Datenschutzhinweise der Deutsche Telekom Security GmbH („Telekom“) für 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?
Erforderliche Verarbeitungen bei der Erbringung des digitalen Dienstes (Art. 6 Abs. 1b DSGVO, §25 Abs. 2 Nr. 2 TDDDG)

Bei der Nutzung der MPP-App, im folgenden digitaler 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 Adresse, 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 Adresse 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 Adresse 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.

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)

Abweichende Verarbeitungen im Bereich TelekomCloud Marketplace (Geschäftskunden)
Text Chat:
TelekomCLOUD Marketplace: Wenn Sie den Text Chat auf dem TelekomCLOUD Dienst für den Kontakt zum Kundenservice nutzen, werden verschiedene Informationen an das Chat-System übertragen (Art. 6 Abs. 1 b, f DSGVO) und nach 7 Tagen gelöscht. Hierzu gehören z. B. Ihre IP-Adresse, Browser-Version, Betriebssystem-Version; diese Daten können von unserem Kundenberater nicht eingesehen werden. Die Daten, die im Rahmen des Service Chats entstehen, werden an unser CRM-System übergeben. Die Chat-Inhalte werden systembedingt spätestens nach 24 Stunden gelöscht. Zusätzliche Daten zum Chat (Startzeitpunkt, Dauer des Chats, interne Vermerke, ggf. im Chat erfragte Kundeninformationen) werden nach 28 Tagen anonymisiert.

Zudem werden von der Chat-Plattform in regelmäßigen Abständen Informationen über die Erreichbarkeit des Chat-Services an den digitalen Dienst der TelekomCLOUD Marketplace übertragen. Mit Hilfe dieser Information wird auf dem digitalen Dienst der Button zum Starten des Text Chats aktiviert oder deaktiviert.

Verarbeitung von Kundendaten mit Salesforce:
Zur Bearbeitung von Kundenservice Anfragen und zur Kundenkommunikation per E-Mail oder Telefon gemäß Ihrer uns erteilten Einwilligung werden Ihre personenbezogenen Kundendaten in unserem CRM-System gespeichert und verarbeitet. Wir nutzen die Services Salesforce Service Cloud & Salesforce Marketing Cloud des Auftragsverarbeiter Salesforce (Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 München) ein.

Wenn Sie uns Ihre Einwilligung erteilt haben, werden wir über dieses System-E-Mail-Nutzungsinformationen (Versand, Öffnungen, Klicks) erheben, um unseren Service für Sie zu verbessern und Ihnen passendere Informationen zukommen zu lassen. Wenn Sie damit nicht mehr einverstanden sind, können Sie dem jederzeit unter „Meine Einstellungen“ widersprechen.

Kundenfeedback mit Salesforce Survey:
Wenn Sie unsere Unterstützungsdienstleistungen in Anspruch nehmen, laden wir Sie per E-Mail gegebenenfalls zur Teilnahme an einer Kundenzufriedenheitsumfrage ein. Die Teilnahme an der Umfrage ist freiwillig und dient dazu, die Qualität unserer Dienstleistungen zu verbessern. Die Ergebnisse der Umfrage werden in diesem Fall mit dem entsprechenden Kundenvorgang verknüpft und personalisiert gespeichert, um zielgerichtet die dazugehörige Dienstleistung bewerten zu können. Für die Durchführung der Umfrage werden Sie auf die Website des Unternehmens Salesforce (Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 München) weitergeleitet. Nähere Informationen zu deren Rechts- und Datenverarbeitungsgrundsätzen finden Sie unter https://www.salesforce.com/company/legal/.

Berechtigungen für Zugriffe auf Daten und Funktionen des Endgerätes durch den digitalen Dienst
Um den digitalen 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 TDDDG).

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.

Bitte beachten Sie, dass Sie im Falle eines Widerspruchs einer oder mehrerer Berechtigungen gegebenenfalls nicht sämtliche Funktionen unseres digitalen Dienstes nutzen können.

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

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.

Weitere Berechtigungen
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 digitale 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.

Basis-Funktionalität des digitalen Dienstes
Diese Verarbeitungen sind immer aktiv und notwendig, damit der digitale Dienst richtig funktioniert.

Funktional
Diese Verarbeitungen sind notwendig, damit Sie durch den digitalen Dienst navigieren und wesentliche Funktionen nutzen können. Sie ermöglichen Grundfunktionen, wie die Bestellabwicklung im Online-Shop und den Zugriff auf gesicherte Bereiche des digitalen Dienstes. Rechtsgrundlage für diese

Verarbeitungen ist §25 Abs. 2 Nr. 2 TDDDG, Art. 6 Abs. 1b DSGVO bzw. bei Drittstaaten Art. 44 ff. DSGVO.

