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

The protection of your personal data has a high priority for Deutsche Telekom Security GmbH. It is important to us to inform you about what personal data are collected, how they are used and what options you have in this regard.

What data are collected, how are they used and how long are they stored?
When using MPP app, hereinafter referred to as online service:
Mobile Protect Pro App protects mobile devices administered by the customer. It generates alarms for the administrators and - if requested, adjustable in the console - for the user of the mobile device in case of threats to the operating system, network connections or stored data on the device.

The Mobile Protect Pro app monitors a wide variety of parameters and vectors, which are derived from the mobile devices, whose operating systems and network connections can be read out.

By correlating these values, a normal condition can be interpreted and

anomalies in the system are determined. In this way, known and unknown.

attacks on the mobile device are detected. The interfaces of the device, its network connections, the operating system and the application levels are monitored. The

observation of these parameters and their interpretation takes place in the app on the mobile

device. The protective effect of the app is given even if there is no connection with the console via the Internet.

In the privacy settings of the MPP console, the administrator can define whether and which data should be collected by the application. Since an attack is detected locally on the device by the z9 engine, very little data is required to identify and securely communicate the device with the MPP console. The data of all courses of actions performed in both the MPP App and the zConsole is stored for 30 days and then deleted. The threat data – which includes all events transmitted from the app to the zConsole as well as the zConsole audit log – is deleted by default after 30 days, but this period can be extended to up to 90 days at the customer's request. Device and user data will be deleted within 7 days. All other data will be deleted at the end of the contract.

Following data may be recorded when using the app:

- For signature updates ('pull' of signature) and verification of certificates (SSL strip) the device connects to the Zimperium backend. The IP of the device is required for communication, so this is transmitted to USA. Zimperium neither stores these accesses nor does it evaluate or otherwise process the data.

When using the Mobile Protect Pro Android app:
- Unique push token of app on the device to verify messages from the console.
- Location: GPS longitude and latitude - on the privacy definitions set by the administrator, street, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Network: MAC and IP Address, BSSID, SSID (optionally adjustable)
- Device: Operating system, Operating system version, Model, Jailbroken, Developer option
- List of installed apps (optionally adjustable)
- Connection status (WLAN or 3G) (optionally adjustable)
- User information: Username /Email (determined from the console)

When using the Mobile Protect Pro iOS app:
- Unique push token of app on the device to verify messages from the console.
- Location: GPS longitude and latitude - on the privacy definitions set by the administrator, street, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Network: MAC and, IP Address BSSID, SSID (optionally adjustable)
- Device: Operating system, operating system version, 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)

Upon detection of an attack
- Time of the event
- Attack description
- Location: GPS longitude and latitude - on the privacy definitions set by the administrator, street, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- App recognition (binary code, hash value)
- 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 WLAN that communicate with the device as well as information about the base station (optionally adjustable)
- Device: Operating system, operating system version, device model, IMEI, active APP (Android), connection status (WLAN or 3G), ARP table of the device (before and after the attack), list of active processes (at the time of attack), in the case of attacks on the file system the fully qualified file/folder path that were changed on the device.
- App Forensics: Apps installed on the device, package name of the detected malware/app (optionally adjustable)
- IOS only: In case of attacks on the profile, all profile information is transmitted to the console. (only available in connection with an MDM) (Art. 6 para. 1b GDPR, §25 para. 2 No. 2 TTDSG (Telecommunications Telemedia Data Protection Act)).

When you use our online service, our servers temporarily record the domain name or IP address of your terminal device as well as other data, such as the content requested or the response code.

The logged data are used exclusively for data security purposes, in particular to defend against attempted attacks on our web server (Art. 6 para. 1f DSGVO). They are neither used for the creation of individual application profiles nor passed on to third parties and are deleted after 7 days at the latest. We reserve the right to statistically evaluate anonymized data records.

