



Datenschutzhinweise der Deutschen Telekom Geschäftskunden GmbH („Telekom“) für Nutzung der MDM Telekom App

Der Schutz Ihrer persönlichen Daten hat für die Deutsche Telekom Geschäftskunden 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?

Erforderliche Verarbeitungen bei der Erbringung des digitalen Dienstes (Art. 6 Abs. 1b DSGVO, §25 Abs. 2 Nr. 2 TDDDG)

Bei der Nutzung der MDM – Deutsche Telekom App, im folgenden digitaler Dienst genannt:

Bei der Registrierung:

Um sich für den digitalen Dienst zu registrieren, geben Sie den von Ihrem IT-Administrator vorgegebenen Usernamen und das Passwort ein (in der Regel Username und E-Mail-Passwort für Ihren Firmen-Mailaccount). Diese Angaben sind für die Nutzung des MDM/UEM Service erforderlich und werden zusammen mit den unter b) aufgeführten Daten auf unseren Servern bis zu 30 Tage nach Ende der Vertragslaufzeit des MDM/UEM Services gespeichert (Art. 6 Abs. 1 b DSGVO) um ihrem Unternehmen im Bedarfsfalle die Daten zu Kontroll- und/oder Migrationszwecken zu überlassen.

Bei der Nutzung des digitalen Dienstes:

Wenn Sie den digitalen Dienst nutzen, verzeichnen unsere Server temporär die IP-Adresse Ihres Gerätes und andere technische Merkmale, wie zum Beispiel die angefragten Inhalte (Art. 6 Abs. 1b DSGVO). In dieser App haben Sie die Möglichkeit neben den Eingaben per Tastatur auch den Text zu diktieren. Die Spracheingabe (Google) oder Diktier-funktion (Apple) ist eine Funktionalität, die das Betriebssystem unserer App zur Verfügung stellt. Bei der Verwendung wird die Sprache durch einen Dritten (z. B. Apple oder Google) als Verantwortlichen verarbeitet und das Ergebnis an unsere App geliefert und im Eingabe-feld ausgegeben. Zu Details zu der Funktionalität, und wie Sie die Nutzung ein- bzw. ausschalten können, informieren Sie sich bitte bei dem jeweiligen Betriebssystemhersteller.

Sonstiges

Für die vertragsgemäße Erbringung unseres MDM/UEM-Service ist es notwendig, dass folgende Daten auf dem UEM Server gespeichert und verarbeitet werden. In der App selbst werden diese Daten nicht gespeichert.

Kundendaten

- Firmenname
- Firmenadresse
- Name des Fleet-Administrator(s)/ IT Verantwortlichen
- Kontakt Details
- Vertrags-ID und Laufzeit
- System Admin Login Detail

Device Management (Kunden- und Nutzerdaten)

- Parameter der VPN-Verbindung
- Parameter des Email-Systems, Active Directory / LDAP
- URL der MDM Instanz des Kunden
- Labels (internes Identifizierungsmerkmal der Kundenorganisation)
- User ID (internes Identifizierungsmerkmal)
- User (Mitarbeiter) Name
- E-Mail-Adresse des Users (Mitarbeiters)
- MSISDN / IMSI
- Operator Name
- Country Code und Name

- Device Inventory
- Device Daten
 - Typ
 - Modell
 - IMEI
 - Device ID
 - Speichergröße (genutzt / frei)
 - RAM Größe (genutzt / frei)
 - Firmware Version
 - SW / auf dem Device befindliche Applikationen
 - Vital Signs (Battery, Signalstärke)
 - Netzwerk, in dem das Device gerade eingebucht ist
 - Höhe des genutzten Datenvolumens (MB, Anz. SMS) und Anzahl der Telefonminuten, um dem Administrator ihrer Firma die Möglichkeit zu geben Warnschwellen zu setzen (keine Rechnungsdaten), Ortsinformation (Geodaten) falls Sie als Endnutzer das freigegeben haben, Devicestatus auf der Plattform (pending / connected / active / wiped / retired).

Diese Daten werden bis zu 30 Tage nach Ende der Vertragslaufzeit des MDM/UEM Services gespeichert, um dem Firmenkunden im Bedarfsfalle die Daten zu Kontroll- und / oder Migrationszwecken zu überlassen.

