Antrag auf Auskunftsersuchen nach § 16 De-Mail-Gesetz

1. Checkliste

Bevor Sie einen Antrag auf Auskunftsersuchen nach § 16 De-Mail-Gesetz stellen, prüfen Sie bitte anhand der nachfolgenden Checkliste, ob die Voraussetzungen für einen wirksamen Antrag erfüllt sind! Andererseits können wir Ihren Antrag nicht bearbeiten.

- ☐ Die Auskunft ist erforderlich zur Verfolgung eines Rechtsanspruchs Ich habe meinen Rechtsanspruch unter Punkt 6 in der Antragsbegründung dargestellt.
- ☐ Das Rechtsverhältnis ist unter Nutzung von De-Mail zustande gekommen (Nachweise (De-Mail Kommunikation, Schriftstücke u. a.) habe ich dem Antrag beigefügt).
- ☐ Vollständige Angabe Ihrer Identitätsdaten (Bitte nutzen Sie dafür das Formular aus diesem Antrag!).
- ☐ Die zu beauskunftenden Daten beziehen sich auf einen De-Mail Account des De-Mail Diensteanbieters Deutsche Telekom Security GmbH.
- ☐ Legitimationsnachweis bei juristischen Personen (Bei juristischen Personen müssen Sie nachweisen, dass Sie legitimiert sind, für das Unternehmen den Antrag zu stellen).

2. Weitere Hinweise

Dieses Formular ist für Auskunftsersuchen nach § 16 De-Mail Gesetz gegenüber der Deutschen Telekom Security GmbH zu verwenden.

Beachten Sie bitte, dass wir keine Auskünfte zu De-Mail Konten geben können, die durch andere De-Mail Diensteanbieter verwaltet werden, da wir nicht über die geforderten Informationen verfügen.

Die Deutsche Telekom Security GmbH kann als akkreditierter Diensteanbieter den Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen verlangen. Wird bei der Bearbeitung Ihres Antrags festgestellt, dass die Vorgaben des Gesetzes zur Regelung von De-Mail Diensten zur gewünschten Auskunftserteilung nicht erfüllt sind, besteht kein Anspruch auf Rückerstattung des Entgelts.

Bitte senden Sie als Antragsteller den vollständig ausgefüllten Antrag nebst erforderlichen Nachweisen aus Ihrem De-Mail Postfach als **absenderbestätigte** De-Mail direkt an unser Funktionspostfach: **notaryservice@t-systems.de-mail.de**

3. Datenschutz

Die Verarbeitung erfolgt ausschließlich im Rahmen des § 16 De-Mail-Gesetz, d. h. zum Zwecke der rechtskonformen Erfüllung des darin enthaltenen Auskunftsanspruchs. Hierzu zählen die Antragsprüfung, die Auskunftserteilung und Unterrichtung des Nutzers sowie die Aufbewahrung für eine nachträgliche Überprüfung.

Wir weisen darauf hin, dass wir als akkreditierter Diensteanbieter nach dem Gesetz verpflichtet sind, den betroffenen Nutzer unverzüglich über die Erteilung einer Auskunft zu informieren. Auch sind wir zum Zwecke der Transparenz und Überprüfbarkeit der Berechtigung der Auskunftserteilung im Nachhinein verpflichtet, folgende Informationen zu dokumentieren und ausschließlich für diesen Zweck für drei Jahre aufzubewahren:

- Antrag zur Auskunftserteilung samt Angabe des Dritten (Auskunftssuchender),
- die Entscheidung des akkreditierten Diensteanbieters,
- die Identifizierungsdaten des bearbeitenden Mitarbeiters des akkreditierten Diensteanbieters,
- die Mitteilung des Ergebnisses an den auskunftsersuchenden Dritten,
- die Mitteilung über die Auskunftserteilung an den Nutzer und
- die jeweilige gesetzliche Zeit bei einzelnen Prozessen innerhalb der Auskunftserteilung.

Im Übrigen gelten die Datenschutzhinweise für De-Mail (https://www.t-systems.de/de-mail/datenschutz) und die darin enthaltenen Rechte für Betroffene.

