



Datenschutzhinweise der Telekom Deutschland GmbH („Telekom“) für die Nutzung der MeinMagenta und MagentaService App

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.

Für die Verarbeitung Ihrer persönlichen Daten gilt der [Allgemeine Datenschutzhinweis der Telekom Deutschland GmbH](#). Bei der Nutzung dieser App gilt ergänzend:

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

Bei der Registrierung:

Bitte beachten Sie hierfür die [Datenschutzhinweise für den Telekom Login](#).

Bei der Nutzung der App

Wenn Sie die App nutzen, verzeichnen unsere Server temporär die IP-Adresse Ihres Gerätes und andere technische Merkmale, wie zum Beispiel die angefragten Inhalte (Art. 6 Abs. 1 b DSGVO).

In dieser App haben Sie die Möglichkeit neben den Eingaben per Tastatur auch den Text zu diktieren. Die Spracheingabe (Google) oder Diktierfunktion (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 Eingabefeld ausgegeben. Zu Details zu der Funktionalität und wie Sie die Nutzung ein- bzw. ausschalten können, informieren Sie sich bitte bei dem jeweiligen Betriebssystemhersteller.

Chatbot

Wenn Sie den Chatbot ("Frag Magenta") als Self-Service bzw. für den Kontakt zum Kundenservice nutzen, werden während des automatisierten Chats verschiedene Informationen an die Dialogplattform übertragen (Art. 6 Abs. 1 a DSGVO). Hierzu gehören z. B. die von Ihnen eingegebenen Fragen und Antworten (Chatverlauf) oder Ihre Kundendaten, wenn Sie sich vorab mit dem Telekom-Login angemeldet haben. Wir verarbeiten die erhobenen Daten in dem cloudbasierten Dialogsystem des Auftragsverarbeiters [IBM Deutschland GmbH](#) („IBM“, Wilhelm-Fay-Straße 30-34, 65936 Frankfurt). Personenbezogene Daten, wie z. B. Ihr Name, Ihre Anschrift, Telefonnummer oder E-Mail-Adresse, werden vor der Übertragung an den Auftragsverarbeiter pseudonymisiert. Dabei erfolgt das Datenhosting im IBM Cloud-Rechenzentrum in Frankfurt am Main, Deutschland. Darüber hinaus werden die Daten vor der Verwendung zur Verbesserung dieses Services durch einen Anonymisierungsservice um potenzielle personenbezogene Daten bereinigt. Das pseudonymisierte Chatprotokoll wird nach dem Dialogende gelöscht. Es besteht die Möglichkeit, dass der Chatbot bei Bedarf und nach Ihrer Zustimmung an unseren Text Chat des Kundenservices übergibt. Dabei werden der Chatverlauf und vorhandene Kundendaten, sofern sie sich vorab mit dem Telekom-Login eingeloggt haben, an den Text Chat übergeben.

Bei Nutzung von Frag Magenta haben Sie die Möglichkeit, Spracheingaben zu diktieren. Die Spracheingabe ist eine Funktionalität, die mittels des Telekom Produktes Smart Speaker bzw. der Hallo Magenta App bereitgestellt wird. Bei der Verwendung wird die Sprache durch die Telekom verarbeitet und das Ergebnis an unsere Frag Magenta Plattform ausgegeben. Zu Details der Funktionalität und wie Sie die Nutzung ein- bzw. ausschalten können, informieren Sie sich bitte in den [Datenschutzhinweisen zum Magenta Smart Speaker bzw. zur Hallo MagentaApp](#).

Text- oder Video-Chat, Rückrufservice

Wenn Sie den Text-, Video-Chat oder Rückrufservice auf der Seite für den Kontakt zum Kundenservice nutzen, werden bei Initialisierung des Chats verschiedene Informationen an den Kundenberater übertragen (Art. 6 Abs. 1 a DSGVO). Hierzu gehören Login-Daten, Kundendaten (Rufnummer, Kundennummer und aktueller Chatverlauf), sowie das von Ihnen auf der Seite ausgewählte Hilfe-Thema, Browser-Version, Betriebssystem-Version und ähnliches. Zusätzlich werden von der Chat-Plattform des Auftragsverarbeiters [Genesys DACH](#) (Joseph-Wild-Straße 20, 81829 München) in regelmäßigen Abständen Informationen über die Erreichbarkeit des Chat-Services übertragen. Mit Hilfe dieser Information wird auf der Kontakt-Seite der Button zum Starten des Text- bzw. Video-Chats aktiviert oder deaktiviert. Wir speichern die Information über den Beginn und das

Ende des Chats (der Session) für 7 Tage. Dazu wird für die Dauer der Session eine Session Information gesetzt, die am Ende der Session gelöscht wird. Das Chatprotokoll wird für 8 Tage von uns gespeichert, um im Falle von Rückfragen darauf zugreifen zu können. Die statistische Auswertung anonymisierter Datensätze behalten wir uns vor.

