

Datenschutzhinweis der Telekom Deutschland GmbH („Telekom“) für Protect Mobile

Allgemeines

Der Schutz Ihrer persönlichen Daten hat für die Telekom Deutschland 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.

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 dieser App durch die Telekom gelten.

Weitere Informationen, auch zum Datenschutz 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 Telekom Deutschland GmbH. 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,

- Auskunft** zu verlangen zu Kategorien der verarbeiteten Daten, Verarbeitungszwecken, etwaigen Empfängern der Daten, der geplanten Speicherdauer (Art. 15 DSGVO);
- die **Berichtigung** bzw. Ergänzung unrichtiger bzw. unvollständiger Daten zu verlangen (Art. 16 DSGVO);
- eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu **widerrufen** (Art. 7 Abs. 3 DSGVO);
- 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);
- 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;
- unter bestimmten Voraussetzungen die **Einschränkung** von Daten zu verlangen, soweit eine Löschung nicht möglich bzw. die Löschpflicht streitig ist (Art. 18 DSGVO);
- 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);

- sich bei der zuständigen **Aufsichtsbehörde** über die Datenverarbeitung zu **beschweren** (für Telekommunikationsverträge: Bundesbeauftragte 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 und 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. Beispiel: Nach Vorlage eines Gerichtsbeschlusses sind wir gemäß § 101 Urheberrechtsgesetz verpflichtet, Inhabern von Urheber- und Leistungsschutzrechten Auskunft über Kunden zu geben, die urheberrechtlich geschützte Werke in Internet-Tauschbörsen angeboten haben sollen.

Wo werden meine Daten verarbeitet?

Ihre Daten werden grundsätzlich in Deutschland und im europäischen Ausland verarbeitet.

Findet eine Verarbeitung Ihrer Daten in Ausnahmefällen auch in Ländern außerhalb der Europäischen Union (also in sog. 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). 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).

Für den Service Protect Mobile werden Ihre Daten grundsätzlich in Deutschland verarbeitet. In Ausnahmefällen (Störfall), werden Ihre Daten im Rahmen der gesetzlichen Zulässigkeit über einen Dienstleister (s.o.) an einen Ersatzserver in einem Drittland übermittelt. Bei Einbindung eines Dienstleisters im Drittland ist über entsprechende Vereinbarungen ([vgl. hier](#)) die Einhaltung europäischen Datenschutzniveaus sichergestellt

Welche Daten werden erfasst, wie werden sie verwendet und wie lange werden sie gespeichert?

a) Bei der Aktivierung der Tarifooption Protect Mobile und der App Protect Mobile:

Zur Aktivierung wird Ihre MSISDN (Mobilfunk Rufnummer) einmalig durch einen Dienstleister ggf. auch einen außereuropäischen Dienstleister im Drittland, an ein Rechenzentrum bei T-Systems in Deutschland übertragen. Diese Angabe ist zur Vertragserfüllung erforderlich und die MSISDN wird nach einem Tag gelöscht. Bei Einbindung eines Dienstleisters im Drittland ist über entsprechende Vereinbarungen die Einhaltung europäischen Datenschutzniveaus sichergestellt ([vgl. hier](#)). Nur im Ausnahmefall (Störfall) findet die Registrierung in einem Drittland statt. Der Dienstleister generiert aus der MSISDN einen verschlüsselten Lizenzcode, der regelmäßig vor Beginn der Nutzung der App vom Dienstleister geprüft wird. Bei einer Kündigung bzw. Wegfall der Option wird der Lizenzcode gelöscht.

b) Bei der Nutzung der App:

