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

General information
The protection of your personal data is a high priority for Deutsche Telekom Security GmbH. It is important for us to inform you what personal data is recorded, how it is used and what options you have.

What data is recorded, how is it used, and how long is it stored?
For registration:
Registration for the app is done by the administrator in the MPP console. After starting the app, following data is recorded:

- 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 (MDS of IMEI or the serial number), for iOS (MDS of IMEI)
- Operating system of the device

Any personal data beyond this, such as your name, address or telephone number, will not be recorded by the APP.

This information is necessary for the identification and secure communication of the end device with the MPP console. All the course of action is stored for 30 days and then deleted.

When using the app
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 course of actions performed in both the MPP App and the Console is stored for 30 days and then deleted. Threat data is stored for 30 days and then deleted.

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)

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, 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)

Coupling 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)

Authorizations
In order to use the app on your device, the app must be able to access various functions and data on your device. For this purpose, it is necessary that you grant certain authorizations (Art. 6 sec. 1a GDPR).

The authorizations are programmed differently by the different manufacturers. For example, individual authorizations can be combined into authorization categories, and you can also approve only the authorization category as a whole.
Please note that if you contradict to one or more authorizations, you may not be able to use all the features of our app.

Insofar as you have granted authorizations, we use these only to the extent described below:

**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 course 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 course 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.

**Energy management**
To allow the app to protect your mobile device in the background, an automatic energy management exception is added to prevent the app from stopping.

**File system**
The app needs access to the local file system of the mobile device to detect unauthorized accesses. Data is not read or transmitted.

**Does the app 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).

Is my usage behavior evaluated, e.g., for advertising or tracking?
No, tools are not used in the MPP app to evaluate usage behavior.

**Required tools**
These tools are necessary to use the Mobile Protect Pro app. The legal basis for these tools is Art. 6 (1b) GDPR or, in the case of third countries, Art. 49 (1b) GDPR.

<table>
<thead>
<tr>
<th>Company</th>
<th>Purpose</th>
<th>Storage duration</th>
<th>Place of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche Telekom Security GmbH</td>
<td>Login</td>
<td>As long as the app is used.</td>
<td>Germany</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Phishing protection</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Secure VPN connection for a secure Wi-Fi network</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Content inspection: Content inspection is an optional</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
</tbody>
</table>

**Location data**
Location data is used 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 course 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 course 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.

**Energy management**
To allow the app to protect your mobile device in the background, an automatic energy management exception is added to prevent the app from stopping.

**File system**
The app needs access to the local file system of the mobile device to detect unauthorized accesses. Data is not read or transmitted.

**Does the app 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).

**Is my usage behavior evaluated, e.g., for advertising or tracking?**
No, tools are not used in the MPP app to evaluate usage behavior.

**Required tools**
These tools are necessary to use the Mobile Protect Pro app. The legal basis for these tools is Art. 6 (1b) GDPR or, in the case of third countries, Art. 49 (1b) GDPR.

<table>
<thead>
<tr>
<th>Company</th>
<th>Purpose</th>
<th>Storage duration</th>
<th>Place of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche Telekom Security GmbH</td>
<td>Login</td>
<td>As long as the app is used.</td>
<td>Germany</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Phishing protection</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Secure VPN connection for a secure Wi-Fi network</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
<tr>
<td>Zimperium</td>
<td>Content inspection: Content inspection is an optional</td>
<td>Data is not stored</td>
<td>USA</td>
</tr>
</tbody>
</table>

**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.

**Note on unused 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 that is important to me?**
This data protection notice provides an overview of the points that apply to the processing of your data in this app by Deutsche Telekom Security GmbH.

For more information, including on data protection in general and in specific products, visit [https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz](https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz) and [http://www.telekom.de/datenschutzhinweise](http://www.telekom.de/datenschutzhinweise).

**Who is responsible for data processing? Who should I contact if I have questions about data privacy at Telekom?**
The data controller is Deutsche Telekom AG. If you have any questions, please contact our Customer Service or contact our data protection officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 55113 Bonn, Germany, datenschutz@telekom.de.

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

a) To request information about the categories of processed data, the purposes of processing, any recipients of the data, the planned storage duration (Art. 15 GDPR);
b) To demand 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 sec. 3 GDPR);
d) To object to data processing that is to be carried out on the basis of a legitimate interest due to your particular situation (Art. 21 (1) GDPR);
e) To request the deletion of data in certain cases, within the framework of Art. 17 GDPR, - in particular insofar as the data is no longer required for the intended purpose or is processed unlawfully, or you have revoked your consent in accordance with (c) above or declared a contradiction in accordance with (d) above;
f) To request the restriction of data under certain conditions, 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 common machine-readable format, such as CSV, and transmit it to others if necessary (Art. 20 GDPR);
h) To complain about data processing to the competent supervisory authority (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).

**Who does Telekom share my data with?**
With processors, they are 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.

With cooperation partners, who provide services on their own responsibility for you or in connection with your Deutsche Telekom Security contract. This is the case if you commission services of such partners from us or if you...
consent to the integration of the partner or if we integrate the partner on the basis of a legal permission.

**Due to legal obligation:** In certain cases, we are legally obliged to transmit certain data to the requesting government agency. Example: Upon presentation of a court order, we are obliged under Section 101 of the Copyright Act to provide owners of copyrights and ancillary copyrights with information about customers who are alleged to have offered copyrighted works on Internet file-sharing networks.

**Where is my data processed?**
Your data will be processed in Germany and in 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), following shall be applicable,

a) insofar as you have expressly consented thereto (Art. 49 sec. 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 USA, which disproportionately interfere with the data protection of European citizens,

b) or as far as it is necessary for our service provision to you (Art. 49 sec. 1b GDPR),

c) or as far as it is provided by law (Art. 6 sec. 1c GDPR).

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

This privacy information was last updated January 2021