Video-Chat und Video-Ident

Für die Legitimationsprüfung im Rahmen eines Vertragsabschlusses nutzen wir innerhalb des Videochats den Service Video-Ident des Auftragsverarbeiters [Purpleview GmbH](#) (Kampstraße 6, 44137 Dortmund) (Art. 6 Abs. 1 b DSGVO). Für Video-Chat und Video-Ident wird für die Dauer der Session eine Session Information gesetzt, die am Ende der Session gelöscht wird. Wir speichern nur die Information über die Session, insbesondere den Beginn und das Ende der Session für 7 Tage. Videoinhalte werden nicht gespeichert.

Betrugsprävention

Zur Vermeidung von Betrugsfällen in unserem Webshop haben wir die Firma [Risk.Ident GmbH](#) mit der Erbringung des Dienstes beauftragt (Art. 6 Abs.1. b DSGVO). Risk.Ident erhebt und verarbeitet auf den Seiten unseres Shops mit Hilfe von Cookies und Tracking-Technologien Daten zur Ermittlung des vom Nutzer verwendeten Endgerätes. Soweit durch Risk.Ident IP-Adressen erhoben werden, werden diese sofort anonymisiert. Die von Risk.Ident verarbeiteten Daten werden in einer Datenbank zur Betrugsprävention hinterlegt. Auf diese greifen wir im Rahmen des Bestellprozesses zum Zweck einer Risikobewertung zu. Darüber hinaus übermitteln wir Daten zu Endgeräten, von denen es bereits zu (versuchten) Betrugstaten gekommen ist, an Risk.Ident. Eine Zuordnung der Daten zu Personen erfolgt zu keinem Zeitpunkt.

Betrugsprävention bei Zahlung mit PayPal

Insbesondere bei wiederkehrender Bezahlung mit dem Bezahlservice von [PayPal](#) (s.g. Einzugsverfahren, d.h. ohne nochmalige Zahlungsfreigabe über einen Login bei PayPal) erhebt PayPal in eigener Verantwortung Daten zu dem Gerät, auf dem die App verwendet wird. Diese Daten werden zum Zwecke der Betrugsprävention erhoben (Art. 6 Abs.1. f DSGVO). Details finden Sie in den [Datenschutzhinweisen von PayPal](#).

Heimnetz-Check

Um das Telekom-Netz noch besser für Sie zu machen, werden bei der Funktion „Heimnetz-Check“ folgende Daten von der App erfasst, gespeichert und verarbeitet:

Messungen über die Qualität der Verbindung

- Gemessene Datenrate in Upload und Download
- Anzahl der Hops zwischen Mess-Client und Mess-Server
- Gemessene Paketlaufzeit
- Gemessener Jitter
- Gemessene Anzahl verlorener Pakete
- DSL Line Downstream/ Upstream (aktueller und maximal möglicher Wert) Kontextinformationen
- Technische Daten des Smartphones
- Verbleibende Batterielaufzeit des Smartphones
- Betriebssystem
- Art der Bewegung des Smartphones
- Router Firmware Version
- Standort
- Präzision des ermittelten Standortes
- Datum/Uhrzeit
- Technologie der Verbindung (2G, 3G, 4G, 5G, WLAN)
- gebuchte Bandbreite des Anschlusses