Wenn Sie den Dienst nutzen, verzeichnen unsere Server temporär die zugeteilte IP-Adresse Ihres Gerätes und andere technische Merkmale, wie zum Beispiel die angefragten Inhalte. Für das Aufrufen der Appfunktion „Statistik“ wird im Hintergrund Ihr Lizenzcode zur Authentifizierung übertragen. Insbesondere werden alle über Ihr Gerät aufgerufenen Webadressen (URL), Namensauflösungen (DNS) und auch die angeforderten Webinhalte erfasst, um diese auf Bedrohungen und Gefährdungen zu prüfen. Zum Teil werden Prüfsummen zu den Inhalten erzeugt und gegen die Prüfsummen von Diensteanbietern abgeglichen. Für die Statistikauswertung in der App wird eine gesamthafte Zählung über alle Kunden durchgeführt ohne direkte Kundenzuordnung. Hierfür werden Informationen wie Logdaten und IP Adresse maximal 7 Tage gespeichert und dann gelöscht. DNS-Anfragen und Inhalte werden nicht gespeichert.

c) Im Netz der Telekom realisierte Dienstleistungen und Datenerhebungen und Verarbeitungen:

Durch Buchung der Option „Protect Mobile“ wird die Datenkommunikation in den Telekom-eigenen Netzen (Mobilfunk, Roaming) geprüft, gefiltert und abgesichert. Wenn Sie den Dienst nutzen, verzeichnen unsere Server temporär die zugeteilte IP-Adresse Ihres Gerätes. Darüber hinaus werden über Ihr Gerät insbesondere aufgerufenen Webadressen (URL), Namensauflösungen (DNS) und auch die angeforderten Webinhalte erfasst, um diese auf Bedrohungen und Gefährdungen zu prüfen. Hierfür werden Informationen wie Logdaten und IP Adresse maximal 7 Tage gespeichert und dann gelöscht. DNS-Anfragen und Inhalte werden nicht gespeichert.

d) In Nicht-Telekom Mobilfunknetzen (z.B. Hotspot, WLAN) wird die Dienstleistung über die App realisiert und ist mit folgenden Datenerhebungen und Verarbeitungen verbunden

Durch die Nutzung der Protect Mobile App wird die Datenkommunikation in Nicht-Telekom-Mobilfunknetzen gleichermaßen geprüft, gefiltert und abgesichert. Hierbei werden keinerlei Daten weitergegeben oder gespeichert.

Berechtigungen

Um die App auf Ihrem Gerät nutzen zu können, muss die App auf verschiedene Funktionen und Daten Ihres Endgerätes 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 unserer App nutzen können.

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

Internetkommunikation

Die App benötigt Zugriff auf das Internet über W-LAN oder Mobilfunk, um Sicherheitsbedrohungen zu erkennen und Ihr Gerät davor zu schützen (Art. 6 Abs. 1 b DSGVO). Die Speicherdauer beträgt 7 Tage, danach werden die Daten gelöscht. Die App benötigt ggf. einen Zugriff auf das Internet auch, um die Datenschutzhinweise abzurufen, damit diese angezeigt werden können.

USB, Fotos, Videos, Apps, Nachrichteninhalte etc.

Die App benötigt Zugriff auf die lokal auf Ihrem Endgerät gespeicherten Dateien, um Sicherheitsrisiken und Bedrohungen zu erkennen und Ihr Gerät zu schützen. Hierbei werden keinerlei Daten weitergegeben oder gespeichert.

Sendet die App Push-Benachrichtigungen?

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

Protect Mobile nutzt die Versendung von Benachrichtigungen, um über den Sicherheitsstatus (z.B. keine Risiken erkannt, bei Erkennung von Schadsoftware oder bei Erkennung von Netzwerken ohne integrierte Schutzmaßnahmen) zu informieren.

Sie können den Empfang von Push-Benachrichtigungen jederzeit in den Einstellungen Ihres Gerätes deaktivieren.

