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

The protection of your personal data has a high priority for Telekom Deutschland GmbH. It is important to us to inform you about what personal data are collected, how they are used and what options you have in this regard.

What data are collected, how are they used and how long are they stored?
When using the MagentaZuhause App, hereinafter referred to as “digital service”:

During registration:
To register for the MagentaZuhause App, use your Telekom Login. You can find more information about the Telekom Login at www.telekom.de/datenschutzhinweise. This information is required for the fulfillment of the contract (Art. 6 (1) b GDPR) and will be stored on our servers until the contract ends.

If you cancel the MagentaZuhause App with Telekom, the Telekom Login data will not be deleted automatically. For details, please refer to the Telekom Login data privacy policy (Art. 6 Par. 1 b GDPR).

When using the MagentaZuhause App:
The following data are collected by us and stored until the end of the contract for your MagentaZuhause App 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 the simplified configuration of notifications in the alarm system, your e-mail address (taken from Telekom Login) is processed locally by the MagentaZuhause App (Art. 6 Par. 1 b GDPR).
- For fulfillment of the contract, we store your Telekom customer number and your e-mail address. We transfer these automatically from your Telekom Login (Art. 6 Par. 1 b GDPR).
- For SMS notification, the mobile numbers you entered are stored in the MagentaZuhause App system (§25 (1) TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 (1) a GDPR). (See also Contacts/Address book.)

When you use our MagentaZuhause App, our servers temporarily record the domain name or IP address of your end device as well as other data, such as the requested content or the response code.

The logged data is used exclusively for data security purposes, in particular for defense against attempted attacks on our web server (Art. 6 para. 1f GDPR). They are neither used for the creation of individual application profiles nor passed on to third parties and are deleted after seven days at the latest. We reserve the right to statistically evaluate anonymized data records.

The MagentaZuhause App ensures the use of the latest available version by checking against Apple AppStore or Google PlayStore, upon which the IP address of your end device is transmitted to Apple or Google.

Use of household management:
The MagentaZuhause App uses Telekom’s central household management.

Within the MagentaZuhause App, the contract partner can invite members to join their household. The invitation is sent by e-mail. Members use their own Telekom Login and must accept the invitation to the household before they can access it. Members can delete their link to the household at any time. The contract partner can remove members from the household at any time.

The following data are processed within the scope of household management (Art. 6 Abs. 1 a GDPR):

- Name of household selected by the contract partner. Initially preassigned with the last name, taken from the Telekom Login.
- Display name chosen by the contract partner or members. Initially preassigned with the first name, taken from the Telekom Login.
- Avatar (profile picture) optionally provided by the contract partner or members.
- E-mail addresses entered by the contract partner for the purpose of inviting members to the household. The e-mail addresses are deleted automatically after 14 days at the latest.
- Electric power consumption entered by the contract partner for the purpose of aggregating the household's power consumption history.
- Electric power utility contract details (name, base price, energy rate, duration, consumption data per year) for the purpose of calculating the household's power consumption cost.

Use of smart home functions:
The following data is collected by us and stored until the end of the contract for your MagentaZuhause App or until you delete the data yourself.

The MagentaZuhause App stores configuration and runtime data in the MagentaZuhause App system (§25 para. 2 No. 2 TTDSG (Telecommunications Telemedia Data Protection Act) Art. 6 para. 1 b GDPR). This includes:

- Current sensor and actuator states (e.g. window open)
- General device information (e.g. weak battery)
- Configuration data for switching groups and automations
- History data (e.g. alarm events, implemented automations, sensor state, measured power consumption)

If you cancel the MagentaZuhause App with Telekom, there will be no automatic deletion of the data on the QIVICON platform. You can initiate the deletion directly via QIVICON Support, who registers your QIVICON account. For details, please refer to QIVICON's privacy policy.

Use of location functions:
The MagentaZuhause App allows the recording of locations (geofences). This allows users 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 you are within such a geofence. Precise and position-independent location data is explicitly not collected in this way.

The following location data is processed as part of the presence function (§25 Para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 Para. 1 a GDPR)

- Addresses and names of locations (geofences) set by users as well as their determined geo-coordinates (GPS).
- Presence at a location that is detected by end devices (geofence).

Sharing your own location
The MagentaZuhause App system allows the members of a household to share their location with each other. In this context, only the presence and absence at the locations set up by the users is shared, as the exact GPS coordinates of the individual members are not recorded. (§25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1 a GDPR).

Each household member decides for themselves whether their end device determines their own location, i.e. their presence in a previously set up geofence, and thus makes it available for automations. Each member decides for themselves whether their location should be shared with other members. Each member can prevent both location detection and location sharing at any time on their end device.