Berechtigungen

Um den MDM/UEM Service für Ihr Gerät zu erbringen, muss der digitale Dienst auf verschiedene Funktionen und Daten Ihres Endgeräts zugreifen können. Dazu ist es erforderlich, dass Sie bestimmte Berechtigungen erteilen (Art. 6 Abs. 1 a DSGVO).

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

Bitte beachten Sie dabei aber, dass Sie im Falle eines Widerspruchs gegebenenfalls nicht sämtliche Funktionen unseres Service nutzen können.

Soweit Sie Berechtigungen erteilt haben, nutzen wir diese nur im nachfolgend beschriebenen Umfang:

Standortdaten

Der digitale Dienst benötigt Informationen zu Ihrem aktuellen Standort zu folgendem Zweck: Jailbreak Erkennung bei iOS Endgeräten, zur Lokalisierung des Gerätes bei Diebstahl oder Verlust; maximale Speicherdauer nach erfolgter Ortung: 72h.

Kontakte / Adressbuch

Der digitale Dienst benötigt Zugriff auf die Kontakte/Adressbuch zu folgendem Zweck:

- Unterscheidung zwischen Business Kontakten und privaten Kontakten
- Erstellung und Konfiguration beruflich genutzter E-Mail-Konten
- Löschung der Business Kontakte und geschäftlicher E-Mail-Konten bei Bedarf (Sie verlassen die Firma, Ihr EG ist nicht mehr richtlinienkonform, bei Diebstahl oder Verlust des EG) um die Firmendaten zu schützen. Es erfolgt keine Speicherung der Daten außerhalb des Endgerätes oder in der genutzten App.

Internetkommunikation

Der digitale Dienst benötigt Zugriff auf das Internet über W-LAN oder Mobilfunk für folgende Zwecke:

- Zur Erbringung des MDM-/UEM-Services (Installation der

Kommunikationsrichtlinien Ihrer Firma etc.)

- Applikationsdownload, Update der Applikationen
- Zusenden von Nachrichten

Kamera, Mikrofon, USB, Fotos, Videos, Nachrichteninhalte etc.

Der digitale Dienst benötigt Zugriff auf alle Medien zu folgendem Zweck:

Erbringung des UEM Services (Medienkontrolle wie z.B. Sperrung der Kamera, Trennung von beruflichen und privaten Daten, Schutz der beruflichen Daten, Zwangsverschlüsselung der Daten auf externen Datenträgern wie USB-Stick und SSD-Karte). Es erfolgt keine Speicherung von Inhalten auf unseren UEM- Servern.

Geräte-ID, Gerätedaten, Vital Signs

Der digitale Dienst benötigt Zugriff auf verschiedene Gerätedaten zu folgenden Zwecken:

- Zur Erbringung des UEM Services ist eine eindeutige Geräteidentifikation notwendig
- Zustand des Gerätes, um den UEM-Service in jeder Situation sicherzustellen
- Sperren des Gerätes bei Diebstahl, Verlust
- Reaktionen je nach Compliance Status des Gerätes

Diese Daten werden nach Entfernen des Endgerätes aus dem Management nach einer festgelegten Zeit (vom IT-Administrator einstellbar, Default 180 Tage) bzw. spätestens 30 Tage nach Ende der Vertragslaufzeit des MDM- / UEM- Services gelöscht, je nachdem was der früheste Zeitpunkt ist.

Zugriff auf Apps

Der digitale Dienst benötigt Zugriff auf die installierten Apps zu folgenden Zwecken:

- Kontrolle des Compliance Zustands der abgesicherten Firmen Apps
- Compliance Reaktion auf Apps, die den Firmenrichtlinien widersprechen (z.B. Löschung einer verbotenen Applikation)
- Absicherung der Daten, die in den geschäftlich genutzten Apps gespeichert werden

Alle Zugriffe werden zu Nachweiszwecken (Informationspflicht) in den Serverlogfiles (es erfolgt keine Speicherung in der App) maximal 90 Tage gespeichert. Logfiles, die älter als 90 Tage sind, werden automatisch vom System gelöscht

Weitere Berechtigungen (z.B. Zugriff auf Apps)

Der digitale Dienst benötigt die unten aufgeführten Zugriffe zu folgendem Zweck: Vertrags-konforme Erbringung des von Ihrer Firma beauftragten MDM/UEM Services:

- Auf Daten des E-Mail-Anbieters zugreifen
- Daten aus dem Internet abrufen
- Verknüpfungen installieren
- Beim Start ausführen
- Auf Bluetooth-Einstellungen zugreifen
- Nahfeldkommunikation steuern
- Pairing mit Bluetooth-Geräten durchführen
- WLAN-Verbindungen herstellen und trennen
- Synchronisierung aktivieren oder deaktivieren
- Google-Servicekonfiguration lesen
- Ruhezustand deaktivieren
- Netzwerkverbindungen abrufen
- Systemeinstellungen ändern
- Zugriff auf alle Netzwerke
- Verknüpfungen deinstallieren

Alle Zugriffe werden zu Nachweiszwecken in den Serverlogfiles maximal 90 Tage gespeichert. Es erfolgt keine Speicherung in der App. Logfiles, die älter als 90 Tage sind, werden automatisch vom System gelöscht.

Sendet der digitale Dienst Push-Benachrichtigungen?

Push-Benachrichtigungen sind Nachrichten, die an Ihr Gerät gesendet und dort priorisiert dargestellt werden. Dieser digitale Dienst verwendet Push-Benachrichtigungen im Auslieferungszustand, sofern Sie bei der App-Installation oder bei der ersten Nutzung eingewilligt haben (Art. 6 Abs. 1 a DSGVO).

Damit wir Ihnen wichtige Hinweise zur sicheren Nutzung der MDM/UEM Applikation senden können, nutzen wir Googles Cloud Firebase Messaging als Bestandteil der Google Firebase Bibliothek. Sie können den Empfang von Push-Benachrichtigungen jederzeit in den Einstellungen Ihres Gerätes deaktivieren. Bitte beachten Sie dabei aber, dass dann der UEM Service nur eingeschränkt genutzt werden kann.

Zwei zusätzliche Tools sind integraler Bestandteil der Google Firebase Bibliothek die bei einer App-Analyse als Tracker ausgewiesen werden und die nicht aus der Bibliothek gelöscht werden können: „Google Crashlytics und Mixpanel. Beide Tracker sind jedoch inaktiv, so dass weder Analyse Daten noch Daten über ihr weiteres Nutzungsverhalten erhoben werden.

Datenkontrolle bei den eingesetzten Social Media Plug-ins bzw. Links zu Social Media Plattformen

Der digitale Dienst verwendet weder Social Media Plug-ins noch Links zu irgendwelchen Social Media Plattformen.

Wird mein Nutzungsverhalten ausgewertet, z. B. für Werbung oder Tracking?

Es erfolgt keine irgendwie geartete Kontrolle, Nachverfolgung oder Auswertung Ihres Nutzungsverhalten. Insbesondere verwendet der digitale Dienst keinerlei Tools zur Auswertung Ihres Nutzungsverhalten z. B. für Werbung oder Tracking (siehe auch den Abschnitt „Sendet die App Push-Benachrichtigungen“).

Wo finde ich weitere Informationen zum Datenschutz bei der Telekom?

Weitere Informationen, auch zum Datenschutz in speziellen Produkten, erhalten Sie unter www.telekom.de/datenschutzhinweise und unter www.telekom.com/datenschutz.

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), unter Angabe dieser Gründe jederzeit für die Zukunft zu widersprechen. Einer Datenverarbeitung für Zwecke der Direktwerbung können Sie jederzeit ohne Angabe dieser Gründe widersprechen (Art. 21 Abs. 2, 3 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 Datenverarbeitung in Drittstaaten statt, geschieht dies, soweit Sie hierin ausdrücklich eingewilligt haben oder es für unsere Leistungserbringung Ihnen gegenüber erforderlich ist oder es gesetzlich vorgesehen ist (Art.49 DSGVO).

Eine Verarbeitung Ihrer Daten in Drittstaaten erfolgt 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, [vgl. hier](#)).

Wer ist verantwortlich für die Datenverarbeitung? Wer ist mein Ansprechpartner, wenn ich Fragen zum Datenschutz bei der Telekom habe?

Datenverantwortliche ist die Deutsche Telekom Geschäftskunden GmbH, Landgrabenweg 149, 53227 Bonn. 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.

Stand des Datenschutzhinweises 28.03.2025