- Signalstärke WLAN (RSSI des Wi-Fi Hotspots) oder Mobilfunk (RSSI und Signalrauschabstand SNR)
- Link Geschwindigkeit des Wi-Fi Hotspots
- Verschlüsselungsmethode des Wi-Fi Hotspots
- Frequenz des Wi-Fi Hotspots
- Bewertung der Internetverbindung durch den Nutzer
- Empfehlungen für den Nutzer, basierend auf dem Ergebnis der Messung des Internet-Anschlusses Kennungen
- App-Installations-ID
- Router-ID (Hersteller, Seriennummer, Modell-Name)
- Lokale IP-Adresse
- Test-ID
- SSID des Wi-Fi Hotspots
- BSSID des Wi-Fi Hotspots
- Räumliche Sektor Zuordnung Cell-ID und Cell-LAC

• Mobile Country Code (MCC) und Mobile Network Code (MNC)
Vollständige Datensätze (d.h. inklusive der App-Installations-ID und der Router-ID) werden für 30 Tage gespeichert und dann automatisch gelöscht.

Vollständige Datensätze (d.h. inklusive der App-Installations-ID und der Router-ID) werden für 30 Tage gespeichert und dann automatisch gelöscht.

Router Einstellungen

Daten Ihres Routers, wie z.B. IP-Adresse, Geräteliste und Router Passwort werden aus dem Router ausgelesen, angezeigt und temporär sicher in der App gespeichert, jedoch nicht an uns übertrage

Berechtigungen

Um verschiedene Funktionen der App auf Ihrem Gerät nutzen zu können, erfragt die App Zugriffsrechte auf Daten bzw. Funktionen Ihres Endgeräts. Dazu ist es erforderlich, dass Sie bestimmte Berechtigungen erteilen (Art. 6 Abs. 1 a DSGVO).

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

Bitte beachten Sie, dass Sie im Falle eines Widerspruchs einer oder mehrerer Berechtigungen gegebenenfalls nicht sämtliche Funktionen unserer App nutzen können. Die folgenden Berechtigungen können Sie in den Einstellungen Ihres Betriebssystems jederzeit wieder entziehen.

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

Kamera, Mikrofon

Die App benötigt Zugriff auf „Kamera und Mikrofon“ zu folgendem Zweck:

Einige Funktionen und Services der App, wie z. B. der Video-Chat oder Video-Ident benötigen diesen Zugriff, um mit Telekom Service-Mitarbeitern in Kontakt zu treten. Videoinhalte werden nicht gespeichert.

Des Weiteren benötigen wir Zugriff auf Ihre Kamera, um den QR-Code auf dem Zugangsdatenschreiben oder auf Ihrem Router zu scannen und die darin enthaltenen Zugangsdaten zu verwenden. Diese werden nur lokal gespeichert.

Außerdem wird der Mikrofonzugriff für die optionale Sprachnutzung des Chatbots „Frag Magenta“ benötigt, um Spracheingaben tätigen zu können. Details zur Sprachnutzung siehe auch unter 1) c).

Kontakte

Die App benötigt Zugriff auf die Kontakte zu folgenden Zwecken:

In der Funktion Prepaid-Guthaben aufladen benötigen wir die Telefonnummer, auf die das Guthaben aufgeladen werden soll. Im Aufladungsprozess haben Sie die Möglichkeit, dafür eine Telefonnummer aus Ihrem Adressbuch zu übernehmen. Die verwendeten Telefonnummern werden auf unseren Servern für die Aufladung und deren Dokumentation gespeichert.

Darüber hinaus werden die gespeicherten Namen und Telefonnummern aus Ihrem Adressbuch ausgelesen, um diese als Vertragsbezeichnung zu verwenden, wenn die Rufnummer zu ihrem Vertragsbestand gehört. Diese Zuordnung erfolgt nur lokal auf dem Gerät, auf dem die App läuft.

Die Berechtigung auf die Kontakte zuzugreifen, können Sie in den Einstellungen Ihres Betriebssystems jederzeit wieder entziehen.

Speicher (nur Android)

Die App benötigt den Zugriff auf „Speicher“ zu folgendem Zweck:

Die App benötigt unter Android diese Berechtigung, um PDF-Dokumente aus dem Hilfe-Bereich zu öffnen.

Standortdaten

Die App benötigt Zugriff auf die Standortdaten zu folgendem Zweck:

Mit dieser App können Sie ganz einfach einen Telekom Shop in Ihre Nähe finden. Hierzu werden Information über Ihren Standort benötigt. Diese Daten werden nur zu diesem Zeitpunkt verwendet und nicht von uns gespeichert.

