various information about your own existing Telekom contracts (date of contract renewal, mobile billing amount, fixed-line network billing amount, amount of remaining/consumed data volume).

Use on the Magenta Smart Speaker:
The voice command “Hello Magenta” (activation command) switches the Magenta Smart Speaker, if present and connected, from the passive to the active state. Passive means that no voice data is recorded. This only happens when the Magenta Smart Speaker is switched into the active state by stating the activation command. In individual cases, however, it cannot be completely ruled out that the Magenta Smart Speaker inadvertently perceives the activation command and unintentionally switches from the passive to the active state. Other conversations and sounds in the environment are then recorded until the Smart Speaker automatically returns to passive mode. To counter this risk, we have included the following functions for you:
- You can deactivate the microphone using the switch on the device, e.g. prior to sensitive conversations.
- You can subsequently delete the accidentally recorded voice data in the conversation history of the MagentaZuhause App.
- The device stops the recording automatically after 8 seconds if it has not recognized a voice command.
- The maximum recording length of a recognized voice command is 9 seconds.

The legal basis for processing voice data is Art. 6 para. 1 b) GDPR in conjunction with Art. 6 para. 1 f) GDPR. This applies to anyone who willingly uses the Magenta Smart Speaker, not only to the owner of the Magenta Smart Speaker in the narrower sense. The recording of what is said is initiated by the voice command “Hello Magenta”. As soon as there is no speaking, the recording is stopped. For any co-users or room users, it is therefore important that they know what activates the Magenta Smart Speaker (activation command), that the device may be recording, and how to stop the recording again. With this knowledge, those affected can exercise their right of privacy accordingly. The owner of the Smart Speaker must ensure that they inform co-users in the aforementioned sense.

Connection with other voice assistants
As a customer, you can also use the voice services of other providers and companies (e.g. Amazon) via the Magenta Smart Speaker. We would like to point out that for the duration of the use of another, non-Telekom voice service, you will leave the Telekom environment from a technical and legal perspective. This means that your data will no longer be processed by Telekom during this period, but by the provider of the selected service. Consequently, the processing of your data during this time is governed exclusively by the providers of the provider you have selected. Telekom does not assume any guarantee or liability for the legally compliant processing of your data by other voice service providers! If you return to the “Magenta Voice Assistant”, the processing of your data will, of course, again be governed by Telekom's data privacy policy described herein.

Connection with other systems and service partners
In order to enable the various services that you as a customer can access via the Telekom Smart Speaker, some of our cooperation partners require the complete machine-written sentences that you have previously spoken into the Magenta Voice Assistant (transcribed voice data) for technical reasons. The processing and transmission of these sentences to our cooperation partners is based on Art. 6 b) GDPR for these cases, as they are necessary for the technical realization and implementation of the service you have selected. As this does not apply to all cooperation partners, the partners for whom the transfer of complete machine-written sentences is necessary are listed below:
- Knowledge function: Retresco GmbH
- MagentaTV function: Telekom Deutschland GmbH

Customer Service support:
You have the option of contacting Customer Service via the app. For this, it is necessary to enable Customer Service access to your data generated under points 1 a) to c). You can do this by clicking/tapping the corresponding button in „Contact“ in the section „Customer Support“ in tab „More“ in the App and by transmitting the diagnostic code displayed in the app to Customer Service.

This consent can be withdrawn in the same way at any time and expires automatically after 28 days at the latest. Access to the generated and saved data is solely for the purpose of troubleshooting.

Connection with other systems:
The MagentaZuhause App system can be linked to a variety of other systems. External systems are generally not linked automatically but must be activated by the user. The link to and between the following Telekom products is established automatically the first time you log in to the MagentaZuhause App:
- MagentaZuhause
- Magenta Sprachassistent
- MagentaTV
- HomeOS
Due to their different integration and functionality, different systems are subject to different data protection requirements, which are explained below:

Connection of Telekom routers
The Telekom Home Experience (Beta) system allows the configuration of Telekom routers (e.g. Speedport Smart 4, Speedport Pro). The router is detected automatically based on the Telekom login without having to re-enter the credentials or the device password. HomeOS provides a protected interface for this purpose which, among other things, allows to change the Wi-Fi password and the Wi-Fi name (SSID) of the router, but not to read out existing passwords.

Device connections
The MagentaZuhause App system offers the possibility to link devices from cooperation partners (e.g. Philips Hue, Sonos, Logitech) and to control them via an application. For this, the partners provide an interface that allows third parties to control devices or read out device information. Some devices require a connection to the cloud or platform of the respective device partner. In most cases, this requires prior registration with the respective device provider. Depending on the provider, it may now be necessary for you to authenticate yourself to MagentaZuhause App by entering the access data of the portal to the cloud of the device provider during the connection so that an exchange of information is possible. Please check which information is transmitted in detail in each individual case before you agree to the data transmission. The links to the privacy policies of the individual device providers are listed at the end of the paragraph.

