Datenschutzhinweise der Deutsche Telekom Security GmbH („Telekom“) für die Nutzung der Mobile Protect Pro App (MPP)

Der Schutz Ihrer persönlichen Daten hat für die Deutsche Telekom Security GmbH einen hohen Stellenwert. Es ist uns wichtig, Sie darüber zu informieren, welche persönlichen Daten erfasst werden, wie diese verwendet werden und welche Gestaltungsmöglichkeiten Sie dabei haben.

Welche Daten werden erfasst, wie werden sie verwendet und wie lange werden sie gespeichert?
Bei der Nutzung der MPP-App, im folgenden Online-Dienst genannt:

Bei der Registrierung:
Die Registrierung für die App erfolgt durch den Administrator in der MPP-zConsole. Nach dem Starten der App werden folgende Daten erfasst:

- Bis einschließlich der Version 4.7 Zugangsdaten (Benutzername/E-Mail und Passwort) – ab Version 4.8.xx eindeutiger Token
- Hashwert des Gerätes (MD5 der IMEI oder der Seriennummer), bei iOS (MD5 der IMEI)
- Betriebssystem des Gerätes

Darüber hinaus gehende personenbezogene Daten, wie z. B. Ihr Name, Ihre Anschrift oder Telefonnummer, werden von der APP nicht erfasst.

Diese Angaben sind zur Identifizierung und sicheren Kommunikation des Endgerätes mit der MPP-zConsole notwendig.

Die Threatdaten – diese umfassen alle Events, die von der App an die zConsole übermittelt werden, sowie das Auditlog der zConsole – werden standardmäßig nach 30 Tagen gelöscht, auf Kundenwunsch kann diese Frist auf bis zu 90 Tage verlängert werden. Device und Userdaten werden binnen 7 Tagen gelöscht. Alle anderen Daten werden zum Vertragsende gelöscht.

Bei der Nutzung der App:
Die MPP-App schützt die vom Kunden administrierten mobilen Endgeräte. Sie generiert Alarme für den die Administratoren und - falls gewünscht einstellbar in der Konsole - für den Nutzer des mobilen Gerätes bei Gefahren für Betriebssystem, Netzwerkverbindungen oder gespeicherten Daten auf dem Gerät.

Die MPP- App beobachtet die unterschiedlichsten Parameter und Vektoren, die aus

den mobilen Endgeräten, deren Betriebssystemen und Netzwerkverbindungen ausgelesen werden können. Durch die Korrelation dieser Werte kann ein Normalzustand interpretiert und Anomalien im System festgestellt werden. Auf diese Weise werden bekannte und unbekannte Angriffe auf das mobile Endgerät erkannt. Es werden die Schnittstellen des Gerätes, seine Netzwerkverbindungen, das Betriebssystem und die Applikationsebene überwacht. Das Beobachten dieser Parameter und deren Interpretation erfolgt in der App auf dem mobilen Endgerät. Die Schutzwirkung der App ist auch gegeben, wenn keine Verbindung mit der Konsole über das Internet besteht.

In den Privacy Settings der MPP-zConsole kann der Administrator definieren, ob und welche Daten von der Anwendung erhoben werden sollen. Da ein Angriff lokal auf dem Endgerät durch die z9 Engine erkannt wird, sind nur sehr wenig Daten zur Identifizierung und sicheren Kommunikation des Endgerätes mit der MPP-zConsole notwendig. Die Daten aller Handlungsverläufe, die sowohl in der MPP-App als auch in der MPP-zConsole durchgeführt werden, werden für 30 Tage gespeichert und anschließend gelöscht. Threatdaten werden für 30 Tage gespeichert und anschließend gelöscht.

Folgende Daten können bei der Verwendung der App erfasst werden:

- Für Signaturupdates („pull‘ der Signatur) und Prüfung von Zertifikaten (SSL-Strip) verbindet sich das Endgerät mit dem Zimperium Backend. Für die Kommunikation wird die IP des Endgerätes benötigt, somit wird diese in die USA übermittelt. Weder speichert Zimperium diese Zugriffe noch werden die Daten ausgewertet oder sonst wie verarbeitet.

