Data Privacy Police for the „Magenta Security OneTimePass.ID SmartToken“-App of Deutsche Telekom Security GmbH

General

Deutsche Telekom AG 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.

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

a) **When registering**:
To activate the app, simply enter the existing e-mail address that identifies you as a user of the OneTimePass platform. This information is only used when sending an activation or reinitialization request to be able to assign it to your OneTimePass account on the platform side. The e-mail address is not stored in the app or on the device. The app also sends the app version, OS version, and device type to the OneTimePass platform for support cases.

Company	Purpose	Storage period	Country of processing
Deutsche Telekom Security GmbH	Activation of the App (“Pairing”)	Until user is deleted	Germany

b) When using the app:
When using the app, there is usually no communication between the app and the platform. The only exception is an update notification that is sent when the OS version or the version of the app has changed.
The app itself does not store any personal data. On the platform, data is only stored for as long as it is required to use OneTimePass.

2. Authorizations

For the app to work on your device, it needs access to various functions and data on the device. You may need to grant certain authorizations for this. 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.
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:
Sending activation and re-initialization requests
Sending update requests

Biometric data

If you want to use biometric data (e.g., fingerprint sensor/FaceID) to unlock the app, the app requires the authorization to use the corresponding functionality on the device. The app is not given direct access to the biometric data itself, but only uses the authentication functions provided by the respective operating system.

3. Does the app send push notifications?

No.

4. Controlling data used by social-media plug-ins and links to social media platforms

We neither use social media plug-ins nor links to social media plattforms.

5. Will my usage habits be evaluated, e.g. for advertising purposes or tracking?

No.

6. 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 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.

7. Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy at Deutsche Telekom?

Deutsche Telekom AG 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.

8. 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).

9. Who does Deutsche Telekom pass my data on to?

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.

10. Where is my data processed?

Your data will be processed in Germany and other European countries..

Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn

Trade Register:
District Court of Bonn HRB 15241,
Registered Office Bonn
VAT ID No. DE 254595345