Unter Android ist die automatische WLAN-Einrichtung mit der Berechtigung des Standorts verknüpft. An dieser Stelle müssen wir die Standortberechtigung abfragen, verwenden den Standort aber nicht.

In der Funktion „Heimnetz-Check“ wird der ungefähre Standort, der genaue Standort und die SSID bzw. BSSID der aktuellen WLAN-Verbindung erfasst und abgesendet (siehe Punkt 1) g)). Das dient dazu, die örtliche Leistung des Telekom Netzes auswerten zu können.

WLAN-Verbindung abrufen (nur Android)

Die App benötigt Zugriff auf „WLAN-Verbindung abrufen“ zu folgendem Zweck:

Wir verwenden diese Berechtigung in der Funktion „Heimnetz-Check“, um Ihnen weitere Details zu Ihrer WLAN-Verbindung anzuzeigen und auszuwerten (siehe Punkt 1) g)).

Auf Netzwerke zugreifen/ Internetdaten erhalten / Netzwerkverbindung abrufen (nur Android)

Die App benötigt Netzwerkzugriff zu folgendem Zweck:

Um auf einige Telekom Services zugreifen zu können, so dass Sie zum Beispiel Ihre Vertragsdaten einsehen können, wird eine Internetverbindung benötigt.

Bei einigen Funktionen der App wird vor der Nutzung überprüft, ob eine Internetverbindung vorliegt, um Sie ggf. darauf hinzuweisen.

Außerdem werden Daten zur aktuellen Netzwerkverbindung in der Funktion „Heimnetz-Check“ erfasst und abgesendet, um die Leistung des Telekom Netzes auswerten zu können (siehe Punkt 1) g))

Vibrationsalarm steuern (nur Android)

Die App benötigt Zugriff auf den Vibrationsalarm zu folgendem Zweck:

Die App kann Push-Benachrichtigungen versenden. Für diese Form der Benachrichtigungen wird diese Berechtigung benötigt.

Audioeinstellungen ändern, Kopplung von Bluetooth-Geräten durchführen, Ruhezustand deaktivieren (nur Android)

Die App benötigt Zugriff auf Audioeinstellungen, die Kopplung von Bluetooth-Geräten und den Ruhezustand zu folgendem Zweck:

Diese Berechtigungen werden benötigt, um Ihnen eine störungsfreie und bequeme Nutzung des Video-Chats und von Video-Ident zu ermöglichen.

Aktivitätserkennung (Android) und Bewegungs- & Fitness-Daten (iOS)

Die App benötigt Zugriff auf die Aktivitätserkennung / Bewegungs- & Fitness Daten zu folgendem Zweck:

Die Funktion „Heimnetz-Check“ erfasst diese Daten und sendet sie ab, um die Leistung des Telekom Netzes in Bezug auf die aktuelle Bewegungsart (z.B. im Auto, zu Fuß, im Zug) auswerten zu können (siehe Punkt 1) g)).

Geräte im lokalen Netzwerk finden und verbinden (nur iOS)

Die App benötigt Zugriff auf „Geräte im lokalen Netzwerk finden und verbinden“ zu folgendem Zweck:

Die Funktionen Router-Einrichtung, Router-Firmwareupdate, Router-Einstellungen und Heimnetz-Check stellen Verbindungen zu Ihren Netzwerkgeräten (z.B. Router) her. Hierbei werden Informationen z.B. zum Router-Modell und Verbindungsstatus ausgelesen und lokal in der App verarbeitet. So können wir z.B. feststellen, ob Ihr Router korrekt eingerichtet wurde.

Die Verarbeitung erfolgt innerhalb der App. Vereinzelt werden bei eventuell auftretenden Fehlern, Fehler-Informationen pseudonym an uns gesendet.

Sendet die App Push-Benachrichtigungen?

Push-Benachrichtigungen sind Nachrichten, die von der App auf 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).

Wir möchten Ihnen Push-Nachrichten zu relevanten Vertragsinformationen (z.B. neue Rechnung, Datenvolumen aufgebraucht) und allgemeinen Servicethemen senden.

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

Die Abwicklung erfolgt über den Auftragsverarbeiter MoEngage (315 Montgomery Street, 10. Etage, San Francisco, 94104, USA).