Camera services
Using MagentaZuhause App with a device provider for camera monitoring systems (e.g. Logitech Circle, Netatmo Security) allows you to monitor your home with the MagentaZuhause App. The connection allows you to use cameras of different types in one app and, for example, trigger a recording when your MagentaZuhause App system detects an alarm situation. Image data and video files, as well as video streams, are retrieved directly from the partner's servers. Through this process, the partner comes into possession of the IP address of the displaying or playing device, among other things. The extent to which this data is used can be found in the partner's privacy policy.

When installing and operating cameras, please ensure that you do not violate the personal rights of third parties (e.g. unlawful recording of neighbors).

Audio services
Using MagentaZuhause App with a device provider for audio output (e.g. Sonos) allows you to provide sound to your home with the MagentaZuhause App. The connection allows you to use speakers of different types in one app and, for example, select tracks when you are playing music. Some systems (e.g. Logitech Circle, Netatmo Security) can also be automated with your MagentaZuhause App system.

Image data and audio files, as well as audio streams, are retrieved directly from the partner's servers. Through this process, the partner comes into possession of the IP address of the displaying or playing device, among other things. The extent to which this data is used can be found in the partner's privacy policy.

Data privacy policies of our device partners
- Magenta Sprachassistent [pdf] (Telekom)
- MagentaTV [pdf] (Telekom)
- QIVICON Plattform [pdf] (Telekom)
- D-Link Corporation
- Lifx
- Logitech
- Netatmo
- Nuqi
- Philips Hue
- QIVICON Plattform [pdf] (Telekom)
- VIIZ

User surveys/customer feedback 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:
- 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.
- 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:
Information as to how the Smart Home gateway (Speedport) and the QIVICON platform exchange data, and how you can view, change or delete personal data at QIVICON can be found at www.qivicon.com.

Additional personal data, e.g. your address, is not collected unless you provide this information voluntarily.

Apart from inputting data using the keyboard you can also use this app to dictate text. Voice input (Google) or dictation function (Apple) is a functionality which our app's operating system provides. During use, a third party processes the speech (e.g., Apple or Google) as processor and delivers the result to our app, entering it into the input field. Contact your specific operating system vendor for details on the functionality, and how you can switch on/off usage.

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 on your current location for the purpose of connecting devices with your own Wi-Fi and the MagentaZuhause App system.

Permission to access location data is requested when accessing Bluetooth because Bluetooth communication could be used to determine the location.

Permission to access location data is requested when accessing the device's current Wi-Fi network because reading the current SSID could be used to determine the location.

Permission to access location data is requested when using the Magenta Voice Assistant but is not mandatory if access to the current location is denied, individual functions cannot be used in full. This applies, for example, to the local weather or tips for places in the vicinity.

Permission to access location data is requested when the user enters geofences. Geofences are locations with a radius that can be captured by the user for the purpose of location-based automation.

Permission to access location data in the background, i.e. while the app is not actively being used, is required to detect the user entering or leaving the geofences created by the user. Precise location data (exact geo-coordinates of the cell phone) are not collected. Data collection is limited to entering and leaving user-defined locations.

Contacts/Address book
The App does not require access to the contacts/address book. Mobile phone numbers have to be entered manually by the user.

In addition to push notifications, the MagentaZuhause App sends SMS messages to Telekom Deutschland GmbH mobile numbers when an alarm is triggered, if you have configured it in such a way. When using the SMS function, you are solely responsible for the use of the mobile numbers when you enter the mobile numbers in the MagentaZuhause App. You are thus also responsible for the consent or possible consent revocation of the respective SMS recipients for the use of the respective mobile phone number. You can delete the mobile numbers entered at any time. You should therefore ensure that you receive information from your SMS recipients when they change their mobile service provider, so that you are always informed which of your specified numbers actually receives an SMS.

Internet communication
The app requires access to the Internet via Wi-Fi or mobile data network for the purpose of being able to retrieve and display data from the...
MagentaZuhause App system, as well as being able to send control commands to actuators connected to your MagentaZuhause App system. In order to provide appropriate assistance, the status of the connection (online, channel, speed) is used.

**Wi-Fi**
The app requires access to the Wi-Fi network (local network) for the following purposes: During startup of the Smart Home gateway (Speedport), the SmartHome control panel is searched for in the local network via UPnP and the MagentaZuhause App functionality is activated.

**Bluetooth**
The app requires access to Bluetooth for the purpose of connecting devices with the user's own Wi-Fi and the MagentaZuhause App system. After the Wi-Fi connection of the device has been established, further communication with the device takes place via the cloud and Wi-Fi. The Bluetooth connection with devices is terminated after startup.