Pairing with other systems:
Mobile Protect Pro offers optional integration with mobile device management (MDM). In the privacy settings of the MPP console, the administrator can define which data should be collected by the application. Thereby, following data can be collected:

- Hash value of local z9 engine (anomaly detection software) and malware database
- Location: GPS longitude and latitude - depending on the privacy definitions set by the administrator, street, city, state (region, time zone, country code, continent) are determined from the GPS data. (optionally adjustable)
- Network: Router BSSID and SSID (optionally adjustable)
- Device: IP and MAC address of the device
- App Forensics: Active apps on the device (Android, iOS)
- Connection status (WLAN or 3G) (optionally adjustable)
- (Art. 6 para. 1a GDPR)

Here, you can find further information on the topic of newsletters.

Permissions for access to data and functions of the end devices by the online service.
In order to use the online service on your terminal device, it must be able to access various functions and data on your terminal device. For this purpose, it is necessary for you to grant certain permissions (Art. 6 para. 1a GDPR, §25 para. 1 GDPR).

The permissions are programmed differently by the various manufacturers. For example, individual permissions may be combined into permission categories and you may also only agree to the permission category as a whole.

Please note that if you object to one or more permissions, you may not be able to use all the functions of our online service.

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

We need information about your current location for the following purpose

- Location data
  If set by your Mobile Protect Pro console administrator, the app requires information about your current location to determine the location where an attack on your mobile device has occurred (e.g. malicious WLANs). The data of all courses of action performed both in the MPP app and in the console are stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.
- Internet communication
  In order to display attacks on your mobile device on your administrator's MPP console, the app requires internet access via Wi-Fi or cellular. The data of all courses of action performed both in the MPP app and in the console are stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.
- Camera, microphone, USB, photos, videos, message contents, etc.
  With the help of the camera, the QR code sent to you can be scanned. This connects the mobile device to the created tenant in the MPP-zConsole Energy management. The online service needs access to the energy management for the following purposes:
  To allow the app to protect your mobile device in the background, an automatic energy manament exception is added to prevent the app from stopping.
- Filesystem
  The online service requires access to the local file system of the mobile device for the following purpose: To detect unauthorized access. No data is read or transmitted.

Does the online service send push notifications?
Push notifications are messages sent from the app to your device, where they are prioritized. This app can use push notifications to show you discovered weak points and attacks on your mobile device if it is set that way by your administrator on the MPP console. This app uses push notifications in delivery status, provided that you have consented to this when installing the app or when using it for the first time (Art. 6 sec. 1 a GDPR).

You can revoke your consent at any time. To do this, please uncheck the box next to "Activate push" in the main menu of the MPP app under notifications.

Is my usage behavior evaluated, e.g. for advertising or tracking?
No, the MPP app does not use any tools to evaluate user behavior.

Required tools
These tools are necessary for you to navigate through the online service and use essential functions. They enable basic functions, such as order processing in the online store and access to secure areas of the online service. Furthermore, they serve the anonymous evaluation of usage behavior in order to continuously develop our online service for you. The legal basis for these tools is §25 para. 2 no. 2 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1b GDPR or, in the case of third countries, Art. 44 ff. GDPR

Company	Purpose	Storage duration	Country
Deutsche Telekom Security GmbH	Login	As long as the app is used	Germany

Optional tools

These tools are used when using the following functions of Mobile Protect Pro:

- Phishing protection
- Secure VPN connection for a secure Wi-Fi network

When using these features of the Mobile Protect Pro app, you can set whether personal data or your traffic is routed via VPN to a gateway to Zimperium in USA. The possible functions are explained in section 1 of this privacy policy. The legal basis for these cookies is §25 para. 1 TTDSG (Telecommunications Telemedia Data Protection Act), Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR

Company	Purpose	Storage duration	Place of processing
Zimperium	Phishing protection	Data is not stored	USA
Zimperium	Secure VPN connection for a secure Wi-Fi network	Data is not stored	USA
Zimperium	Content inspection: Content inspection is an optional function of the phishing policy. The URL of the page to be examined is transmitted directly from the device to a Zimperium backend and examined there. To enable this communication, the IP of the device is also transmitted	Data is not stored	USA

Analytic tools
We use for sending push notifications on Android, Firebase Cloud Messaging, a component of Firebase from the company Google. Related code fragments with a reference to other Firebase tools such as Google AdMob, Google CrashLytics, Google Firebase Analytics, etc. are possible. However, these tools are not active and are not used for any evaluations.