Bei Verwendung der MPP-Android-App:

- Eindeutiger Push Token der App auf dem Gerät, um Nachrichten von der Konsole zu verifizieren
- Lokation: GPS-Längen- und Breitengrade - auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS-Daten ermittelt. (optional einstellbar)
- Netzwerk: MAC- und IP Address, BSSID, SSID (optional einstellbar)
- Gerät: Betriebssystem, Betriebssystem Version, Model, Jailbroken, Entwickler Option
- Liste installierter Apps (optional einstellbar)
- Zur Analyse und Einstufung von bisher unbekannten Apps, können diese direkt vom Gerät an Zimperium übertragen werden. Für die Kommunikation wird die IP des Endgerätes benötigt, somit wird diese in die USA übermittelt. Weder speichert Zimperium diese Zugriffe noch werden die Daten ausgewertet oder sonst wie verarbeitet.
- Verbindungsstatus (WLAN oder 3G) (optional einstellbar)
- Benutzer Informationen: Benutzername /E-Mail (aus der Konsole ermittelt

Bei Verwendung der MPP- iOS-App:

- Eindeutiger Push Token der App auf dem Gerät, um Nachrichten von der Konsole zu verifizieren
- Lokation: GPS-Längen- und Breitengrade – auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS-Daten ermittelt. (optional einstellbar)
- Netzwerk: MAC- und, IP Address BSSID, SSID (optional einstellbar)
- Gerät: Betriebssystem, Betriebssystem Version, SNO (wenn verfügbar)
- Liste installierter Apps (nur verfügbar, wenn ein MDM angebunden ist)
- Verbindungsstatus (WLAN oder 3G) (optional einstellbar)
- Benutzer Informationen: Benutzername/E-Mail (aus der Konsole ermittelt)

Bei der Entdeckung eines Angriffs:

- Zeit des Ereignisses
- Angriffsbezeichnung
- Lokation: GPS-Längen- und Breitengrade – auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS-Daten ermittelt. (optional einstellbar)
- Erkennung der App (Binärcode, Hashwert)
- Netzwerk: Mac und IP-Adresse, Router BSSID und SSID, Benachbarte WLAN Netzwerke (BSSID / SSID), Netzwerkstatistiken (bestehende TCP / UDP Verbindungen zum Zeitpunkt des Angriffs inclusive IP und Port Adresse), ARP Tabelle aller lokalen Hosts im WLAN, die mit dem Gerät kommunizieren sowie Informationen zur Basisstation (optional einstellbar)
- Gerät: Betriebssystem, Betriebssystem Version, Gerätemodel, IMEI, aktive APP (Android), Verbindungsstatus (WLAN oder 3G), ARP-Tabelle des Gerätes (vor und nach dem Angriff), Liste von (zum Zeitpunkt des Angriffes) aktiven Prozessen, im Fall von Angriffen auf das Filesystem der vollqualifizierte Datei-/Ordnerpfad die auf dem Gerät geändert wurden.
- App Forensik: Auf dem Gerät installiert Apps, Paketname der entdeckten Schadsoftware/App (optional einstellbar)
- Nur iOS: Im Fall von Angriffen auf das Profil, werden alle Profile

Informationen an die Konsole übermittelt. (nur in Verbindung mit einem MDM verfügbar) (Art. 6 Abs. 1b DSGVO, §25 Abs. 2 Nr. 2 TTDSG)

Wenn Sie unseren Online-Dienst nutzen, verzeichnen unsere Server vorübergehend den Domain-Namen oder die IP- Adresse Ihres Endgerätes sowie weitere Daten, wie z. B. die angefragten Inhalte oder den Antwort-Code.

Die protokollierten Daten werden ausschließlich für Zwecke der Datensicherheit, insbesondere zur Abwehr von Angriffsversuchen auf unseren Webserver verwendet (Art. 6 Abs. 1f DSGVO). Sie werden weder für die Erstellung von individuellen Anwenderprofilen verwendet noch an Dritte weitergegeben und werden nach spätestens 7 Tagen gelöscht. Die statistische Auswertung anonymisierter Datensätze behalten wir uns vor.

