Datenschutzhinweise der Deutsche Telekom Security GmbH („Telekom“) für Mobile Protect Pro Konsole (MPP) / Data privacy information Deutsche Telekom Security GmbH („Telekom“) for Mobile Protect Pro Console (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 MPP-zConsole, im folgenden Online-Dienst genannt:

Bei der Registrierung:
Für den Login an der MPP-zConsole wird ein User sowie ein Passwort benötigt:

- Username (Vor- und Nachname)
- E-Mail-Adresse
- Passwort (nur für Administratoren)
- Telefonnummer (optional)

Beim Login:
Userkennung und Uhrzeit des Logins werden im Auditlog gespeichert

Bei Nutzung:
Getätigte Änderungen an den Einstellungen werden im Auditlog gespeichert

Weitere Daten:
Sämtliche von den Mobilen Endgeräten erhobenen Daten sind in der MPP-zConsole sichtbar. Welche Daten erhoben werden wird in der MPP-zConsole eingestellt Für weitere Informationen zu Datenschutzhinweise der App klicken Sie bitte hier.

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.

Für die Rechnungsstellung wird die Anzahl der in der MPP-zConsole registrierten Geräte erfasst (Art. 6 Abs. 1b DSGVO, §25 Abs. 2 Nr. 2 TTDSG)

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

Erforderliche Tools
Diese Tools sind notwendig, damit die MPP-zConsole einwandfrei funktioniert. Rechtsgrundlage für diese Tools ist §25 Abs. 2 Nr. 2 TTDSG, Art. 6 Abs. 1b DSGVO bzw. bei Drittstaaten Art. 44 ff. DSGVO.

The protection of your personal data has a high priority for Deutsche Telekom Security. 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 zConsole, hereinafter referred to as online service:

For registration:
A username and password are required to log in to the zConsole:

- Username (first and last name)
- E-mail address
- Password (for administrators only)
- Phone number (optional)

For login:
User ID and time of login are stored in the audit log

For use:
Changes made to the settings are saved in the audit log

Other data:
All data collected from mobile devices is visible in the zConsole. The data collected, is set in the zConsole. For more information regarding the app's privacy policy, please click here.
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.
For invoicing, the number of devices registered in the MPP-zConsole is recorded

(Art. 6 para. 1b GDPR, §25 para. 2 No. 2 TTDSG (Telecommunications Telemedia Data Protection Act)).

Is my usage behavior evaluated, e.g. for advertising or tracking?
No, the MPP-zConsole 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. 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

Firma	Zweck	Speicherdauer	Land
Deutsche Telekom Security GmbH	Login	So lange wie Mobile Protect Pro genutzt wird	Deutschland
Zimperium	Dieses Cookie (csrftoken) ist mit der Django-Webentwicklungsplattform für Python verknüpft. Es soll eine Website vor bestimmten Softwareangriffen auf Webformulare schützen	Nutzungsdauer / Sessiondauer	Deutschland
Zimperium	Sitzungstoken sind Daten, die in der Netzwerkkommunikation (häufig über HTTP) verwendet werden, um eine Sitzung zu identifizieren. Zudem wird es verwendet, um mehrere zusammengehörige Anfragen eines Benutzers zu erkennen und einer Sitzung zuzuordnen.	Nutzungsdauer / Sessiondauer	Deutschland
Zimperium	zme wird verwendet, um die Client-Website über den Kunden (system_token) zu informieren, der dem Benutzer zugeordnet ist. Sie gelten auch als Erstanbieter-Cookies. Diese werden von der vom Benutzer besuchten Website gesetzt.	Nutzungsdauer / Sessiondauer	Deutschland

Bei optionaler Nutzung von Tools
Diese Tools werden dann verwendet, wenn sie folgende Funktionen der Mobile Protect Pro nutzen:

- Phishing Schutz
- Sichere VPN-Verbindung für einen sicheren Wi-Fi Netzwerk

Wenn Sie diese Funktionen der Mobile Protect Pro App benutzen, können Sie einstellen, ob personenbezogenen Daten bzw. Ihr Traffic über VPN an ein Gateway an Zimperium in den USA geroutet werden. Rechtsgrundlage für diese Cookies ist §25 Abs. 1 TTDSG, Art. 6 Abs. 1a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1a DSGVO.

Firma	Zweck	Speicherdauer	Land
Zimperium	Phishing Schutz	Es werden keine Daten gespeichert	USA
Zimperium	Sichere VPN-Verbindung für einen sicheren Wi-Fi Netzwerk	Es werden keine Daten gespeichert	USA

Company	Purpose	Storage duration	Place of processing
Deutsche Telekom Security GmbH	Login	As long as the Mobile Protect Pro is used.	Germany
Zimperium	This cookie (csrftoken) is linked to the Django web development platform for Python. It is designed to protect a website from certain software attacks on web forms.	Duration of use / session duration	Germany
Zimperium	Session tokens are data, which is used in network communication (often over HTTP) to identify a session. In addition, it is used to recognize multiple related requests from a user and assign them to a session.	Duration of use / session duration	Germany
Zimperium	zme is used to inform the client site about the customer (system_token), which is assigned to the user. They are also considered first-party cookies. These are set by the website visited by the user.	Duration of use / session duration	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 the USA.

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	Contentinspection: Die Contentinspection ist eine optionale Funktion der Phishingpolicy. 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. Diese Tools sind allerdings nicht aktiv und werden für keinerlei Auswertungen genutzt.

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).

Zimperium	Zimperium	Content inspection: Content inspection is an optional feature of the phishing policy. The URL of the page to be examined is transmitted directly from the end device to a Zimperium backend and it is examined there. To enable this communication, the IP of the end device is also transmitted	Data is not stored

Analytic tools
For sending push notifications on Android, we use 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.

The legal basis for these tools 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.

Is the audit log stored and for how long?
The audit log stores action histories that are performed in both the MPP AppMPP app and the MPP-zConsole. This includes, for example, logging into the MPP app or making changes in the MPP-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 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 http://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, 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);

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

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 authorit**y 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