

Data privacy information from Telekom Deutschland GmbH („Telekom“) for using the GCA App

General

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.

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 for 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?

Telekom Deutschland GmbH is the party responsible for data privacy ("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 purpose of the processing, any recipients of the data, the envisaged storage period (Art. 15 GDPR);
- b) To request incorrect or incomplete data is **rectified** or supplemented (Art. 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 (Art 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 objected 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 your data which you provided to us, in a commonly used and machine-readable format, such as CSV and can, where necessary, transmit 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, Art. 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, 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 contract with us services from these partners or if you consent to the incorporation of the partner or if we incorporate the partner on the basis of legal permission.

Owing to legal obligations: In certain cases, we are legally obliged to transfer certain data to the requesting state authority. Example: Upon presentation of a court order, we are obliged under § 101 of the German Copyright Act (Urheberrechtsgesetz – 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?

In general, your data is processed in Germany and in other European countries.

If your data is also processed in countries outside the European Union (i.e. in third countries) by way of exception, this is done only if you have explicitly given your consent or it is required so we can provide you with services or it is prescribed by law (Art. 49 GDPR). Furthermore, your data is only 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 ff. GDPR).

What data is recorded, how is it used and how long is it stored?

- a) **At registration:**
To register for the app, please enter your first name, surname, e-mail address, user name, and password. These details are required for login to the HotSpots and will be stored on our servers for contract fulfillment purposes for as long as you are able to use the service.
- b) **When using the app:**
When you use the app, our servers temporarily record your device's IP address and other technical features such as the requested content (Art. 6 (1) b GDPR).
You can dictate text and input data using the keyboard in this app. 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 and outputs it in the input field. Contact your specific operating system vendor for details on the functionality, and how you can switch on/off usage.
- c) **Miscellaneous:**
The app will analyze data for the purposes of assessing the quality of HotSpots, eliminating faults, and identifying the best HotSpots for

you, based on your personal movement profile. To do so, the following data will be collected by the Global Corporate Access App and passed on to iPass Inc. (3800 Bridge Parkway, Redwood City, California 94065, USA) during the time when you are using the app:

- a) Identifying device data (e.g., Android ID)
- b) Technical specifications of the smartphone
- c) Technology used (2G, 3G, 4G, Wi-Fi)
- d) Geolocation of the smartphone
- e) Data rate measured in both download and upload
- f) Package runtime measured
- g) Number of hops between measuring client and measuring server
- h) Date/time
- i) Spatial sector allocation cell ID and cell LAN
- j) RSSI, RSRP, and RSRQ signal strength
- k) Transferred data volume measured
- l) User name and password for authentication to the HotSpot
- m) When forwarded to iPass, this encrypted data will be subject to the data privacy laws of the United States. Deutsche Telekom accepts no responsibility for the data which is forwarded to iPass.

It will not be possible to provide the service without forwarding this data. I have taken note of this fact and will bring it to the attention of anyone sharing with me the device on which the app is installed.

The use of other Wi-Fi providers is enabled by default. If you are using the Global Corporate Access App and you turn off the automatic connection ("Auto-Connect") to other networks, these networks will be shown, but not automatically used.

If you turn this function on, then you automatically accept the terms of use and data privacy notes of the respective Wi-Fi provider. To view the terms of use or data privacy notes of other Wi-Fi providers, please deactivate this function in the app and connect to the relevant Wi-Fi provider using the Wi-Fi settings of the operating system of your device.

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 authorization categories are programmed differently by the various manufacturers. With Android for example, individual authorizations are grouped into authorization categories and you can only agree to the authorization category as a whole.

However, please remember that in the case of revocation 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 following purpose:

Localizing the user in order to use the HotSpot finder

Internet communication

The app requires access to the Internet via Wi-Fi or mobile communications for the following purposes:

- Establishing Wi-Fi access through authentication
- Downloading profile data
- Uploading data on quality

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 can deactivate receipt of push notifications at any time in your device settings.

Services from companies that are not tied in through processing and assume responsibility for providing their services

Google

Incorporation of Google Maps: We use Google Maps for maps, locations and route planning on individual app pages. Google Maps is run by Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. By embedding Google Maps your IP address is transferred to Google and a cookie stored. You can obtain information and opt out at any time from data processing by Google at <http://www.google.de/intl/de/policies/privacy>.

We use the remarketing and Google AdWords function from Google Inc. ("Google") in our app. This function is implemented via a cookie and is used to present app users with web advertising tailored to their interests as part of the Google advertising network. Users can then be shown on these pages advertisements which relate to content they have accessed previously that use the Google remarketing function. According to its own statements, Google does not collect any personal data with this process. If you, however, do not want to use Google's remarketing function, you can disable this permanently by adjusting the relevant settings at <http://www.google.com/settings/ads>. Alternatively, you can disable the use of cookies for targeted advertising via the advertising network initiative by following the instructions at http://www.networkadvertising.org/managing/opt_out.asp. Further information on Google remarketing and Google's privacy policy is available at: <http://www.google.com/privacy/ads/>.

If you access our app via a Google ad, Google AdWords stores a cookie on your device. This cookie becomes invalid after 30 days. No conclusions can be drawn about you as a person. We use the information collected with the aid of this conversion cookie to create statistics about our conversion rate. This means that we find out how many users came to our app via a Google ad and acquire a product within 30 days. If you do not wish to participate in the tracking process, you can disable cookies for conversion tracking by specifying in your browser settings that cookies from the relevant domain are to be blocked: Google AdWords: googleadservices.com