

Datenschutzhinweise der T-Systems International GmbH für De-Mail

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 im Rahmen der De-Mail Leistungen 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 durch die T-Systems im Rahmen von De-Mail gelten. Weitere Informationen zum Thema Datenschutz erhalten Sie unter <https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz>.

2 Wer ist verantwortlich für die Datenverarbeitung? Wer ist mein Ansprechpartner, wenn ich Fragen zum Datenschutz bei der Telekom bzw. zu De-Mail der T-Systems habe?

Datenverantwortliche ist die T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main. Bei Fragen können Sie sich an unseren Kundenservice + 49 391 5976 2665 wenden oder an unseren Datenschutzbeauftragten, Herrn Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.

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

Die De-Mail Daten werden im De-Mail System unter hohen Sicherheitsvorkehrungen in zwei nach ISO 27001 zertifizierten Rechenzentren in Deutschland (Frankfurt am Main) mehrfach redundant gespeichert. Dabei halten wir uns an die gesetzlichen Lösch- und Aufbewahrungsfristen für die jeweiligen Datenarten.

3.1 Vertragsdaten

Wenn Sie als unser Kunde De-Mail nutzen, erfassen und verarbeiten wir die für die Begründung, Durchführung, Änderung und Beendigung des Vertrages erforderlichen nachfolgend aufgeführten Daten (Art. 6 Abs. 1 b) DSGVO):

3.1.1 Identitätsdaten

Zur eindeutigen Identifizierung erheben wir im Rahmen des Registrierungsprozesses gemäß § 3 Abs. 2 De-Mail-Gesetz persönliche Daten wie folgt:

Juristische Personen oder Personengesellschaften: Firma, Name oder Bezeichnung, Rechtsform, Registernummer, soweit vorhanden, Anschrift des Sitzes / der Hauptniederlassung, Namen der Mitglieder des Vertretungsorgans / der gesetzlichen Vertreter; sofern ein Mitglied des Vertretungsorgans / der gesetzliche Vertreter eine juristische Person ist, deren Firma, Name oder Bezeichnung, Rechtsform, soweit vorhanden, Registernummer, Anschrift des Sitzes / der Hauptniederlassung bzw.

Vertretungsberechtigte (natürliche) Person: Vorname, Name, Anschrift, Geburtsdatum und Geburtsort.

Diese Daten werden in einem Identifizierungsprozess anhand eines vorzulegenden aktuellen Handelsregisterauszuges sowie eines amtlichen Lichtbildausweises verifiziert. Alternativ können natürliche Personen auch den elektronischen Identitätsnachweis (eID-Funktion) mittels Personalausweis zur Online-Identifizierung nutzen. Es werden auch in diesem Fall ausschließlich die zuvor genannten Daten ausgelesen und gespeichert.

Sollten sich während der Dauer des Vertragsverhältnisses Änderungen an den Identitätsdaten ergeben, so sind die aktuellen Daten ebenfalls der T-Systems mitzuteilen und ggf. ist eine erneute Identifizierung erforderlich.

Die De-Mail Identitätsdaten werden getrennt von anderen Kundendaten verschlüsselt in einer Kundendatei im De-Mail System gespeichert und für die Dauer des Vertrages bis einschließlich 31.12. des Folgejahres nach Vertragsbeendigung aufbewahrt. Die Daten werden, bis auf die unter Punkt 7 genannten Fälle, nicht an Dritte weitergegeben.

3.1.2 Daten zu Abrechnungszwecken

Ihnen wird monatlich ein tarif- und leistungsabhängiges Entgelt zur Überlassung von De-Mail in Rechnung gestellt. Dazu erhebt und verarbeitet die T-Systems die Firmenbezeichnung sowie ggf. den Namen eines Ansprechpartners, Anschrift, Vertragsnummer (Referenz-ID), De-Mail Domain und Vertragstyp bzw. gebuchten Tarif sowie Ihre Kontoverbindungsdaten (bei SEPA-Lastschriftverfahren), Anzahl, Größe und Zeitstempel versandter De-Mails, genutzten Postfachspeicher, Anzahl zusätzlich angelegter Postfächer, genutzte Versandoptionen sowie die Empfängeradressen aus De-Mails.

Wenn Sie den Einzelverbindungsnaechweis beauftragen, erhalten Sie eine Übersicht über die von Ihnen versandten kostenpflichtigen De-Mails. Die Übersicht ermöglicht es Ihnen, Ihre Rechnung zu überprüfen.