Where can I find the information important to me?
This privacy policy provides an overview of the points that apply to Telekom's processing of your data in this online service.

Further information, including on data privacy in general and in specific products, is available at https://www.telekom.com/en/company/data-privacy-and-security/governance-data-privacy and at https://www.telekom.de/datenschutzhinweise/.

Who is responsible for data processing? Who do I contact if I have questions about the data privacy policy at Telekom?
Deutsche Telekom Security GmbH, Bonner Talweg 100 53113 Bonn is responsible for data. If you have any questions, please contact our Customer Service or our data privacy officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany, privacy@telekom.de

What rights do I have?
You have the right,

a. To request **information** on the categories of data processed, the purposes of processing, any recipients of the data, or the planned storage period (Art. 15 GDPR);

b. to demand the **correction** or completion of incorrect or incomplete data (Art. 16 GDPR);

c. to **revoke** given consent at any time with effect for the future (Art. 7 para. 3 GDPR);

d. to **object** to data processing that is to be carried out on the basis of a legitimate interest for reasons arising from your particular situation (Art. 21 (1) GDPR);

e. in certain cases, within the framework of Art. 17 GDPR, to demand the deletion of data – in particular, insofar as the data are no longer required for the intended purpose or is processed unlawfully, or you have revoked your consent in accordance with (c) above or declared an objection in accordance with (d) above;

f. under certain conditions, to demand the **restriction** of data, insofar as deletion is not possible or the obligation to delete is disputed (Art. 18 GDPR);

g. to **data portability**, i.e. you can receive your data that you have provided to us in a conventional machine-readable format, such as CSV, and transmit it to others if necessary (Art. 20 GDPR);

h. to issue a complaint to the competent **supervisory authority** about the data processing (for telecommunication contracts: Federal Commissioner for Data Protection and Freedom of Information; otherwise: State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia).

To whom does Telekom pass my data?
To **order processors**, i.e. companies that we commission with the processing of data within the scope provided by law, Art. 28 GDPR (service providers, vicarious agents). Telekom remains responsible for the protection of your data even in this case. We commission companies in the following areas in particular: IT, sales, marketing, finance, consulting, customer service, human resources, logistics, printing.

To **cooperation partners** who independently provide services for you or in connection with your Telekom contract. This is the case if you order services from such partners from us, if you consent to the involvement of the partner or if we involve the partner on the basis of legal permission.

Due to legal obligation: In certain cases, we are legally obligated to transmit certain data to the requesting government agency.

Where are my data processed?
Your data are processed in Germany and other European countries. If, in exceptional cases, processing of your data also takes place in countries outside the European Union (in so-called third countries), this will happen,

- if you have expressly consented to this (Art. 49 para. 1a GDPR). (In most countries outside the EU, the level of data protection does not meet EU standards. This applies in particular to comprehensive monitoring and control rights of state authorities, e.g. in the USA, which disproportionately interfere with the data protection of European citizens,
- or insofar as it is necessary for our provision of services to you (Art. 49 para. 1b DSGVO),
- or insofar as it is provided for by law (Art. 6 para. 1c GDPR).

Furthermore, your data will only be processed in third countries if certain measures ensure that an adequate level of data protection exists (e.g. adequacy decision of the EU Commission or so-called suitable guarantees, Art. 44ff GDPR)

Status of privacy policy March 2024