Using the Home Network Check:
To make the Telekom network even better for you, the following data is collected, stored and processed by the MagentaZuhause App in the "Home Network Check" function.

Measurements about the quality of the connection (§25 (1) TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 (1) a GDPR):

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

Context information:
- Technical data of the smartphone
- Remaining battery runtime of the smartphone
- Operating system
- Type of movement of the smartphone
- Router firmware version
- Location
- Precision of the determined location
- Date/time
- Connection technology (2G, 3G, 4G, 5G, WLAN)
- Connection bandwidth booked
- Wi-Fi signal strength (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
- Rating of the Internet connection by the users
- Recommendations for the users, based on the result of the measurement of 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
- BSSID of the Wi-Fi hotspot
- Spatial sector assignment Cell ID and Cell LAC
- Mobile Country Code (MCC) and Mobile Network Code (MNC)

Complete data records (i.e. including the app installation ID and the router ID) are stored for 30 days before being deleted automatically.

Coupling with other systems:
The MagentaZuhause App system can be connected to a variety of other systems. External systems are not connected automatically but must be activated by the users themselves. The connection with and between the following Telekom products is established automatically the first time you log in to the MagentaZuhause App:
- MagentaZuhause
- MagentaTV
- HomeOS

Different systems are subject to different data privacy requirements due to their different integration and operation, which are explained below:

Connection of Telekom Routers:
The MagentaZuhause App system enables 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 enter the access data or the device password again. HomeOS provides a protected interface for this purpose which, among other things, makes it possible 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 option of connecting to devices from cooperation partners (e.g. Philips Hue, Sonos, Logitech) and controlling them via an app. The partners provide an interface for this purpose 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 registration with the respective device provider in advance. Depending on the provider, it may be necessary to authenticate yourself to the 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 exactly which information is transmitted in each individual case before you agree to the data transmission. The links to the data privacy policies of the individual device providers are listed at the end of the paragraph.

To connect Wi-Fi devices the password of the wireless home network must be provided. The password can be stored locally on the mobile device to be used in subsequent device pairing flows.

Camera services
Using the 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 different cameras 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 data privacy policy.

When installing and operating cameras, please take care not to infringe on the personal rights of third parties (e.g. illegal recording of neighbors).

Audio services
Using the MagentaZuhause App with a device provider for audio output (e.g. Sonos) allows you to use the MagentaZuhause App to provide sound to your home. The connection allows you to use different speakers in one app and, for example, emit an alarm sound when your MagentaZuhause App system detects an alarm situation. Playing audio streaming providers (e.g. Sonos) 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 data privacy policy.

Voice assistants
Depending on the service or product used, you can also use the voice services of other providers and companies (third party, e.g. Amazon). We would like to point out that for the duration of use you technically and legally leave the Telekom environment. This means that your data (names, status und IDs of devices and routines) will no longer be processed solely by Telekom during this period, but by the third party of the chosen service. The processing of your data for this period is governed exclusively by the provisions of the provider you have selected. Telekom does not assume any guarantee or liability for the legally compliant processing of your data by third parties!

Data privacy policies of our devices partners:
- MagentaTV (pdf) (Telekom)
- QIVICON platform (Telekom)
- Amazon Alexa
- D-Link Corporation
- Eurotronic
- Gardena
- Google Home
- Lifx
- Logitech
- Netatmo
- Nuki
- Philips Hue

- SONOS, Inc.
- WiZ

Support by Customer Service:
You have the option of contacting Customer Service via the MagentaZuhause App. For this, it is necessary to approve access to your data generated under points 1 a) to c) for Customer Service. This is done by clicking/tapping the corresponding “Contact” button in the “Customer Service” section in the “More” tab in the MagentaZuhause App and by communicating the diagnostic code displayed in the MagentaZuhause App to Customer Service.

This consent can be revoked at any time in the same way and expires automatically after 28 days at the latest.

Access to the generated and stored data is solely for the purpose of troubleshooting.

Surveys/Feedback from customers with GetFeedback:
We use the service of SurveyMonkey Europe UC (2 Shelbourne Buildings, 2nd Floor, Shelbourne Road, Ballsbridge, Dublin 4, Ireland) (please note: SurveyMonkey has taken over the formerly used company Usabilla and its tool of the same name) for customer surveys. Ratings as well as your feedback may be requested (Art. 6 para. 1a GDPR). Our customers’ opinions and suggestions for improvement are important components for the improvement of our digital services. Only anonymous information is processed, and it is not possible to draw conclusions about the sender. We store and evaluate the data for 24 months.