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 Auftragsverarbeitung beauftragte Unternehmen, Nutzungsprofile an. Ein unmittelbarer Rückschluss auf Sie ist dabei nicht möglich. Nachfolgend informieren wir Sie allgemein über die verschiedenen Zwecke. Über die Datenschutz-Einstellungen haben Sie die Möglichkeit der Tool-Nutzung zuzustimmen oder diese abzulehnen. Tools, die zur Erbringung der App erforderlich sind, (siehe Erläuterung oben im Abschnitt 1)) können nicht abgelehnt werden.

Marktforschung / Reichweitenmessung (Opt-In)

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.

Zur Verbesserung der technischen App-Qualität (Opt-In)

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

Profil zur bedarfsgerechten Gestaltung der App (Opt-In)

Um die App stetig verbessern zu können, nutzen wir die erfassten Events aus dem Event Tracking. Diese entsprechen 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.

Profil für personalisierte Empfehlungen (Opt-In)

Die Telekom spielt Ihnen individuell angepasste und personalisierte Handlungs- und Klick-Empfehlungen für Angebote, Dienste oder Produkte aus. Dazu legen wir mit Hilfe von Dienstleistern ein pseudonymisiertes Profil über die von Ihnen ausgelösten Events in der App (z. B. von Ihnen aufgerufene Dienste und Seiten) an und ordnen diesem Profil Kategorien zu. Sie erhalten zum Profil passende Inhalte oder Hinweise angezeigt.

Geräte- und partnerübergreifende Profile zur interessengerechten Auspielung von Werbung und App-Inhalten

Wir erheben über unsere App unter anderem Informationen zu Ihrem Nutzungsverhalten und im eingeloggt Zustand auch Vertragsinformationen zu gekauften Produkten, Tarifen oder Optionen, sowie Vertragslaufzeiten, um Webinhalte als auch Online-Werbung interessengerechter auszuspielen zu können. Um dies sowohl geräte- als auch anbieterübergreifend umsetzen zu können, arbeiten wir mit Partnern zusammen.

Erforderliche Tools

Diese Tools sind notwendig, damit Sie durch die Seiten navigieren und wesentliche Funktionen nutzen können. Sie ermöglichen Grundfunktionen, wie die Bestellabwicklung im Online-Shop und den Zugriff auf gesicherte Bereiche der App. Zudem dienen sie der anonymen Auswertung des Nutzerverhaltens, die von uns verwendet wird, um unsere App stetig für Sie weiterzuentwickeln. Rechtsgrundlage für diese Tools ist Art. 6 Abs. 1 b DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 b DSGVO.

Firma	Zweck	Speicherdauer	Land der Verarbeitung
PurpleView GmbH	Video-Chat, Video-Ident	Session	Deutschland
Telekom	Login	Bis zum Logout	Deutschland

RabbitMQ	statistische Auswertung	Session	Deutschland, Indien
Kibana	Fehleranalyse, statistische Auswertung	90 Tage	Deutschland, Indien

bei optionaler Nutzung von Tools

Diese Tools werden dann verwendet, wenn Sie zusätzliche Funktionen, wie z. B. Chat, nutzen. Die möglichen Funktionen werden im Abschnitt 1) dieses Datenschutzhinweises erläutert. Rechtsgrundlage für diese Tools ist Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 b DSGVO.

Firma	Zweck	Speicherdauer	Land der Verarbeitung
MoEngage	Push-Nachrichten für Service- und Vertragszwecke	24 Monate	Indien
IBM Deutschland GmbH	Chatbot (Frag Magenta)	Session	Deutschland
Genesys	Text-, Video-Chat	7 Tage (Session-Daten) 8 Tage (Chat-Verlauf)	Deutschland

Analytische Tools

Diese Tools helfen uns, das Nutzungsverhalten besser zu verstehen.

Analysetools ermöglichen die Erhebung von Nutzungs- und Erkennungsmöglichkeiten durch Erst- oder Drittanbieter, in so genannten pseudonymen Nutzungsprofilen. Wir benutzen beispielsweise Analysetools, um die Zahl der individuellen Nutzer einer App zu ermitteln oder um technische Informationen bei einem Absturz der App zu erheben, als auch das Nutzerverhalten auf Basis anonym und pseudonymer Informationen zu analysieren, wie Nutzer mit der App interagieren. Ein unmittelbarer Rückschluss auf eine Person ist dabei nicht möglich. Rechtsgrundlage für diese Tools ist Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 b DSGVO

Firma	Zweck	Speicherdauer	Land der Verarbeitung
MoEngage	Bedarfsgerechte Gestaltung, In-App-Nachrichten und Push-Nachrichten	24 Monate	Indien

Marketing / Retargeting

Diese Tools werden eingesetzt, um Ihnen personalisierte und dadurch relevante werbliche Inhalte anzeigen zu können.