Text oder Video-Chat
Kopplung mit anderen Systemen: Die MPP-App bietet eine optionale Integration in ein Mobile Device Management (MDM). In den Privacy Settings der MPP-Konsole kann der Administrator definieren, welche Daten von der Anwendung erhoben werden sollen. Dabei können folgende Daten erfasst werden:

- Hashwert der lokalen z9 Engine (Anomalieerkennungssoftware) und Schadsoftware Datenbank
- Lokation: GPS-Längen- und Breitengrade – je nach den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS-Daten ermittelt. (optional einstellbar)
- Netzwerk: Router BSSID und SSID (optional einstellbar)
- Gerät: IP und MAC-Adresse des Gerätes
- App Forensik: Aktive Apps auf dem Gerät (Android, iOS)

Verbindungsstatus (WLAN oder 3G) (optional einstellbar). (Art. 6 Abs. 1a DSGVO)

Berechtigungen für Zugriffe auf Daten und Funktionen des Endgerätes durch den Online-Dienst
Um den Online-Dienst auf Ihrem Endgerät nutzen zu können, muss dieser auf verschiedene Funktionen und Daten Ihres Endgeräts zugreifen können. Dazu ist es erforderlich, dass Sie bestimmte Berechtigungen erteilen (Art. 6 Abs. 1a DSGVO, §25 Abs. 1 TTDSG).

Die Berechtigungen sind von den verschiedenen Herstellern unterschiedlich programmiert. So können z. B. Einzelberechtigungen zu Berechtigungskategorien zusammengefasst sein und Sie können auch nur der Berechtigungskategorie insgesamt zustimmen.

- Standortdaten
  Wir benötigen Informationen zu Ihrem aktuellen Standort zu folgendem Zweck Sofern von Ihrem Administrator der MPP-zConsole eingestellt, um die Lokation wo ein Angriff auf ihr mobiles Endgerät stattgefunden hat, zu bestimmen (z.B. maliziöse WLANS). Die Daten aller Handlungsverläufe, die sowohl in der MPP-App als auch in der MPP-zConsole durchgeführt werden, werden für 30 Tage gespeichert und anschließend gelöscht. Threatdaten werden für 30 Tage gespeichert und anschließend gelöscht.
- Internet-Kommunikation
  Der Online-Dienst benötigt Zugriff auf das Internet über W-LAN oder Mobilfunk für folgende Zwecke Um ggf. Angriffe auf Ihr mobiles Endgerät auf der MPP-zConsole Ihres Administrators anzuzeigen. Die Daten aller Handlungsverläufe, die sowohl in der MPP-App als auch in der Konsole durchgeführt werden, werden für 30 Tage gespeichert und anschließend gelöscht. Threatdaten werden für 30 Tage gespeichert und anschließend gelöscht.
- Kamera, Mikrofon, USB, Fotos, Videos, Nachrichteninhalte etc.
  Der Online-Dienst benötigt Zugriff auf Kamera zu folgendem Zweck Mithilfe der Kamera kann der zugesendete QR-Code gescannt werden. Dadurch wird das mobile Endgerät mit dem erstellten Tenant in der MPP-zConsole verbunden.
- Energiemanagement
  Der Online-Dienst benötigt Zugriff auf das Energiemanagement des mobilen Endgerätes>> zu folgendem Zweck Damit die App im Hintergrund das mobile Endgerät schützen kann wird eine Ausnahme für das automatische Energiemanagement hinzugefügt, um ein Stopp der App zu verhindern.
- Filesystem
  Der Online-Dienst benötigt Zugriff auf das lokale Filesystem des mobilen Endgerätes zu folgendem Zweck Um unberechtigte Zugriffe zu detektieren. Es werden keine Daten ausgelesen oder übermittelt.

Sendet der Online-Dienst Push-Benachrichtigungen?
Push-Benachrichtigungen sind Nachrichten, die auf Ihr Endgerät gesendet und dort priorisiert dargestellt werden. Die MPP-App kann Push-Benachrichtigungen verwenden, um Ihnen entdeckte Schwachstellen und Angriffe auf Ihrem mobilen Endgerät anzuzeigen, wenn es von Ihrem Administrator auf der MPP-Konsole so eingestellt ist. Dieser Online-Dienst verwendet Push-Benachrichtigungen im Auslieferungszustand, sofern Sie bei der Installation oder bei der ersten Nutzung eingewilligt haben (Art. 6 Abs. 1a DSGVO).