The surveys can be conducted in two different ways:

- Feedback button: You can use this button to give us your feedback at any time. If you do not use this function, no data will be transmitted.
- Display of an active feedback query: You can deny this query or cancel it at any time. Responses will not be sent until you complete the survey.

Other:
You can find information on how the SmartHome gateway (Speedport) 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 address, is not collected unless you provide this information voluntarily.

In the MagentaZuhause App, you have the option of dictating the text in addition to entering it using the keyboard. 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 the MagentaZuhause app and displayed in the input field. For details on the functionality and how you can enable or disable use of this, please contact the respective operating system manufacturer.

Permissions for access to data and functions of the end device by the digital service
In order to use the digital service on your device, it must be able to access various functions and data on your device. For this purpose, it is necessary for you to grant certain permissions (Art. 6 para. 1a GDPR, §25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act)).

The permissions are programmed differently by the various manufacturers. For example, individual permissions may be combined into permission categories and you may also only agree to the permission category as a whole.

Please note that if you object to one or more permissions, you may not be able to use all the functions of our digital service.

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

Location data
We need information about your current location for the following purpose: To connect devices to their own Wi-Fi and the MagentaZuhause App system.

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

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

Authorization to access location data is required when users record geofences. Geofences are locations with a radius that can be captured by the user for the purpose of location-based automation

Permission for accessing location data in the background, i.e. while the MagentaZuhause App is not being actively used, is required for detection when entering or leaving the created geofences. Precise location data (exact geo-coordinates of the cellphone) is not collected. The data collection is limited to entering or leaving the locations defined by the users

Contacts/Address book
The MagentaZuhause App does not require access to the contacts/address book. Mobile numbers must 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 set to do so by you.

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 revocation of the respective SMS recipients for the use of the mobile numbers. You can delete the mobile numbers entered at any time. You should therefore ensure that you receive information from the SMS recipients when they change their mobile provider, so that you are always informed which of your specified numbers actually receives an SMS.

Internet communication
The MagentaZuhause App needs access to the Internet via Wi-Fi or mobile network for the following purposes: To retrieve and display data from the MagentaZuhause App system and to send control commands to actuators connected to your MagentaZuhause App system. In order to be able to provide appropriate assistance, the status of the connection (online, channel, speed) is used.

Wi-Fi
The MagentaZuhause App needs access to the Wi-Fi (local network) for the following purposes: During startup of the SmartHome gateway (Speedport), it is searched for in the local network via UPnP and the MagentaZuhause App functionality activated.

Bluetooth
The MagentaZuhause App needs access to Bluetooth for the following purposes: To connect devices to their own Wi-Fi and the MagentaZuhause App system. After the device's Wi-Fi connection is 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 MagentaZuhause App needs access to the microphone for the following purposes:

For implementing the intercom function in the live stream from supporting cameras and door systems. While the permission for access to the microphone is automatically requested once, the activation of recording and transmission in individual cases only takes place after explicit approval by the user.

Camera
The MagentaZuhause App needs access to the camera for the following purposes:

For implementing the intercom function in the live stream of supporting cameras and door systems. While the permission for access to the camera is automatically requested once, the activation of recording and transmission in individual cases only takes place after explicit approval by the user.

To capture QR codes from devices and connect them to your own Wi-F and the MagentaZuhause App system.

To allow a photo (avatar) to be taken for the user's own profile within the household.

Files and media
The MagentaZuhause App needs access to files and media for the following purposes:

To allow users to select an image (avatar) for their own profile within the household.

Sensors and accelerometers
The MagentaZuhause App needs access to accelerometer sensors for the following purposes:

To be able to process physical gestures like “shake device” as input.

Does the digital service send push notifications?
Push notifications are messages that are sent to your end device and displayed there in a prioritized manner. This digital service uses push notifications in delivery state, provided that you have consented to this during installation or when using it for the first time (Art. 6 (1a) GDPR).

You can revoke your consent at any time. To do so, please remove the checkmark next to “Receive notifications” under Notifications in the main menu of the MagentaZuhause App.

Is my usage behavior evaluated, e.g. for advertising or tracking? Explanations and definitions
We want you to enjoy using our digital services and to make use of our products and services. This is in our economic interest. In order for you to find the products that interest you and for us to be able to design our digital service in a user-friendly way, we analyze your usage behavior anonymously or pseudonymously. Within the framework of the legal regulations, we, or companies commissioned by us, create usage profiles. It is not possible to track this information directly back to you. In the following, we inform you in general about the different purposes. Via the query “Consent to data processing”, which appears when you call up our digital service, you have the option of consenting to the processing or rejecting it in part or in full. Processing that is necessary to provide the digital service (see explanation above under 1.) cannot be refused.