Marketingtools werden eingesetzt, um interessante Werbeeinhalte anzuzeigen und die Wirksamkeit unserer Kampagnen zu messen. Dies geschieht nicht nur auf Seiten der Telekom Deutschland GmbH, sondern auch auf anderen Werbepartner-Seiten (Drittanbieter). Dies wird auch als Retargeting bezeichnet, es dient zur Erstellung eines pseudonymen Interessenprofils und der Schaltung relevanter Werbung in anderen Apps. Ein unmittelbarer Rückschluss auf eine Person ist dabei nicht möglich. Marketing und Retargeting Tools helfen uns mögliche relevanten Werbeeinhalte für Sie anzuzeigen. Durch das Unterdrücken von Marketing Tools sehen Sie auch weiterhin die gleiche Anzahl an Werbung, die aber möglicherweise weniger relevant für Sie ist. Rechtsgrundlage für diese Tools ist Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 b DSGVO.

Zudem können durch diese Tools personalisierte Angebote sowie personalisierte Servicemeldungen (z.B. Tipps zur Nutzung der App) als Push-Benachrichtigung gesendet werden. Wenn Sie diese Push-Benachrichtigung nicht erhalten möchten, bitten wir Sie, die Zustimmung zu Marketing Tools in den Datenschutz-Einstellungen zu widerrufen.

Firma	Zweck	Speicherdauer	Land der Verarbeitung
MoEngage	Push-Nachrichten für personalisierte Service Nachrichten und Angebote	24 Monate	Indien
Campaign 2.0	Personalisierte Angebote	4 Monate	Deutschland, Indien

Dienste von anderen Unternehmen (eigenverantwortliche Drittanbieter)

Auf einigen Seiten unserer App haben wir Drittanbieter Dienste eingebunden, die ihre Services eigenverantwortlich erbringen. Dabei werden bei der Nutzung unserer App Daten mithilfe von Tools erfasst und an den jeweiligen Dritten übermittelt. Zum Teil für Telekomeigene Zwecke. Rechtsgrundlage für diese Tools ist Art. 6 Abs. 1 a DSGVO. In welchem Umfang, zu welchen Zwecken und auf Basis welcher Rechtsgrundlage eine Weiterverarbeitung zu eigenen Zwecken des Drittanbieters erfolgt, entnehmen Sie bitte den Datenschutzhinweisen des Drittanbieters. Die Informationen zu den eigenverantwortlichen Drittanbietern finden Sie nachfolgend:

YouTube

In unserer App setzen wir eingebettete Videos von „YouTube“ ein. Hierbei handelt es sich um ein Videoportal der YouTube LLC., 901 Cherry Ave., 94066 San Bruno, CA, USA, nachfolgend nur „YouTube“ genannt.

YouTube ist ein Tochterunternehmen der Google LLC., Gordon House, Barrow Street, Dublin 4, Irland, nachfolgend nur „Google“ genannt.

Durch die [Zertifizierung nach dem EU-US Privacy Shield](#) garantiert Google und damit auch YouTube, dass die Datenschutzvorgaben der EU auch bei der Verarbeitung von Daten in den USA eingehalten werden.

Daten werden erst an YouTube übermittelt, wenn Sie eines der Videos starten. Hierbei wird Ihre IP-Adresse, Zugriffsdatum und Uhrzeit übertragen.

Sie können sich jederzeit über die Datenverarbeitung durch Google unter <http://www.google.de/intl/de/policies/privacy> informieren und dieser widersprechen.

Google Analytics

Wir verwenden Google Analytics, um die App-Nutzung zu analysieren. Die daraus gewonnenen Daten werden genutzt, um unsere App sowie Werbemaßnahmen zu optimieren.

Google Analytics ist ein Analysedienst, der von Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) betrieben und bereitgestellt wird. Google verarbeitet die Daten zur Website-Nutzung in unserem Auftrag und verpflichtet sich vertraglich zu Maßnahmen, um die Vertraulichkeit der verarbeiteten Daten zu gewährleisten.

