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 the Deutsche Telekom Security GmbH. It is important for us to inform you about what personal data is collected, how they are used and what options you have in this regard.

What data is collected, how is it used, and how long is it stored? Necessary processing for the provision of the digital service (Art. 6 para. 1b GDPR, §25 para. 2 no. 2 TDDDG)
When using the MPP-app hereinafter referred to as the digital service:

When registering:
Registration of the app is done by the administrator in the MPP-zConsole. After launching the app, the following data is collected:

- Up to and including version 4.7 access data (username/email and password) – from version 4.8.xx unique token
- Hash value of the device (MD5 of the IMEI or serial number), for iOS (MD5 of the IMEI)
- Operating system of the device

Additional personal data, such as Your name, address or telephone number will not be collected by the APP.

This information is necessary for the identification and secure communication of the end device with the MPP-zConsole.

The threat data – which includes all events transmitted from the app to the zConsole as well as the zConsole audit log – is deleted after 30 days by default, and 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.

When using the MPP app:
The MPP app protects the 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 MPP app observes a wide variety of parameters and vectors that can be read out from the mobile devices, their operating systems and network connections. By correlating these values, a normal state can be interpreted and anomalies in the system can be detected. 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 level are monitored. These parameters are observed and interpreted in the app on the mobile device. The app's protection is also present when there is no connection to the console via the Internet.

In the privacy settings of the MPP-zConsole, 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 between the device and the MPP-zConsole. The data of all actions that are carried out in both the MPP app and the MPP-zConsole are stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.

The following data may be collected 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 MPP-Android-app:

- Unique push token of the 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 configurable)
- Device: Operating System, Operating System Version, Model, Jailbroken, Developer Option
- List of installed apps (optionally configurable)
- To analyze and classify previously unknown apps, they can be transferred directly from the device to Zimperium. The IP-address of the device is required for communication, so it is transmitted to the USA. Zimperium does not store these accesses, nor is the data evaluated or otherwise processed.
- Connection status (WLAN or 3G) (optionally configurable)
- User Information: Username/Email (determined from the console)

When using the MPP-iOS-app:

- Unique push token of the 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 configurable)
- 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 configurable)
- User Information: Username/Email (determined from the console)

When an attack is detected:

- 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 the WLAN that communicate with the device as well as information about the base station (optionally configurable)
- Device: operating system, operating system version, device model, IMEI, active APP (Android), connection status (Wi-Fi or 3G), ARP table of the device (before and after the attack), list of active processes (at the time of the attack), in case of attacks on the file system, the fully qualified file/folder path that was changed on the device.
- App Forensics: Apps installed on the device, package name of the detected malware/app (optionally configurable)
- 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)

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

The logged data is used exclusively for data security purposes, in particular to defend against attack attempts on our web server (Art. 6 para. 1f GDPR). They are not used to create individual user profiles or passed on to third parties and are deleted after 7 days at the latest. We reserve the right to carry out the statistical evaluation of anonymized data sets.

Pairing with other systems: The MPP app 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. The following data can be collected:

- Hash value of the 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 (Wi-Fi or 3G) (optionally adjustable)

(Art. 6 para. 1a GDPR)

Different processing in the area of TelekomCloud Marketplace (business customers)
Text Chat TelekomCLOUD Marketplace: If you use Text Chat on the TelekomCLOUD service to contact customer service, various information will be transmitted to the chat system (Art. 6 para. 1 b, f GDPR) and deleted after 7 days. These include, for example: your IP address, browser version, operating system version; this data cannot be viewed by our customer advisor. The data generated during the service chat is transferred to our CRM system. Due to the system, the chat content will be deleted after 24 hours at the latest. Additional data about the chat (start time, duration of the chat, internal notes, customer information requested in the chat, if applicable) will be anonymized after 28 days.

In addition, information about the accessibility of the chat service is transmitted from the chat platform to the digital service of the TelekomCLOUD Marketplace at regular intervals. With the help of this information, the button to start the text chat is activated or deactivated on the digital service.