Sie können Ihre Einwilligung jederzeit widerrufen. Dafür entfernen Sie bitte im Hauptmenü der MPP-App unter Benachrichtigungen den Haken neben "Push aktivieren".

Wird mein Nutzungsverhalten ausgewertet, z. B. für Werbung oder Tracking?
Nein, in der MPP-App werden keine Tools zur Auswertung des Nutzungsverhaltens eingesetzt.

Erforderliche Tools
Diese Tools sind notwendig, damit Sie die MPP-App und wesentliche Funktionen nutzen können. Rechtsgrundlage für diese Tools ist §25 Abs. 2 Nr. 2 TTDSG, Art. 6 Abs. 1b DSGVO bzw. bei Drittstaaten Art. 44 ff. DSGVO.

Firma	Zweck	Speicherdauer	Land
Deutsche Telekom Security GmbH	Login	So lange wie die App genutzt wird	Deutschland

Bei optionaler Nutzung von Tools
Diese Tools werden dann verwendet, wenn sie folgende Funktionen der MPP-App nutzen:

- Phishing Schutz
- Sichere VPN-Verbindung für ein sicheres Wi-Fi Netzwerk

Wenn Sie diese Funktionen der MPP-App benutzen, können Sie einstellen, ob personenbezogene Daten bzw. Ihr Traffic über VPN an ein Gateway an Zimperium in den USA geroutet werden soll.

Rechtsgrundlage für diese Cookies ist §25 Abs. 1 TTDSG, Art. 6 Abs. 1a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1a DSGVO.

Bei der Überprüfung von Links/Webseiten mit der MPP-App wird ausschließlich die URL über die, in Deutschland betriebene, zConsole an das Zimperium Backend übermittelt.

Firma	Zweck	Speicherdauer	Land
Zimperium	Phishing Schutz	Es werden keine Daten gespeichert	USA
Zimperium	Sichere VPN-Verbindung für ein sicheres Wi-Fi Netzwerk	Es werden keine Daten gespeichert	USA
Zimperium	Contentinspection: Die Contentinspection ist eine optionale Funktion der Phishing Policy. Dabei wird vom Endgerät die URL der zu untersuchenden Seite direkt an ein Backend von Zimperium übermittelt und dort untersucht. Um diese Kommunikation zu ermöglichen, wird die IP des Endgerätes mit übertragen.	Es werden keine Daten gespeichert	USA

Analytische Tools
Wir verwenden für den Versand von Push-Benachrichtigungen bei Android, Firebase Cloud Messaging, einem Bestandteil von Firebase der Firma

Google. In dem Zusammenhang stehende Codefragmente mit einem Bezug auf weitere Firebase Tools wie Google AdMob, Google CrashLytics, Google Firebase Analytics usw. sind möglich.

Wo finde ich die Informationen, die für mich wichtig sind?
Dieser Datenschutzhinweis gibt einen Überblick über die Punkte, die für die Verarbeitung Ihrer Daten in diesem Online-Dienst durch die Telekom gelten.

Weitere Informationen, auch zum Datenschutz im allgemeinen und in speziellen Produkten, erhalten Sie auf https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz und unter http://www.telekom.de/datenschutzhinweise.

Wer ist verantwortlich für die Datenverarbeitung? Wer ist mein Ansprechpartner, wenn ich Fragen zum Datenschutz bei der Telekom habe?
Datenverantwortliche ist die Deutsche Telekom AG. Bei Fragen können Sie sich an unseren Kundenservice wenden oder an unseren Datenschutzbeauftragten, Herrn Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.