3.1.3 Daten zur Bereitstellung der De-Mail Dienste

Bei der Nutzung von De-Mail fallen, wie bei anderen elektronischen Kommunikationsverbindungen auch, Verkehrsdaten an. Diese umfassen die De-Mail Adresse des Senders und des Empfängers, die ID des De-Mail Kontos, den De-Mail Diensteanbieter (DMDA) des Senders und des Empfängers, das Datum und den Zeitpunkt des Versands und des Eingangs, die gewählte Versandoption, das jeweils verwendete Authentisierungsniveau, die Größe der De-Mails, Inhalte der De-Mails, ggf. E-Mail-Adresse (Benachrichtigungsadresse).

Diese Daten werden für die Dauer der Vertragsbeziehung gespeichert bzw. wenn die Daten mit einer konkreten De-Mail verknüpft sind, solange bis Sie die jeweilige De-Mail in Ihrem Postfach löschen.

Die Nutzungsdaten umfassen beispielsweise die verwendeten Login-Daten, um die Authentifizierung zu ermöglichen. Diese Daten werden im De-Mail System für die Dauer ihrer Gültigkeit gespeichert (z. B. bis Sie Ihren Benutzernamen ändern oder eine neue Mobilfunknummer oder einen neuen Personalausweis hinterlegen) bzw. im Falle des Passworts bis nach dem dritten Passwortwechsel (270 Tage), um die Passworrichtlinien einzuhalten. Im Web-Frontend werden die Login-Daten unmittelbar nach Beendigung der Session gelöscht.

Personenbezogene Daten von Ihren Kontakten, die Sie selbst im persönlichen Adressbuch Ihres De-Mail Postfachs speichern, werden von uns so lange vorgehalten, bis Sie diese entweder selbst löschen oder das De-Mail Konto aufgelöst wird.

3.2 Daten- und Betriebssicherheit (Art. 6 Abs. 1 f DSGVO, § 100 TKG)

Die von Ihnen verwendeten Login-Daten werden neben der Verwendung zu vertraglichen Zwecken auch für Zwecke der Datensicherheit und zur Sicherstellung des ordnungsgemäßen Betriebs des De-Mail Systems erhoben und verwendet.

Darüber hinaus verzeichnet der Web-Server vorübergehend den Domain-Namen oder die IP-Adresse Ihres Computers, die Ressourcenanfrage Ihres Web-Browsers (URL) sowie den http-Antwort-Code.

Die protokollierten Daten werden ausschließlich für Zwecke der Datensicherheit, insbesondere zur Abwehr von Angriffsversuchen auf unseren Web-Server verwendet. Sie werden weder für die Erstellung von individuellen Anwenderprofilen verwendet noch an Dritte weitergegeben.

Die Logdateien werden nach 7 bzw. 90 Tagen automatisch aus dem De-Mail System gelöscht.

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

Wie unter 3.2 beschrieben wird das Nutzungsverhalten ausschließlich zu Zwecken der Datensicherheit und Sicherstellung des ordnungsgemäßen Betriebs (u. a. Betrugsprävention) ausgewertet. Eine Auswertung zu Werbezwecken oder Tracking findet auf den Seiten des De-Mail Web-Frontends (Registrierung, De-Mail Postfach) nicht statt.

5 Eingesetzte Techniken

5.1 Cookies

Wir setzen ausschließlich Session Cookies im De-Mail Web-Frontend ein. Session Cookies sind Cookies, die nur für die Dauer einer Internetsitzung (Session) auf Ihrem Computer gespeichert werden und für Transaktionen benötigt werden (z. B. für das Login oder den Abschluss der Registrierung). Sie enthalten lediglich eine Transaktions-ID. Der Web-Server löscht die Session nach der Abmeldung des Nutzers am De-Mail Web-Frontend bzw. nach Ablauf der Internetsitzung. Dadurch wird die Transaktions-ID ungültig.

Sie haben grundsätzlich die Möglichkeit, Ihren Web-Browser so einzustellen, dass Cookies gar nicht erst gespeichert werden. Bitte beachten Sie dabei aber, dass sie das De-Mail Web-Frontend dann nicht mehr nutzen können. Informationen zu den Browser-Einstellungen finden Sie unter:

<https://www.sicherdigital.de/sicher-surfen#sicher-surfen-browsereinstellungen>.

5.2 JavaScript

Unsere Webanwendung nutzt JavaScript. Grundsätzlich werden dabei keine JavaScript-Inhalte von externen Anbietern geladen.