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

Erläuterungen und Definitionen:

Wir möchten, dass Sie unsere App gerne nutzen und unsere Produkte und Dienste in Anspruch nehmen. Daran haben wir ein wirtschaftliches Interesse. Damit Sie die Produkte finden, die Sie interessieren und wir unsere App nutzerfreundlich ausgestalten können, analysieren wir anonymisiert oder pseudonymisiert Ihr Nutzungsverhalten. Im Rahmen der gesetzlichen Regelungen legen wir, oder von uns im Rahmen einer Auftragsdatenverarbeitung beauftragte Unternehmen, Nutzungsprofile an. Ein unmittelbarer Rückschluss auf Sie ist dabei nicht möglich. Nachfolgend informieren wir Sie allgemein über die verschiedenen Zwecke und Techniken. Daran anschließend haben Sie die Möglichkeit des Widerspruchs. Bitte beachten Sie dabei aber, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen unserer App nutzen können.

a) Verwendungszwecke (Art. 6 Abs. 1f DSGVO / §15 Abs. 3 TMG)

Tag-Management

Das Tag-Management dient der Verwaltung von Tracking-Tools in Apps. Dazu wird für jede Seite eine Markierung (engl. Tag) festgelegt. Anhand der Markierung kann dann festgelegt werden, welche Tracking-Tools für diese Seite zum Einsatz kommen sollen. Über das Tag-Management kann somit das Tracking gezielt gesteuert werden, sodass die Tools nur dort zum Einsatz kommen, wo sie Sinn ergeben.

Marktforschung / Reichweitenmessung

Ziel der Reichweitenmessung ist es, die Nutzungsintensität und die Anzahl der Nutzer einer App statistisch zu bestimmen sowie vergleichbare Werte für alle angeschlossenen Angebote zu erhalten. Zu keinem Zeitpunkt werden einzelne Nutzer identifiziert. Ihre Identität bleibt immer geschützt.

Profile zur bedarfsgerechten Gestaltung der App

Um die App stetig verbessern zu können, erstellen wir sogenannte Clickstream-Analysen. Der Clickstream entspricht Ihrem Bewegungspfad in der App. Die Analyse der Bewegungspfade gibt uns Aufschluss über das Nutzungsverhalten der App. Dieses lässt uns mögliche Strukturfehler in der App erkennen und so die App verbessern, damit die App auf Ihre Bedürfnisse zu optimieren. Zu keinem Zeitpunkt werden einzelne Nutzer identifiziert.

Profile zur Verbesserung der technischen App-Qualität

Um die Qualität der Programmierung einer App zu messen oder Abstürze und deren Ursache zu registrieren, werden Programmablauf und Nutzungsverhalten ausgewertet. Einzelne Nutzer werden dabei nicht identifiziert.

b) Techniken

Messpixel

Messpixel sind meist nur 1×1 Pixel groß bemessene Bilder und sind transparent oder in der Farbe des Hintergrundes erstellt, damit sie nicht sichtbar sind. Wird eine Seite der App, die ein Messpixel enthält, geöffnet, dann wird dieses kleine Bild von dem Server des

Anbieters im Internet geladen, wobei das Herunterladen dort registriert wird. So kann der Anbieter des Verfahrens sehen, wann und wie viele Nutzer diesen Messpixel anforderten bzw. wann eine Seite der App besucht wurde. Ferner kann der Anbieter weitere Informationen erfassen, wie z.B. Browserinformationen, Betriebssystem, Bildschirmauflösung.

Sie können der Datenerhebung, -verarbeitung und -nutzung mit dem Schalter "Pseudonyme Nutzungsdaten übermitteln" widersprechen. Bitte beachten Sie, dass dabei nur die Nutzungsanalyse dieser App deaktiviert wird.

In dieser App genutzten Verfahren.

Firma	Zweck	Speicherdauer	Eingebunden als
Tealium	Tag-Management	24 Monate	Auftragsverarbeiter
Webtrekk	Bedarfsgerechte Gestaltung	14 Monate	Auftragsverarbeiter
360Dialog GmbH	Bedarfsgerechte Gestaltung, Werbung	24 Monate	Auftragsverarbeiter
Aptelligent	Technische App-Qualität	30 Tage	Auftragsverarbeiter
Adjust	Bedarfsgerechte Gestaltung	1 Monat	Auftragsverarbeiter
Contiamo	Bedarfsgerechte Gestaltung	24 Monate	Auftragsverarbeiter