Datenschutzhinweise für App Versiegelte Cloud, Stand GPR 01.03.2018

Allgemeines

Der Schutz Ihrer persönlichen Daten hat für die T-Systems International 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.

1. **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.

2. **Wer ist verantwortlich für die Datenverarbeitung? Wer ist mein Ansprechpartner, wenn ich Fragen zum Datenschutz bei der Telekom habe?**
   Datenverantwortliche ist die T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main. 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.

3. **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).

4. 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. 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.

5. 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).

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

a) Registrierung: Eine Registrierung an der App ist nicht notwendig. Zur Benutzung der App geben Sie Username und Kennwort Ihres Zuganges zur Versiegelten Cloud ein.

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.

7. Berechtigungen

   Um die App auf Ihrem Gerät nutzen zu können, muss die App 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 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 für den Zugriff auf Ihre Daten in der Versiegelten Cloud.

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

   Die App benötigt Zugriff auf Kamera, Mikrofon, Fotos, Videos zu folgendem Zweck: Erstellung von Inhalten für die Versiegelte Cloud.

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

   Nein.

Allgemeine Einstellungen und Besonderheiten Ihrer „Versiegelte Cloud“

Verschiedene Einstellungen und Besonderheiten innerhalb Ihres Produktes können einerseits den Komfort im Umgang mit dem Produkt erhöhen, als auch Datenschutz/Sicherheitsbedenken hervorbringen. Bitte berücksichtigen Sie hier die für Sie angestrebte Schutzklasse.

Produktregistrierung

Zum Zeitpunkt der Produktregistrierung unter https://my.versiegelte-cloud.telekom-dienste.de/ erhalten sie eine Nummer zur Wiederherstellung des Passwortes, die PUK. Diese PUK wird Ihnen nur einmalig hier angezeigt! Bitte drucken Sie diese aus. Sollte kein Drucker zur Verfügung stehen, schreiben Sie die Nummer ab oder kopieren Sie sie in einem sicheren Passwortsafe. Bewahren Sie die PUK an einem sicheren für andere unzugänglichen Ort auf.

Wir weisen ausdrücklich darauf hin, dass bei Vergessen Ihres Passwortes und gleichzeitigem Verlust der PUK keine Wiederherstellung der angelegten Daten möglich ist!

Session Timeout

Ob es einen Timeout einer Sitzung gibt, kann vom Administrator festgelegt werden.
Um zu vermeiden, dass nicht-autorisierte Personen Nutzer-Sitzungen übernehmen können, ist eine kurze Ablauffrist der Sitzung bei Inaktivität sinnvoll. Lange Time-Outs sollten nur bei Nutzung des Dienstes innerhalb vertrauenswürdiger Umgebungen akzeptiert werden. Konsequenzen für die Schutzklassen des Trusted Cloud Datenschutzprofils (TCDP):
Für die Schutzklasse III sollten Sie zentral eine kurze Session Time-Out (z.B. 20 Minuten) erzwingen.

WebDAV

Die Nutzung von WebDAV erfordert meistens die lokale Speicherung von Nutzername und Passwort und ist daher sicherheitstechnisch nur empfehlenswert, wenn sich das genutzte Gerät in einer vertrauenswürdigen Umgebung befindet. Stellen Sie insbesondere sicher, dass der Speicherort der Daten auf Ihrem lokalen Gerät, der mit der Versiegelten Cloud verbunden wird, vor Fremdzugriff /Manipulation /Viren /Ransomware etc. geschützt ist.

Konsequenzen für die Schutzklassen des Trusted Cloud Datenschutzprofils (TCDP):
Um den Anforderungen der Schutzklassen II und III des TCDP zu entsprechen, sollten Sie WebDAV nicht verwenden.

2-Faktor-Authentisierung erzwingen

Konsequenzen für die Schutzklassen des Trusted Cloud Datenschutzprofils (TCDP):
Um den Anforderungen der Schutzklassen II und III des TCDP zu entsprechen, sollten Sie SMS Pass Code beim Login erzwingen.

Zusätzliche Passwort-Kriterien

Damit Kennwörter nicht leicht erraten werden können und ggf. bekannt gewordene Kennwörter nur über einen begrenzten Zeitraum gelten, können entsprechende Passwortregeln festgelegt werden.

Konsequenzen für die Schutzklassen des Trusted Cloud Datenschutzprofils (TCDP):

Für die Schutzklasse I genügt die generell gültige Anforderung einer Mindestlänge von 8 Zeichen. Für die Schutzklasse II sollten Sie:

- einen Klein- und einen Großbuchstaben,
- eine Ziffer und
- ein Sonderzeichen vorschreiben.

Für Schutzklasse III sollten Sie zusätzlich eine Ablaufzeit für Kennwörter definieren und eine Wiederverwendung der letzten Kennwörter unterbinden.

Speicherung und Löschung von Daten

Mit dem Beenden Ihres Vertrages wird Ihr Konto deaktiviert. Ihre Daten werden bis zu 3 Monate weiter vorgehalten. Ein Anspruch auf Erhaltung Ihrer Daten besteht nicht. Ohne Kenntnis Ihres privaten Schlüssels (PUK) bleiben ausschließlich Sie weiterhin in der Lage, Ihre Daten zu Entschlüsseln. Sollten Sie Ihren Vertrag binnen 3 Monaten nicht wieder aktivieren lassen, werden die Schlüssel zum Entschlüsseln Ihrer Daten gelöscht und der belegte Datenspeicher BSI/DIN-konform gelöscht.
Möchten Sie Ihre Daten früher gelöscht haben, senden Sie bitte eine formlose E-Mail an: VC_Sales@telekom.de unter Verwendung ihrer im Kundenkonto hinterlegten E-Mail.

Outlook-AddIn – Signatur

Das Outlook-AddIn (optional) erfordert Microsoft Outlook 2010 oder neuer. Es ist als Softwarekomponente signiert von unserem Technologiepartner „Uniscon universal identity control GmbH, Agnes-Pockels-Bogen 1, 80992 München, Germany“. Bitte vertrauen Sie bei der Installation dieser Komponente unserem Partner.

Office-AddIn – Signatur

Das Office-AddIn (optional) erfordert Microsoft Office 2010 oder neuer. Es ist als Softwarekomponente signiert von unserem Technologiepartner „Uniscon universal identity control GmbH, Agnes-Pockels-Bogen 1, 80992 München, Germany“. Bitte vertrauen Sie bei der Installation dieser Komponente unserem Partner.

Stand der Datenschutzhinweise 01.09.2018