Zur Anzeige von PGP verschlüsselten De-Mails interagiert unsere Anwendung mit der Erweiterung Mailvelope, falls Sie diese in Ihrem Web-Browser eingerichtet haben. Weitere Informationen zu Mailvelope und die Datenschutzhinweise des Anbieters finden Sie auf dessen Webseite: <https://www.mailvelope.com/de>.

6 Wo werden meine Daten verarbeitet?

Die Datenverarbeitung im Rahmen von De-Mail findet ausschließlich in Deutschland statt.

7 An wen gibt die T-Systems meine Daten weiter?

Einige Daten müssen unter strengen vertraglichen und gesetzlichen Auflagen weitergegeben werden:

7.1 An Auftragsverarbeiter

Das sind Unternehmen, die wir im gesetzlich vorgesehenen Rahmen mit der Verarbeitung von Daten beauftragen, Art. 28 DSGVO (Dienstleister, Erfüllungsgehilfen). Die T-Systems bleibt auch in dem Fall weiterhin für den Schutz Ihrer Daten verantwortlich. Wir beauftragen Unternehmen insbesondere in folgenden Bereichen: Identifizierung, IT, Beratung / Kundenservice, Druck / Lettershop. In den meisten Fällen handelt es sich bei den Auftragsverarbeitern um andere Gesellschaften des Telekom-Konzerns. Die Auftragsverarbeiter werden von uns regelmäßig kontrolliert.

7.2 Aufgrund gesetzlicher Verpflichtung (Art. 6 Abs. 1 c) und e) DSGVO)

Auf Verlangen muss die T-Systems International GmbH nach § 16 De-Mail-Gesetz Dritten Auskunft über Name und Anschrift eines De-Mail Nutzers erteilen, sofern der Dritte einen Rechtsanspruch gegen den Nutzer glaubhaft macht. Das Formular zum Auskunftersuchen nach § 16 De-Mail-Gesetz finden Sie hier:

<https://www.t-systems.de/de-mail/auskunftersuchen>

Zudem sind wir in bestimmten Fällen verpflichtet, Daten an staatliche Stellen zu übermitteln, wenn dies gesetzlich vorgeschrieben ist bzw. ein entsprechender Gerichtsbeschluss vorliegt (z. B. im Rahmen der Strafverfolgung oder der Terrorismusbekämpfung) (§§ 94 ff. StPO, § 2 Artikel 10-Gesetz, § 112 TKG i. V. m. § 7 KDAV).

8 Welche Rechte habe ich?

8.1 Auskunft zu verlangen zu Kategorien der verarbeiteten Daten, Verarbeitungszwecken, etwaigen Empfängern der Daten, der geplanten Speicherdauer (Art. 15 DSGVO);

8.2 die Berichtigung bzw. Ergänzung unrichtiger bzw. unvollständiger Daten zu verlangen (Art. 16 DSGVO) bzw. können Sie Ihre Daten über Ihr De-Mail Konto selbst anpassen;

8.3 eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu **widerrufen** (Art. 7 Abs. 3 DSGVO);

8.4 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);

8.5 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 Punkt 8.3 widerrufen oder einen Widerspruch gemäß Punkt 8.4 erklärt haben. Teilweise können Sie Daten auch selbst in Ihrem De-Mail Konto löschen;

8.6 unter bestimmten Voraussetzungen die **Einschränkung** von Daten zu verlangen, soweit eine Löschung nicht möglich bzw. die Löschpflicht streitig ist (Art. 18 DSGVO);

8.7 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);

8.8 sich bei der zuständigen **Aufsichtsbehörde** über die Datenverarbeitung zu **beschweren** (für De-Mail Verträge: Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit).

9 Wie kann ich De-Mail nutzen?

Der Zugang zum De-Mail Postfach erfolgt verschlüsselt, entweder über ein De-Mail Gateway, welches an Ihre E-Mail Infrastruktur angeschlossen wird, oder alternativ über eine Weboberfläche (Web-Frontend) mit einem aktuellen Web-Browser. Hier können Nachrichten erstellt und versendet, sowie unterschiedliche Versandoptionen ausgewählt werden. Eingehende und versendete Nachrichten werden in speziellen Ordnern abgelegt. Weitere Informationen, insbesondere zum Anmeldeverfahren und zum Leistungsumfang, finden Sie in den Leistungsbeschreibungen sowie im Informationsblatt nach § 9 De-Mail-Gesetz. Sie finden diese unter:

<https://www.telekom.de/agb/direkt?AGBID=2043>

10 Wie erhalte ich eine De-Mail Domain bzw. -Adresse?

Zur Nutzung von De-Mail wird eine De-Mail Adresse vergeben. Diese enthält bei natürlichen Personen den Vor- und Nachnamen bzw. Teile davon, sowie ergänzend eine Nummer, sofern die Kombination aus Vor- und Nachnamen bereits für einen anderen Nutzer vergeben wurde. De-Mail Adressen von Firmen und Institutionen haben eine Bezeichnung im Domainteil, welche in direktem Bezug zu Ihrer Firma, Namen oder sonstigen Bezeichnung steht. Die Bildung der De-Mail Adresse vor dem Domainteil obliegt Ihnen als Geschäftskunde. Um eine De-Mail Domain für Ihr Unternehmen zu erhalten, müssen Sie zunächst einen Termin mit einem unserer Kundenbetreuer (Fachvertriebsmitarbeiter) vereinbaren. Zusammen mit dem für Sie zuständigen Mitarbeiter werden Ihre Daten erfasst (Registrierung) und im Anschluss verifiziert (Identifizierung). Nach erfolgreicher Identifizierung erhalten Sie Ihre De-Mail Domain.

11 Wie funktioniert der Verzeichnisdienst De-Mail?

Sie haben die Möglichkeit, ausgewählte Daten (z. B. Ihren Firmennamen, De-Mail Adresse(n) und Anschrift) im De-Mail Verzeichnisdienst einzutragen. Dieser funktioniert wie ein öffentliches Verzeichnis (vgl. Telefonbuch), steht allerdings nur angemeldeten De-Mail Nutzern zur Verfügung. Den Umfang der Veröffentlichung Ihrer Daten können Sie jederzeit über Ihr De-Mail Konto beschränken oder die Eintragung auch vollständig löschen. Der Veröffentlichung Ihrer Daten im De-Mail Verzeichnisdienst stellt eine konkludente Zugangseröffnung dar, d.h. Sie erteilen die Erlaubnis, die behördliche Kommunikation über De-Mail abzuwickeln, was mit zusätzlichen Rechtsfolgen verbunden sein kann. Weitere Informationen finden Sie im Informationsblatt zu § 9 De-Mail-Gesetz.

12 Wie wird die Sicherheit meiner De-Mail Daten gewährleistet?

12.1 Allgemein

Als akkreditierter De-Mail Diensteanbieter erfüllen wir die durch das De-Mail-Gesetz geforderten und durch die Technische Richtlinie De-Mail konkretisierten hohen Anforderungen an die organisatorische und technische Sicherheit der angebotenen De-Mail Dienste, um Ihre bei uns vorgehaltenen personenbezogenen Daten vor unberechtigtem Zugriff und Missbrauch zu schützen. Die Einhaltung dieser Sicherheitsanforderungen wird regelmäßig durch die Aufsichtsbehörden (Bundesamt für Sicherheit in der Informationstechnik und Bundesbeauftragte(r) für Datenschutz und Informationsfreiheit) überprüft.

12.2 Verschlüsselung

12.2.1 Transportverschlüsselung

Die Kommunikation zwischen Web-Browser und dem De-Mail Postfach ist durch eine Transportverschlüsselung (TLS) gesichert. Bei der Transportverschlüsselung handelt es sich um eine Punkt-zu-Punkt-Verschlüsselung zwischen dem verwendeten Web-Browser des De-Mail Nutzers und den Servern des De-Mail Diensteanbieters. Die verwendeten Verschlüsselungsalgorithmen werden durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben.

12.2.2 Inhaltsverschlüsselung und Schadsoftwareprüfung

Der Inhalt von De-Mail Nachrichten ist sowohl beim De-Mail Diensteanbieter als auch bei der Übertragung zwischen den De-Mail Diensteanbietern verschlüsselt. Für diese Inhaltsverschlüsselung wird der S/MIME Standard verwendet.

Im Rahmen der Registrierung holen wir Ihre Einwilligung in die Schadsoftwareprüfung ein. Dazu sind wir gesetzlich verpflichtet. Wir dürfen Ihnen ohne diese Einwilligung die De-Mail Dienste nicht bereitstellen (§ 3 Abs. 4 Nr. 4 De-Mail-Gesetz). Beim Versand von Nachrichten findet eine automatische systemseitige Überprüfung auf Schadsoftware statt, um das De-Mail System vor Viren und anderer Schadsoftware zu schützen. Zu diesem Zweck wird der Inhalt der Nachrichten im Versand-Prozess kurzzeitig entschlüsselt um sie von einem Virenprüfwerkzeug überprüfen zu lassen. Anschließend wird der Inhalt der Nachricht wieder verschlüsselt und innerhalb des De-Mail Systems transportverschlüsselt übertragen. Nachrichten, die Schadsoftware enthalten, werden nicht versendet. In diesem Fall erhalten Sie eine entsprechende Systemmeldung. Eingehende Nachrichten werden ebenfalls auf Schadsoftware geprüft. Als infiziert festgestellte Nachrichten werden dem Empfänger nicht zugestellt. Sowohl der Sender als auch der Empfänger der Nachricht erhalten eine entsprechende Systemmeldung. Nachrichten, die während der Schadsoftwareprüfung als befallen identifiziert werden, werden nach Versand der Systemmeldungen gelöscht.