Processing customer data with Salesforce:
In order to process customer service inquiries and for customer communication by e-mail or telephone in accordance with your consent, your personal customer data will be stored and processed in our CRM system. We use the services Salesforce Service Cloud & Salesforce Marketing Cloud of the processor Salesforce (Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 Munich, Germany).

If you have given us your consent, we will collect email usage information (sending, openings, clicks) via this system in order to improve our service to you and provide you with more relevant information. If you no longer agree to this, you can object to this at any time under "My Settings".

Customer feedback with Salesforce Survey: If you use our support services, we may email you to participate in a customer satisfaction survey. Participation in the survey is voluntary and serves to improve the quality of our services. In this case, the results of the survey are linked to the corresponding customer case and stored in a personalized form in order to be able to evaluate the associated service in a targeted manner. To complete the survey, you will be redirected to the website of Salesforce (Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 Munich, Germany. For more information on their legal and data processing principles, please see https://www.salesforce.com/company/legal/.

Authorisations for access to data and functions of the device by the digital service
In order to be able to use the digital service on your device, it must be able to access various functions and data on your device. To do this, it is necessary for you to grant certain permissions (Art. 6 para. 1a GDPR, §25 para. 1 TDDDG).

The permissions are programmed differently by the different manufacturers. For example, individual permissions can be grouped into permission categories, or you can agree to only the permission category as a whole.

Please note that in the event of a conflict between one or more authorizations, you may not be able to use all the features of our digital service.

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

Location
We need information about your current location for the following purpose: If set by your administrator of the MPP-zConsole, to determine the location where an attack on your mobile device has taken place (e.g. malicious WLANs). The data of all actions that are carried out in both the MPP app and the MPP-zConsole are stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.

Internet Communications
The digital service requires access to the Internet via Wi-Fi or mobile communications for the following purposes: To display any attacks on your mobile device on your administrator's MPP-zConsole. The data of all actions carried out in both the MPP app, and the zConsole are stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.

Camera, microphone, USB, photos, videos, message content, etc.
The digital service requires access to the camera for the following purpose: With the help of the camera, the QR code sent can be scanned. This connects the mobile device to the created tenant in the MPP-zConsole.

Additional Permissions
Energy management
The Digital Service requires access to the energy management of the mobile device for the following purpose: In order for the app to be able to protect the mobile device in the background, an exception for automatic energy management is added to prevent the app from stopping.

Filesystem
The digital Service requires access to the filesystem of the mobile device for the following purpose: To detect unauthorized access. No data is read or transmitted.

Does the digital service send push notifications?
Push notifications are messages that are sent to your device and displayed there in a prioritized manner. The MPP app can use push notifications to show you discovered vulnerabilities and attacks on your mobile device if it is set to do so by your administrator on the MPP console. This digital service uses push notifications in the state of delivery, provided that you have given your consent during installation or first use (Art. 6 para. 1a GDPR).

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

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

Basic digital service functionality
These processing’s are always active and necessary for our digital service to function properly.

Functional
These processing’s are necessary for you to be able to navigate through the Digital Service and use essential functions. They enable basic functions, such as order processing in the online shop and access to secure areas of the digital service. The legal basis for this processing is §25 (2) No. 2 TDDDG, Art. 6 (1b) GDPR or, in the case of third countries, Art. 44 et seq. GDPR.

Processing purpose according to consent category	Login
Processing company with company address/data recipient	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Products used/short description of the service used	The MPP app and the zConsole
Description of specific processing purpose	Login, Assignment of alarms to users
Responsibilities	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Processed data	E-Mail address
Storage period	Duration of use
Legal basis (Processing)	25 para. 2 no. 2 TDDDG, Art. 6 para. 1b GDPR or, in the case of third countries, Art. 44 et seq. GDPR
Third country processing	--
Legal basis (Third country processing)	--

Optional Processing
These processing’s are used when you use additional features, such as chat. The possible functions are explained in section 1 of this Privacy Policy. The legal basis for this processing is §25 (1) TDDDG, Art. 6 (1) (a) GDPR or, in the case of third countries, Art. 49 (1) (a) GDPR.