In the background, the MagentaZuhause App continuously uses the Bluetooth connection to search for other connectable devices. The search is currently limited exclusively to supported devices from the manufacturers Wiz and D-Link.

**Microphone**
The app requires access to the microphone for the following purposes:

For implementing the intercom function in the live stream from supporting connected services. Market research is designed to learn more about your navigation within the app. The system displays content or information that matches your profile.

The app requires access to files and media for the following purposes:

To allow the user to take a photo (avatar) for their own profile within the household.

*Does the app send push notifications?*
Push notifications are messages that the app sends to your device and that are displayed with top priority. This app uses push notifications by default, provided you have given your consent during the app installation or the first time you use the app (Art. 6 (1) a GDPR).

You may revoke your consent at any time. To do so, uncheck the box next to “Receive notifications” in this app’s main menu under “Notifications”.

**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 information. This information cannot cause you to be identified. These tools help us to understand your usage habits and improve the app accordingly.

**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.

**Improvement of the app’s technical quality (opt-in)**
To measure the quality of the app programming or to register crashes and causes, the program sequence and usage habits are analyzed. Individual users are not identified.

**Profiles for a user-gear presentation of the app (opt-in)**
To continuously improve the app, we also use the events captured in the event tracking. These retrace your navigation within the app. Analyzing this navigation allows us to obtain insights about the app’s usage patterns, which in turn allows us to detect any problematic user experiences and improve the app accordingly. Individual users are not identified at any time.

**Profiles for personalized recommendations (opt-in)**
Deutsche Telekom provides you with personalized action and click recommendations for offerings, services or products. With the help of service providers, we create a pseudonymous profile about the events you have triggered in the app (e.g. the services and pages you have accessed) and allocating categories to the profile. The system displays content or information that matches your profile.

**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 user 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.

<table>
<thead>
<tr>
<th>Company</th>
<th>Purpose</th>
<th>Storage period</th>
<th>Country of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telekom</td>
<td>Login</td>
<td>For the session or 6 months (stay logged-in)</td>
<td>Germany</td>
</tr>
<tr>
<td>Telekom</td>
<td>Push messages</td>
<td>For the session</td>
<td>Germany</td>
</tr>
<tr>
<td>SurveyMonkey (formerly Usability)</td>
<td>User surveys</td>
<td>24 months</td>
<td>Ireland</td>
</tr>
<tr>
<td>Telekom</td>
<td>Push messages</td>
<td>12 months</td>
<td>Germany</td>
</tr>
</tbody>
</table>

**Tools with optional usage**
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.

<table>
<thead>
<tr>
<th>Company</th>
<th>Purpose</th>
<th>Storage period</th>
<th>Country of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telekom</td>
<td>Technical app quality</td>
<td>30 days</td>
<td>Germany</td>
</tr>
<tr>
<td>Telekom</td>
<td>Customized design</td>
<td>12 months</td>
<td>Germany</td>
</tr>
</tbody>
</table>

You can find the opt-in switch in „Privacy Settings“ in tab „More“ in the App.

**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.

<table>
<thead>
<tr>
<th>Company</th>
<th>Purpose</th>
<th>Storage period</th>
<th>Country of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telekom</td>
<td>Technical app quality</td>
<td>30 days</td>
<td>Germany</td>
</tr>
<tr>
<td>Telekom</td>
<td>Customized design</td>
<td>12 months</td>
<td>Germany</td>
</tr>
</tbody>
</table>

You can find the opt-in switch in „Privacy Settings“ in tab „More“ in the App.

**Marketing/Retargeting**
These tools are used to serve you personalized and therefore relevant advertising content.

Marketing tools are used to serve interesting web content and to measure the effectiveness of our campaigns. This happens not only in Apps or on
Telekom webpages, but also on the pages of other advertising partners (third party providers). This is also called retargeting. It is used to create pseudonymous content or ad profiles, to the placement of relevant advertising on other websites and to derive insights into target groups that have viewed the ads and content. This information cannot be traced back to a person. Marketing and retargeting tools assist us in serving you advertising content that is potentially relevant for you. By suppressing marketing tools, you will continue to see the same number of ads, but they may be less relevant for your interests. The legal basis for these tools is Art. 6 (1) a GDPR respectively for third Countries Art. 49 (1) a GDPR.

You can find the opt-in switch in „Privacy Settings“ in tab „More“ in the App.

Services by other companies (independent third party providers)
Some pages of our app pages feature services of 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.


Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy at Deutsche Telekom?
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn acts as the data controller. 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. 15 GDPR);
b) To request that incorrect or incomplete data be rectified or supplemented (Article 16 GDPR);
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 erasure 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. 18 GDPR);
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. 20 GDPR);
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., EU Commission's adequacy decision or suitable guarantees, Art. 44 et seq. GDPR).

This privacy information was last updated 31.01.2022.