12.2.3 Ende-zu-Ende-Verschlüsselung

Darüber hinaus ist es möglich, eine De-Mail Nachricht via PGP oder S/MIME Ende-zu-Ende verschlüsselt zwischen Sender und Empfänger zu übertragen. Hierbei werden die Daten schon vom Sender verschlüsselt und können nur vom Empfänger wieder entschlüsselt werden. Eine Überprüfung auf Schadsoftware ist in diesem Fall nicht möglich. Dazu ist der vorherige Austausch entsprechender Schlüssel bzw. Zertifikate zwischen Sender und Empfänger erforderlich. Sowohl die S/MIME-Zertifikate im X.509 Format als auch die PGP-Schlüssel können im De-Mail Verzeichnisdienst anderen Nutzern bereitgestellt werden. Für eine Ende-zu-Ende-Verschlüsselung ist der Einsatz von spezieller Software notwendig.

13 Wozu dient die qualifizierte elektronische Signatur?

Die qualifizierte elektronische Signatur ist die Entsprechung zur herkömmlichen Unterschrift in der elektronischen Welt. Sie ermöglicht die langfristige Überprüfbarkeit der Urheberschaft einer Erklärung im elektronischen Datenverkehr, wie etwa einer elektronischen Nachricht oder eines anderen Dokuments. Mit Hilfe dieser Signatur ist zweifelsfrei feststellbar, wer ein Dokument erstellt hat und dass dieses Dokument danach nicht verändert wurde. So werden z. B. Versand- und Eingangsbestätigungen vom De-Mail Anbieter mit einer elektronischen Signatur versehen. Die qualifizierte elektronische Signatur besteht aus einem personengebundenen Signaturzertifikat (spezielle Datei), die entweder auf Smart-Cards oder auch auf dem Personalausweis mit Online-Ausweisfunktion gespeichert werden können. Beim elektronischen „Unterschreiben“ wird über den Inhalt der Nachricht ein sogenannter Hash-Wert gebildet und dieser mit dem Zertifikat signiert.

14 Informationen zur manuellen Überprüfung von Web-Browser-Zertifikaten

Die Echtheit der Webseite sowie die Verschlüsselung der Web-Browser-Kommunikation kann auch manuell überprüft werden. Hierzu kann der Fingerabdruck (Fingerprint) genutzt werden. Zur manuellen Prüfung kann der Fingerprint im Web-Browser (verfügbar unter Zertifikatsanzeige unter dem Menüpunkt Sicherheitseinstellungen) mit den u. a. Angaben verglichen werden. Zur erweiterten Prüfung sind auch die Vergleichswerte des Wurzelzertifikats aufgeführt.

Ein Fingerprint ist eine Folge von Zahlen und Buchstaben, mit der ohne weitere technische Unterstützung die Echtheit des Zertifikats im Browser auch manuell überprüft werden kann. Zum Wurzelzertifikat können, abhängig von den verwendeten mathematischen Verfahren, verschiedene Fingerprints generiert werden. Es wird hier der Fingerprint SHA1 in Datenblock-Notation dargestellt.

Name:	www.de-mail.t-systems.de
Seriennummer:	00 80 aa 32 a2 5a 60 43 78
Nicht gültig vor:	02.10.2017 (MESZ)
Nicht gültig ab:	07.10.2019 (MESZ)
Fingerprint nach SHA-1:	75 82 dd ce 9d 6a 3c b8 97 67 52 eb ab 4b 1f 83 6e e7 a3 9a
Fingerprint über das Wurzelzertifikat nach SHA-1:	55 a6 72 3e cb f2 ec cd c3 23 74 70 19 9d 2a be 11 e3 81 d1
Schlüsselkennung des Wurzelzertifikats:	b5 03 f7 76 3b 61 82 6a 12 aa 18 53 eb 03 21 94 bf fe ce ca
Aussteller:	TeleSec ServerPass Extended Validation Class 3 CA; T-TeleSec GlobalRoot Class 3