Data privacy information from Deutsche Telekom AG („Telekom“) for Leadership App (LEAP)

General

Deutsche Telkom AG, Human Resources Development 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 – UhhG) 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?

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.

a) Text chat:
If you use the Text chat on the app to contact the Customer Services department, various types of information are sent to the customer adviser when you initialize the chat (Art. 6 (1) a GDPR). This includes, for instance, the help topic you selected in the app, app version, operating system version, and the like. The chat platform also regularly transfers information regarding the accessibility of the chat

service. Using this information, the button to start the Text chat is enabled or disabled.

b) **Other: UUiD:**
is used inside the app for the chat functionality to id messages and files uploaded to the server. These UUiDs are stored indefinitely on the server.

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:

Internet communication
The app requires access to the Internet via Wi-Fi or mobile communications for the following purposes download content from the backend and it is stored as long as the content resides on the server if updates are regular or until the app is deleted from the device. Allows chatting with other users provided by the backend, the chats are stored on the device until the app is deleted from the device. The data is stored on the servers indefinitely.The app requires access to the contacts/address book in order to assign voicemails to contacts

Camera, microphone, photos.
The app requires access to camera and photos gallery for the following purpose allowing the user to share pictures via the messaging functionality.

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.

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 you can find the products that interest you and so 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. Subsequently we inform you generally about the various purposes and techniques.

Purposes (Art. 6 (1) f GDPR / §15 (3) German Telemedia Act (Telemediengesetz – TMG)

Tag management
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
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. Individual users are not identified at any time. Your identity is always protected.

Profiles for designing the app based on needs
To improve the app constantly, we create clickstream analyses. The clickstream corresponds to your movement path in the app. Analyzing the movement paths provides us with an insight into the app's usage habits. This lets us identify possible structural errors in the app and thus improve the app so it is optimally tailored to your needs. Individual users are not identified at any time.

Profiles for improving the technical app quality
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..