Welche Rechte habe ich?
Sie haben das Recht,

a. **Auskunft** zu verlangen zu Kategorien der verarbeiteten Daten, Verarbeitungszwecken, etwaigen Empfängern der Daten, der geplanten Speicherdauer (Art. 15 DSGVO);

b. die **Berichtigung** bzw. Ergänzung unrichtiger bzw. unvollständiger Daten zu verlangen (Art. 16 DSGVO);

c. eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu **widerrufen** (Art. 7 Abs. 3 DSGVO);

d. einer Datenverarbeitung, die aufgrund eines berechtigten Interesses erfolgen soll, aus Gründen zu **widersprechen**, die sich aus Ihrer besonderen Situation ergeben (Art 21 Abs. 1 DSGVO);

e. in bestimmten Fällen im Rahmen des Art. 17 DSGVO die **Löschung** von Daten zu verlangen - insbesondere soweit die Daten für den vorgesehenen Zweck nicht mehr erforderlich sind bzw. unrechtmäßig verarbeitet werden, oder Sie Ihre Einwilligung gemäß oben (c) widerrufen oder einen Widerspruch gemäß oben (d) erklärt haben;

f. unter bestimmten Voraussetzungen die **Einschränkung** von Daten zu verlangen, soweit eine Löschung nicht möglich bzw. die Löschpflicht streitig ist (Art. 18 DSGVO);

g. auf **Datenübertragbarkeit**, d.h. Sie können Ihre Daten, die Sie uns bereitgestellt haben, in einem gängigen maschinenlesbaren Format, wie z.B. CSV, erhalten und ggf. an andere übermitteln (Art. 20 DSGVO;)

h. sich bei der zuständigen **Aufsichtsbehörde** über die Datenverarbeitung zu beschweren (für Telekommunikationsverträge: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit; im Übrigen: Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen).

An wen gibt die Telekom meine Daten weiter?
An **Auftragsverarbeiter**, das sind Unternehmen, die wir im gesetzlich vorgesehenen Rahmen mit der Verarbeitung von Daten beauftragen, Art. 28 DSGVO (Dienstleister, Erfüllungsgehilfen). Die Telekom bleibt auch in dem Fall weiterhin für den Schutz Ihrer Daten verantwortlich. Wir beauftragen Unternehmen insbesondere in folgenden Bereichen: IT, Vertrieb, Marketing, Finanzen, Beratung, Kundenservice, Personalwesen, Logistik, Druck.

An **Kooperationspartner**, die in eigener Verantwortung Leistungen für Sie bzw. im Zusammenhang mit Ihrem Telekom-Vertrag erbringen. Dies ist der Fall, wenn Sie Leistungen solcher Partner bei uns beauftragen oder wenn Sie in die Einbindung des Partners einwilligen oder wenn wir den Partner aufgrund einer gesetzlichen Erlaubnis einbinden.

Aufgrund gesetzlicher Verpflichtung: In bestimmten Fällen sind wir gesetzlich verpflichtet, bestimmte Daten an die anfragende staatliche Stelle zu übermitteln.

Wo werden meine Daten verarbeitet?
Ihre Daten werden in Deutschland und im europäischen Ausland verarbeitet. Findet eine Verarbeitung Ihrer Daten in Ausnahmefällen auch in Ländern außerhalb der Europäischen Union (in sog. Drittstaaten) statt, geschieht dies,

- soweit Sie hierin ausdrücklich eingewilligt haben (Art. 49 Abs. 1a DSGVO). (In den meisten Ländern außerhalb der EU entspricht das Datenschutzniveau nicht den EU Standards. Dies betrifft insbesondere umfassende Überwachungs- und Kontrollrechte staatlicher Behörden, zB. in den USA, die in den Datenschutz der europäischen Bürgerinnen und Bürger unverhältnismäßig eingreifen,
- oder soweit es für unsere Leistungserbringung Ihnen gegenüber erforderlich ist (Art. 49 Abs. 1b DSGVO),
- oder soweit es gesetzlich vorgesehen ist (Art. 6 Abs. 1c DSGVO).

Darüber hinaus erfolgt eine Verarbeitung Ihrer Daten in Drittstaaten nur, soweit durch bestimmte Maßnahmen sichergestellt ist, dass hierfür ein angemessenes Datenschutzniveau besteht (z.B. Angemessenheitsbeschluss der EU-Kommission oder sog. geeignete Garantien, Art. 44ff. DSGVO).

Stand des Datenschutzhinweises März 2024