These tools are used when you use the following features of the MPP app:

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

When you use these functions of the MPP app, you can set whether personal data or Your traffic should be routed via VPN to a gateway to Zimperium in the USA.

The legal basis for these cookies is §25 para. 1 TTDSG, Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR.

When checking links/websites with the MPP app, only the URL is transmitted to the Zimperium backend via the zConsole, which is operated in Germany.

Processing purpose according to consent category	Phishing Protection
Processing company with company address/data recipient	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Products used/short description of the service used	Phishing Protection
Description of specific processing purpose	Service provision
Responsibilities	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Processed data	IP, URL to check
Storage period	No data is stored
Legal basis (Processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR
Third country processing	USA
Legal basis (Third country processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR

Processing purpose according to consent category	VPN
Processing company with company address/data recipient	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Products used/short description of the service used	Secure VPN connection for a secure Wi-Fi network.
Description of specific processing purpose	Service provision
Responsibilities	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Processed data	IP
Storage period	No data is stored
Legal basis (Processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR
Third country processing	USA
Legal basis (Third country processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR

Processing purpose according to consent category	Conteninspection
Processing company with company address/data recipient	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Products used/short description of the service used	Zimperium, 4055 Valley View Suite 300 Dallas, TX 75244 Content inspection is an optional feature of the phishing policy. The URL of the page to be examined is transmitted directly from the device to a backend of Zimperium and examined there. To enable this communication, the IP of the device is also transmitted.
Description of specific processing purpose	Service provision
Responsibilities	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Processed data	IP, URL to check
Storage period	No data is stored
Legal basis (Processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR
Third country processing	USA
Legal basis (Third country processing)	§25 para. 1 TDDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR

Where can I find the information that is important to me?
Additional information on data protection when using our products, in particular on the purposes of use, deletion periods, etc., can be found in the data protection information for the respective product under www.telekom.de/datenschutzhinweise, in the Telekom Shop or under www.telekom.com/datenschutz.

What rights do I have?
You have the right to:

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

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

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

d) to object at any time for the future 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 para. 1 GDPR), stating these reasons. You can object to data processing for direct marketing purposes at any time without stating these reasons (Art. 21 para. 2, 3 GDPR);

e) in certain cases, request the deletion **of data within the framework of Art. 17 GDPR** - in particular if the data is no longer required for the intended purpose or is processed unlawfully, or if you have withdrawn your consent in accordance with (c) above or have declared an objection in accordance with (d) above;

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

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

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

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

To **cooperation partners** who provide services for you on their own responsibility or in connection with your telecom contract. This is the case if you commission services from such partners with us or if you consent to the involvement of the partner or if we involve the partner on the basis of a legal permission.

In addition, Deutsche Telekom is striving to cooperate with other service providers (e.g. smart home services). If you are also a user of these services, you can link your respective account to them. This linking must be done by you separately for each service. Once you have made a link, the personal data listed in this Privacy Policy may be used from your respective account for the relevant service. The respective service provider will inform you about the processing of your personal data.

Due to legal obligation: In certain cases, we are required by law to transmit certain data to the requesting government entity.

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

In some cases, your data is also processed in countries outside the European Union (i.e. in so-called third countries), currently for example:

Storage/hosting of customer data (excluding traffic data) by Amazon Web Services EMEA SARL, Microsoft Ireland Operations Ltd., Google Cloud EMEA Limited, Ireland and Salesforce.com Germany GmbH in Europe. Only administrators with technical support access from the USA are possible.

In all other respects, the following applies: If data processing takes place in third countries, this will take place insofar as you have expressly consented to this or if it is necessary for our provision of services to you or if it is provided for by law (Art. 49 GDPR).

Your data will only be processed in third countries if certain measures are taken to ensure that an adequate level of data protection is in place (e.g. adequacy decision of the EU Commission or so-called suitable safeguards, Art. 44 et seq. GDPR, (see here).

Who is responsible for data processing? Who is my contact person if I have questions about data protection at Deutsche Telekom?
The data controller is the Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn. If you have any questions, you can contact our customer service or our data protection officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.

Status of the Privacy Policy 10.02.2025