Required tools
Tag management
Tag management is used to manage the use of the tools on the various pages of our digital service. For this purpose, a tag is defined for each page. The tag can then be used to determine which tools are to be used for this page. Tag management can thus be used to specifically ensure that tools are only used where they make sense and are legally legitimized.

Analytic tools
Market research/Reach measurement
The aim of reach measurement is to statistically determine the intensity of use and the number of users of a digital service, as well as to obtain comparable values for all connected offers. Market research aims to learn more about the target groups that use services or applications and view ads. At no time are individual users identified. Their identity always remains protected.

Affiliate marketing
Affiliate marketing or advertising (also called partner program) is based on the principle of commission. Here, payment is not made for the display of the advertisement. Depending on the model, the commission is only paid when the advertisement is clicked or when an order is placed. The advertisement contains an affiliate link, e.g. in the form of a cookie with a special code that uniquely identifies the offer and the affiliate (partner) with the merchant. This enables the merchant to recognize who referred the customer to its online store and which offer the customer chose.

Marketing tools
Profiles for needs-oriented design of the digital service
In order to be able to constantly improve the digital service, we would like to create so-called clickstream analyses. The clickstream corresponds to your movement in the digital service. The analysis of the movement paths provides us with information about the usage behavior. This allows us to identify possible structural errors and thus improve the user experience.

Profiles for personalized recommendations

Telekom would like to offer you individually adapted, personalized, action and click recommendations for offers, services or products. To do this, we use service providers to create a pseudonymous profile of the digital services you access on the Internet and assign categories to this profile. You will be shown content or information that matches the profile.

Required tools
These tools are necessary for you to navigate through the digital service and use essential functions. They enable basic functions, such as order processing in the online store and access to secure areas of the digital service. Furthermore, they serve the anonymous evaluation of usage behavior in order to continuously develop our digital service for you. The legal basis for these tools is §25 para. 2 no. 2 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1b GDPR or, in the case of third countries, Art. 44 ff. GDPR.

Company	Purpose	Storage duration	Country
Telekom	Login	Session, 6 months	Germany
		(remain logged in)	
Telekom	Push notifications	For the session	Germany

Optional tools
dThese tools are used when you use additional functions, such as the chat. The possible functions are explained in section 1 of this data privacy policy. The legal basis for these cookies is §25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR

Company	Purpose	Storage duration	Country (processing/access)
Survey Monkey (formerly Usabilla)	Usage surveys	24 months	Ireland
Telekom	Push notifications	12 months	Germany

Analytic tools
These tools help us to better understand usage behavior.

Analytic tools enable the collection of usage and recognition data by us or third parties, in so-called pseudonymous usage profiles. For example, we use analytic tools to determine the number of individual users of a digital service or to collect other statistics relating to the operation of our products, as well as to analyze usage behavior based on anonymous and pseudonymous information about how users interact with digital services. It is not possible to draw any direct conclusions about a specific person. The legal basis for these tools is §25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR.

Company	Purpose	Storage duration	Country (processing/access)
Telekom	Technical app quality	30 days	Germany
Telekom	Needs-oriented design	12 months	Germany

Marketing/Retargeting
These tools are used to show you personalized and therefore relevant promotional content.

Marketing tools are used to display interesting advertising content and to measure the effectiveness of our campaigns. This is done not only in Telekom digital online services, but also in other digital online services (third-party providers). This is also referred to as retargeting. It is used to create pseudonymous content or ad profiles, to serve relevant ads in other digital online services and to derive insights about target groups that have viewed the ads and content. It is not possible to draw any direct conclusions about a person in this context. Marketing and retargeting tools help us to display potentially relevant advertising content to you. By suppressing marketing cookies, you will continue to see the same number of advertisements, but they may be less relevant to you. The legal basis for these cookies is §25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR.

Company	Purpose	Storage duration	Country (processing/access
Telekom	Push notifications	12 months	Germany

You can find the opt-in switch in the “Data privacy settings” in the “More” tab in the MagentaZuhause App.

Services from other companies (independent third-party providers)
We have integrated services from third-party providers who provide their services under their own responsibility. In the process, data are collected by means of cookies or similar technologies when using our digital service and transmitted to the respective third party. Partly for Telekom’s own purposes. The legal basis for this tool is Art. 6 (1a) or Art. 49 (1a) GDPR. For information

as to what extent, for what purposes and on what legal basis further processing for the third party provider's own purposes takes place, please refer to the data protection policy of the third party provider. You can find the information on the independent third-party providers below.

