Data privacy information Deutsche Telekom Security GmbH („Telekom“) for Mobile Encryption App (MECrypt)

General
Deutsche Telekom Security 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:
The app is registered from the administrator in mySHS. The administrator there creates end users for the use of the MECrypt service. For this purpose, the following data of the end user is registered:

- Name, E-Mail Address

This data remains stored in mySHS as long as th MECrypt service is used.

When using the app:
The MECrypt ID is used to provide the services of Deutsche Telekom Security GmbH. This will be sent to you after conclusion of the contract. The Mobile Encryption App encryption system is designed to use a new key for each call. After the conversation, the key material is deleted immediately. Additional personal data, e.g. Your name, address or e-mail address will not be recorded unless you provide this information voluntarily.

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

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

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

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

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

If desired, MECrypt can import contacts from the system directory into an encrypted data container to exchange encrypted messages with the contacts or call them directly. The data remains on the phone after import and will not be transferred to the Internet

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 can use push notifications to show you discovered vulnerabilities and attacks on your mobile device if your administrator has set it up on the MPP zConsole. 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?
No, no tools / cookies are used in the MECrypt app to evaluate user behavior.

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.

Company	Purpose	Storage period	Country of processing
Telekom	Login	As long as the app is used	Germany

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 Security GmbH processing your data in this app.

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

Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy at Deutsche Telekom Security GmbH?
Deutsche Telekom Security GmbH 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.15GDPR);
b) To request that incorrect or incomplete data be **rectified** or supplemented (Article16GDPR);
c) To **withdraw** consent at any time with effect for the future (Art. 7 (3) GDPR);
d) To **object** to the processing of data on the grounds of legitimate interests, for reasons relating to your particular situation (Article 21 (1) GDPR);
e) To request the **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.18GDPR);
g) To **data portability,** i.e., you can receive the data that you provided to us in a commonly used and machine-readable format such as CSV, and can, where necessary, transfer the data to others (Art.20GDPR);
h) To **file a complaint** with the competent **supervisory authority** regarding data processing (for telecommunications contracts: the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit); for any other matters: State Commissioner for Data Protection and Freedom of Information, North Rhine-Westphalia (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen).

Who does Deutsche Telekom Security GmbH pass my data on to?
To processors, i.e., companies we engage to process data within the legally defined scope, Article 28GDPR (service providers, agents). In this case, Deutsche Telekom Security GmbH 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 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 only.

This privacy information was last updated July 2021