Verarbeitungszweck nach Consent Kategorie	Login
Verarbeitendes Unternehmen mit Firmenadresse / Datenempfänger	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Genutzte Produkte/kurze Beschreibung des genutzten Services	Die MPP App und zConsole
Beschreibung des konkreten Verarbeitungszwecks	Login, Zuordnung von Alarmen zu Usern
Verantwortlichkeiten	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Verarbeitete Daten	E-Mailadresse
Speicherdauer	Nutzungsdauer
Rechtsgrundlage (Verarbeitung)	§25 Abs. 2 Nr. 2 TDDDG, Art. 6 Abs. 1b DSGVO bzw. bei Drittstaaten Art. 44 ff. DSGVO
Verarbeitung in Drittländern	--
Rechtsgrundlage (Drittländer)	--

Optionale Verarbeitungen
Diese Verarbeitungen werden verwendet, wenn Sie zusätzlichen Funktionen, wie z. B. den Chat nutzen. Die möglichen Funktionen werden im Abschnitt 1 dieses Datenschutzhinweises erläutert. Rechtsgrundlage für diese Verarbeitungen ist §25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO.

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

Verarbeitungszweck nach Consent Kategorie	Phishing Schutz
Verarbeitendes Unternehmen mit Firmenadresse / Datenempfänger	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Genutzte Produkte/kurze Beschreibung des genutzten Services	Phishing Schutz
Beschreibung des konkreten Verarbeitungszwecks	Leistungserbringung
Verantwortlichkeiten	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Verarbeitete Daten	IP, zu prüfende URL
Speicherdauer	Es werden keine Daten gespeichert
Rechtsgrundlage (Verarbeitung)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO
Verarbeitung in Drittländern	USA
Rechtsgrundlage (Drittländer)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO

Verarbeitungszweck nach Consent Kategorie	VPN
Verarbeitendes Unternehmen mit Firmenadresse / Datenempfänger	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Genutzte Produkte/kurze Beschreibung des genutzten Services	Sichere VPN-Verbindung für ein sicheres Wi-Fi Netzwerk
Beschreibung des konkreten Verarbeitungszwecks	Leistungserbringung
Verantwortlichkeiten	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Verarbeitete Daten	IP
Speicherdauer	Es werden keine Daten gespeichert
Rechtsgrundlage (Verarbeitung)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO
Verarbeitung in Drittländern	USA
Rechtsgrundlage (Drittländer)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO

Verarbeitungszweck nach Consent Kategorie	Contentinspection
Verarbeitendes Unternehmen mit Firmenadresse / Datenempfänger	Zimperium, 4055 Valley View Suite 300, Dallas, TX 75244
Genutzte Produkte/kurze Beschreibung des genutzten Services	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.
Beschreibung des konkreten Verarbeitungszwecks	Leistungserbringung
Verantwortlichkeiten	Deutsche Telekom Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 Bonn
Verarbeitete Daten	IP, zu prüfende URL
Speicherdauer	Es werden keine Daten gespeichert
Rechtsgrundlage (Verarbeitung)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO
Verarbeitung in Drittländern	USA
Rechtsgrundlage (Drittländer)	§25 Abs. 1 TDDDG, Art. 6 Abs. 1 a DSGVO bzw. bei Drittstaaten Art. 49 Abs. 1 a DSGVO

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.

Ergänzend strebt die Telekom Kooperationen mit anderen Service Anbietern an (z. B. Smart Home Services). Wenn Sie auch Nutzer dieser Services sind, können Sie Ihr jeweiliges Konto mit diesen verknüpfen. Diese Verknüpfung muss von Ihnen für jeden Service separat durchgeführt werden. Sobald Sie eine Verknüpfung vorgenommen haben, können die personenbezogenen Daten, die in diesen Datenschutzhinweisen aufgeführt sind, aus Ihrem jeweiligen Konto für den entsprechenden Service genutzt werden. Der jeweilige Service Anbieter informiert Sie über die Verarbeitung Ihrer personenbezogenen Daten.

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.

Teilweise findet eine Verarbeitung Ihrer Daten auch in Ländern außerhalb der Europäischen Union (also in sog. Drittstaaten) statt, derzeit etwa:

Speichern/Hosting von Kundendaten (ausgenommen Verkehrsdaten) durch Amazon Web Services EMEA SARL, Microsoft Ireland Operations Ltd., Google Cloud EMEA Limited, Irland und Salesforce.com Germany GmbH in Europa. Lediglich Administratoren Zugriffe im Rahmen eines technischen Supports sind aus den USA möglich.

Im Übrigen gilt: 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 Security GmbH, Friedrich-Ebert-Allee 71-77, 53113 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 10.02.2025