Während Ihres App-Besuchs werden u.a. folgende Daten aufgezeichnet:

- Aufgerufene Bereiche in der App
- Bestellungen inkl. des Umsatzes und der bestellten Produkte
- Die Erreichung von "App-Zielen" (z.B. Kontaktanfragen und Newsletter-Anmeldungen)
- Verhalten auf den Seiten (beispielsweise Klicks, Scroll-Verhalten und Verweildauer)
- ungefähre Standort (Land und Stadt)
- IP-Adresse (in gekürzter Form, sodass keine eindeutige Zuordnung möglich ist)
- Technische Informationen wie Internetanbieter, Endgerät und Bildschirmauflösung
- Herkunftsquelle Ihres Besuchs (über welches Werbemittel Sie zu uns gekommen sind)

Diese Daten werden an einen Server von Google in den USA übertragen.

Google Analytics speichert die Daten für die Dauer von zwei Jahren seit Ihrem letzten Besuch. Die erhobenen Daten werden unter einer zufallsgenerierten User-ID (einschließlich Android Advertising ID bzw. Advertising Identifier für iOS) gespeichert, mit der Sie bei zukünftigen App-Besuchen wiedererkannt werden können.

Die aufgezeichneten Daten werden zusammen mit der zufallsgenerierten User-ID gespeichert, was die Auswertung pseudonymer Nutzerprofile ermöglicht. Diese nutzerbezogenen Daten werden automatisch nach 14 Monaten gelöscht. Sonstige Daten bleiben in aggregierter Form unbefristet gespeichert.

Stand November 2021

Durch die [Zertifizierung nach dem EU-US Privacy Shield](#) garantiert Google, dass die Datenschutzvorgaben der EU auch bei der Verarbeitung von Daten in den USA eingehalten werden.

Sie können sich jederzeit über die Datenverarbeitung durch Google unter <https://policies.google.com/privacy> informieren und dieser widersprechen.

Google Analytics für Firebase

Google Analytics für Firebase oder Firebase Analytics ist ein Analyse-Dienst von Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA). Firebase Analytics kann Daten mit anderen von Firebase bereitgestellten Tools wie Crash Reporting, Authentication, Remote Config oder Notifications gemeinsam nutzen.

Diese Anwendung verwendet Identifikatoren für mobile Geräte (einschließlich Android Advertising ID bzw. Advertising Identifier für iOS) und Cookie-ähnliche Technologien für die Ausführung des Google Analytics für Firebase-Dienstes.

Nutzer können sich über die entsprechenden Geräteeinstellungen mobiler Geräte von bestimmten Firebase-Funktionen abmelden, wie etwa über die Werbeeinstellungen für mobile Geräte, oder indem sie gegebenenfalls den Anweisungen anderer Abschnitte dieser Datenschutzrichtlinie bezüglich Firebase folgen.

Erhobene personenbezogene Daten: Cookie, Eindeutige Gerätekennzeichnung für Werbung (Google-Werbe-ID oder IDFA, beispielsweise) und Nutzungsdaten. Der Verarbeitungsort der Daten befindet sich in den USA.

Sie können sich jederzeit über die Datenverarbeitung durch Google unter <https://policies.google.com/privacy> informieren und dieser widersprechen

emetriq GmbH

emetriq ist Anbieter von Targeting-Dienstleistungen im Bereich der Online-Vermarktung von Werbeplätzen. Targeting steht für eine genaue Zielgruppenansprache in der Online-Vermarktung. Zu diesem Zwecke betreibt emetriq einen Datenpool, dessen Ziel es ist, die Qualität von Targeting signifikant zu steigern, damit Werbetreibende relevante Werbung gemäß Ihren Interessen einblenden können. Um zu ermöglichen, dass nutzerspezifische Werbung angezeigt werden kann, erfasst die emetriq GmbH, Vorsetzen 35, 20459 Hamburg, Informationen über das Surfverhalten bzw. die App Nutzung. Verwendet werden Cookies, Messpixel, APIs oder SDKs, die folgenden Informationen erheben bzw. verarbeiten können:

- Identifier for Advertising (IDFA) oder Advertisings-ID (AdID)
- Informationen der App oder des Browsers, zum Beispiel Browser-Kennung, Zeitzone, Sprache, Betriebssystem
- Informationen über gesehene bzw. angeklickte Werbebanner
- URL der besuchten Internetseiten unserer angebotenen Vermarkter
- Surfverhalten im Online-Shop, zum Beispiel welche Artikel-Kategorien und welche Artikelbeschreibungen angesehen wurden
- Soziodemografische Daten, wie Altersdekaden, Anrede und gekürzte Postleitzahl
- Verhashte Login Daten (E-Mail)
- usw.

