Data privacy information Deutsche Telekom Security GmbH („Telekom“) for Mobile Protect Pro App (MPP)

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?

In the privacy settings of the MPP zConsole, the administrator can define which data is to be collected by the application. The following data can be collected. By configuration, the customer administrator can set whether this data is collected. Since an attack is detected locally on the terminal by the z9 engine, very little data is needed for identification and secure communication of the device with the MPP console. The data of all courses of action that are carried out both in the MPP app and in the zConsole are saved for 30 days and then deleted. Threatdata is saved for 30 days and then deleted.

a) **At Login (Starting the app):**
- Up to and including version 4.7 access data (user name / email and password) - from version 4.8.xx unique token
- Hash value of the device (MD5 of the IMEI or the serial number), on iOS (MD5 of the IMEI)
- Operating system of the device

b) **Device information after login (Android):**
- Unique push token of the app on the device to verify messages from the console
- Location: GPS latitude and longitude - on the privacy definitions set by the administrator, road, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Network: MAC and, IP Address BSSID, SSID
- Device: Operating System, Operating System Version, Model, IMEI, Jailbroken, Developer Option
- List of installed apps
- Connection status (WLAN or 3G)
- User Information: Username / Email (determined from the console).

c) **Device information after login (iOS):**
- Unique push token of the app on the device to verify messages from the console
- Location: GPS latitude and longitude - on the privacy definitions set by the administrator, road, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Network: MAC and, IP Address BSSID, SSID
- Device: Operating System, Operating System Version, IMEI, SNO (if available)
- List of installed apps (only available if an MDM is connected)
- Connection status (WLAN or 3G) (optionally adjustable)
- User Information: Username / Email (determined from the console)

d) **At the synchroniziation:**
- Hash value of the local z9 machine (anomaly detection software) and malware database
- Location: GPS latitude and longitude - depending on the privacy
- definitions set by the administrator, the street, city, state (region, time zone, country code, continent) will be determined from the GPS data. (optionally adjustable)
- Network: Router BSSID and SSID
- Device: IP and MAC address of the device
- App forensics: Active apps on the device (Android, iOS)
- Connection status (WLAN or 3G)

e) **At the detection of an attack:**
- Time of the event
- Attack Name
- Location: GPS longitude and latitude -on the privacy definitions set by the administrator, road, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Binary code of the app (no data)
- Network: Mac and IP address, Router BSSID and SSID, Neighboring WLAN networks (BSSID / SSID), network statistics (existing TCP / UDP connections at the time of the attack including IP and port address), ARP table of all local hosts in the WLAN using Communicate with the device and information about the base station
- Device: operating system, operating system version, device model, IMEI, active APP (Android), ARP table of the device, list of (at the time of attack) active processes, in case of attacks on the file system the fully qualified file / folder path on the Device have been changed.
- App Forensics: Devices installed on the device, package name of detected malware / app
- iOS only: In the case of attacks on the profile, all profiles are sent to the console.

Additional personal data, such as your name, address or telephone number are not recorded by the APP.

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:

Location data
If your administrator has set this option in the MPP zConsole (see above), the app needs information about your current location in order to determine the location where an attack on your mobile device took place (e.g. malicious WLANs).

Internet communication
In order to display attacks on your mobile device on your administrator's MPP zConsole, the app requires access to the Internet via Wi-Fi or mobile data network.

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).

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

No, no tools / cookies are used in the MPP app to evaluate user behavior. (related to MPP app)

No, only tools / cookies that are strictly necessary for the operation of the zConsole are used in the zConsole. These are the following: (based on MPP zConsole)

Strictly necessary tools
These tools / cookies are necessary for the MPP zConsole (management console) to work properly. These are technically necessary tools / cookies. The legal basis for these tools / cookies is Art. 6 Para. 1 b GDPR **(s. Annex).**

Is the auditlog recorded? If yes, how long is the audit log saved? (based on MPP zConsole)

The audit log stores courses of action that are carried out both in the MPP app and in the zConsole. These include e.g. logging into the MPP app or making changes in the zConsole. This information is only visible to the administrator. The data is stored for 30 days and then deleted.

Where can I find the information that is important to me?

Dieser 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 Security?

Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn 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. 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).

Who does Deutsche Telekom Security pass my data on to?

To processors, i.e., companies we engage to process data within the legally defined scope, Article 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, and 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 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 only be saved and processed in Germany.

Is the data saved securely?

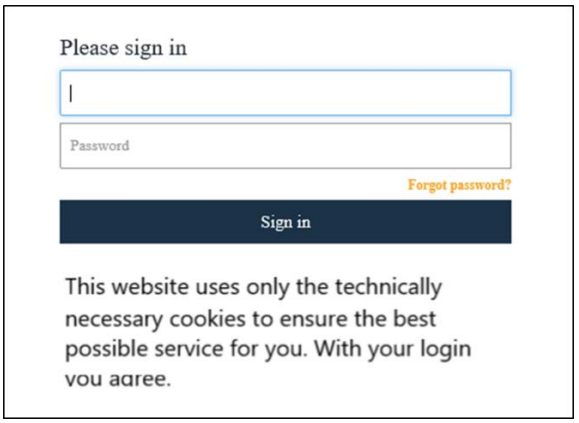
To protect your data from unauthorized access and misuse, we have taken extensive technical and operational security measures in accordance with German law (GDPR).

Will I be informed about changes to this data privacy notice?

Your data will only be saved and processed in Germany. If we need to change this data privacy notice, we will notify you (customer administrators) as part of software updates about the corresponding changes.

Your data privacy settings

The MPP zConsole uses only technically necessary tools / cookies. By Login you accept the use of the technically necessary tools / cookies.



This Data Protection Statement was last updated 18.06.2020

Annex:

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

a) Strictly necessary tools

Company	Name	Description (Function)	Involved as
Zimperium	csrftoken	This cookie is associated with the Django web development platform for Python. It is designed to help protect a site against cross-site request forgery attack on web forms	Processors
Zimperium	zcookie	Session token The session token is a piece of data that is used in network communications (often over HTTP) to identify a session, a series of related message exchanges. It is also used to identify several related requests from a user and to assign them to a session.	Processors
Zimperium	zcookie panel	Session token für zpanel zPanel is the administration tool with which we manage all customers in one environment (VPC).	Processors
Zimperium	zme	System token, First-party cookies zme is used to tell the client website about the customer (system_token) associated with the user. they are also considered as First-party cookies and are set by the website visited by the user.	Processors