Google
Google Maps
On individual pages of the digital service, e.g. in the Shopfinder, we use Google Maps to display maps, locations and for route planning. Google Maps is operated by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. By embedding Google Maps, your IP address is transmitted directly to Google and a cookie is stored as soon as you visit such a page. You can get informed about data processing by Google at https://policies.google.com/privacy?hl=de&gl=de at any time and have the possibility to object to it.

Where can I find the information important to me?
This data privacy policy provides an overview of the points that apply to Telekom's processing of your data in this digital service.

Further information, including on data privacy in general and in specific products, is available at https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz and at http://www.telekom.de/datenschutzhinweise.

Who is responsible for data processing? Who do I contact if I have questions about the data privacy policy at Telekom?
Telekom Deutschland GmbH (Landgrabenweg 151, 53227 Bonn, Germany) is responsible for data. If you have any questions, please contact Customer Service or our data privacy officer Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.

What rights do I have?
You have the right

a. to request **information** on the categories of data processed, the purposes of processing, any recipients of the data, or the planned storage period (Art. 15 GDPR);

b. to demand the **correction** or completion of incorrect or incomplete data (Art. 16 GDPR);

c. to **revoke** given consent at any time with effect for the future (Art. 7 para. 3 GDPR);

d. to **object** to data processing that is to be carried out on the basis of a legitimate interest for reasons arising from your particular situation (Art. 21 (1) GDPR);

e. in certain cases, within the framework of Art. 17 GDPR, to demand the deletion of data – in particular, insofar as the data are no longer required for the intended purpose or is processed unlawfully, or you have revoked your consent in accordance with (c) above or declared an objection in accordance with (d) above;

f. under certain conditions, to demand the **restriction** of data, insofar as deletion is not possible or the obligation to delete is disputed (Art. 18 GDPR);

g. to **data portability**, i.e. you can receive your data that you have provided to us in a conventional machine-readable format, such as CSV, and transmit it to others if necessary (Art. 20 GDPR);

h. to issue a complaint to the competent **supervisory authority** about the data processing (for telecommunication contracts: Federal Commissioner for Data Protection and Freedom of Information; otherwise: State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia).

To whom does Telekom pass my data?
To **order processors,** i.e. companies that we commission with the processing of data within the scope provided by law, Art. 28 GDPR (service providers, vicarious agents). Telekom remains responsible for the protection of your data even in this case. We commission companies in the following areas in particular: IT, sales, marketing, finance, consulting, customer service, human resources, logistics, printing.To order processors, i.e. companies that we commission with the processing of data within the scope provided by law, Art. 28 GDPR (service providers, vicarious agents). Telekom remains responsible for the protection of your data even in this case. We commission companies in the following areas in particular: IT, sales, marketing, finance, consulting, customer service, human resources, logistics, printing.

To **cooperation partners** who independently provide services for you or in connection with your Telekom contract. This is the case if you order services from such partners from us, if you consent to the involvement of the partner or if we involve the partner on the basis of legal permission. In addition, Telekom is pursuing collaborations with other service providers (e.g., Smart Home Services). If you are also a user of these services, you can link your respective account with them. This linking process must be done separately for each service. Once you have established a connection, the personal data listed in this privacy notice can be used from your respective account ort he corresponding service. The respective service provider informs you about the processing of your personal data.

Due to legal obligation: In certain cases, we are legally obligated to transmit certain data to the requesting government agency. Example: After the presentation of a court order, we are obligated, in accordance with § 101 of the Copyright Act, to provide information to rights holders about customers who are suspected of having offered copyrighted works on Internet file-sharing platforms

Where are my data processed?
Your data are processed in Germany and other European countries. If, in exceptional cases, processing of your data also takes place in countries outside the European Union (in so-called third countries), this will happen,

- if you have expressly consented to this (Art. 49 para. 1a GDPR). (In most countries outside the EU, the level of data protection does not meet EU standards. This applies in particular to comprehensive monitoring and control rights of state authorities, e.g. in the USA, which disproportionately interfere with the data protection of European citizens,
- or insofar as it is necessary for our provision of services to you (Art. 49 para. 1b GDPR),
- or insofar as it is provided for by law (Art. 6 para. 1c GDPR).

Furthermore, your data will only be processed in third countries if certain measures ensure that an adequate level of data protection exists (e.g. adequacy decision of the EU Commission or so-called suitable guarantees, Art. 44ff GDPR).

Status of data privacy policy 01.11.2023