Die IP-Adresse wird technologisch bedingt an emetriq übermittelt. Diese wird jedoch sofort wieder verworfen und an keiner Stelle verwendet oder weiterverarbeitet. Die erhobenen Daten werden bereits in der App oder im Browser des Nutzers pseudonymisiert und erst dann an den Datenpool übertragen. Sämtliche erhobenen Informationen über einen Nutzer werden ausschließlich anhand einer automatisch und zufällig generierten Cookie-ID, bzw. einer IDFA oder AdID gespeichert. Ein Cookie ist eine Textdatei auf einem Endgerät (z.B. Mobiltelefon, Computer) und ist immer einem Browser zugeordnet. Verwendet ein Nutzer auf seinem Endgerät zwei oder mehr Browser, werden dementsprechend viele Cookies auf dem Endgerät erzeugt. Sämtliche erhobenen Informationen über einen Nutzer werden ausschließlich mit dieser pseudonymen ID gespeichert. emetriq löscht diese Daten nach spätestens 6 Monaten.

Für jedes ihrer genutzten Endgeräte vergibt emetriq eine Kennung (ID) unter Rückgriff auf Ihre verhashten Login Daten. Damit sind wir imstande, in den Fällen, in denen Sie sich auf unseren Webseiten unter Nutzung verschiedener Endgeräte eingeloggt haben, die verschiedenen vergebenen IDs einander zuzuordnen. Die Kennung (ID) sowie die Information, welchem Nutzer (Login) diese zugeordnet ist, wird an eine neutrale Instanz (Trusted-Third-Party) übermittelt. Die an die Trusted-Third-Party übermittelten Informationen werden durch diese verschlüsselt. Eine Zuordnung der Informationen zu einer Person ist damit nicht mehr möglich. Die verschlüsselten Informationen werden dann an die emetriq zur Auswertung übermittelt. Die emetriq GmbH stellt die Auswertungsergebnisse den

einzelnen Partnern über die Trusted-Third-Party, die dieses wieder entschlüsselt, zur Verfügung. Möglich wird damit in Einzelfällen eine partnerübergreifende Zuordnung eines Endgerätes zu einem Nutzer, auch wenn sich dieser mit seinem Endgerät auf den Telekom Webseiten nicht eingeloggt hat. Zudem sind wir in der Lage die Nutzung der Telekom Dienste durch Sie von verschiedenen Endgeräten einander zuzuordnen. Dieses Verfahren hat den Vorteil, dass auch ohne ein Login eine interessensgerechte Anpassung des Angebots möglich ist.

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 unsere Datenschutz-Themenseite](#) und in den [Datenschutzhinweisen der Telekom Deutschland GmbH](#)

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, Landgrabenweg 151, 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.

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: 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, 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,

- a) 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, z.B. in den USA, die in den Datenschutz der europäischen Bürgerinnen und Bürger unverhältnismäßig eingreifen,
- b) oder soweit es für unsere Leistungserbringung Ihnen gegenüber erforderlich ist (Art. 49 Abs. 1 b DSGVO),
- c) oder soweit es gesetzlich vorgesehen ist (Art. 6 Abs. 1 c 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).

Datenverarbeitungen finden auch außerhalb der Europäischen Union in sog. Drittstaaten statt, derzeit etwa:

Entwicklung und technischer Support teilweise in Indien (Deutsche Telekom Digital Labs, Neu-Delhi).

Versand von Pushnachrichten (MoEngage, Indien).

Die Datenverarbeitung in Drittstaaten erfolgt im gesetzlich vorgesehen Rahmen aufgrund von Regelungen, die ein sicheres Datenschutzniveau gewährleisten (vgl. [hier](#)).

Stand der Datenschutzhinweise 19.11.2021