4. Antragsteller/-in

☐ **Natürliche Person** (Privatperson)

☐ Frau ☐ Herr

Name

Vorname

Straße/Hausnr.

Land PLZ Ort

De-Mail Adresse

DEUTSCHE TELEKOM SECURITY GMBH
Aufsichtsrat: Adel Al-Saleh (Vorsitzender) | Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn, HRB 15241, Sitz der Gesellschaft: Bonn, Deutschland
WEEE-Reg.-Nr.: DE 56768674

Antrag auf Auskunftsersuchen nach § 16 De-Mail-Gesetz

4. Fortsetzung Antragsteller/-in

☐ **Juristische Person** (Unternehmen, Institution)

Name

Vertretungsberechtigte Person

☐ Frau ☐ Herr

Name

Vorname

Straße/Hausnr.

Land PLZ Ort

De-Mail Adresse

. d e - m a i l . d e

5. Zu beauskunftende De-Mail Adresse

Für die folgende De-Mail Adresse wird die Beauskunftung von Name und Anschrift beantragt.

De-Mail Adresse

. d e - m a i l . d e

6. Begründung für Auskunftsersuchen

7. Einwilligung in Überprüfung der Identitätsdaten

Hiermit willige ich ein, dass der für die angefragte De-Mail Adresse zuständige De-Mail Diensteanbieter meine hier angegebenen Identitätsdaten zur Feststellung der Richtigkeit gemäß § 16 Abs. 1 Nr. 4 De-Mail Gesetz bei meinem De-Mail Diensteanbieter überprüft. Diese Einwilligung ist nicht widerrufbar, da sie sich auf eine einmalige gesonderte Aktion bezieht.

Datum

Name des Antragstellers

Wichtige Informationen zu De-Mail
Informationsblatt gemäß § 9 De-Mail-Gesetz

1 Maßnahmen zur Verhinderung des Zugangs von Unbefugten zum De-Mail-Konto

1.1 Sichere Anmeldung

Eine Anmeldung am De-Mail-Konto über die Web-Oberfläche (Web-Frontend) erfordert spezielle Zugangsdaten. Neben der Anmeldung mit Benutzername und Passwort („normales" Authentisierungsniveau), ist auch eine Anmeldung mittels mobileTAN (mTAN), die an Ihr Mobiltelefon gesendet wird oder dem Personalausweis mit Online-Ausweisfunktion (eID-Funktion) möglich. Die beiden letzten Varianten stehen für das Authentisierungsniveau „hoch", das Ihnen einen noch höheren Schutz bietet. Bestimmte Aktionen können nur mit dem hohen Authentisierungsniveau durchgeführt werden. Dies umfasst beispielsweise die Nutzung des Verzeichnisdienstes und die Einrichtung einer Weiterleitungsadresse. Die Zugangsdaten müssen vor dem Zugriff Dritter stets geschützt aufbewahrt werden. Haben Sie die Vermutung, dass Unbefugte von diesen Kenntnis erlangt haben, so ändern Sie diese umgehend oder lassen Sie Ihr De-Mail-Postfach solange sperren, bis Sie über neue Zugangsdaten verfügen. Durch den Missbrauch Ihres De-Mail-Kontos können Ihnen oder auch anderen Benachteiligungen entstehen, die unter Umständen Rechtsfolgen nach sich ziehen können.

Ein in der Kundenumgebung betriebenes De-Mail-Gateway authentifiziert sich am De-Mail-Konto mittels eines Hardware-Tokens. Hierbei wird eine Chipkarte mit Zertifikaten zur Anmeldung mit hohem Authentisierungsniveau eingesetz.

1.2 Verschlüsselung

1.2.1 Transport- und Inhaltsverschlüsselung

Die Kommunikation zwischen dem De-Mail-Gateway in der Kundenumgebung bzw. dem Web-Zugriff per Internetbrowser 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 Internetbrowser oder Gateway des De-Mail-Nutzers und den Servern des De-Mail-Diensteanbieters („DMDA"). Die verwendeten Verschlüsselungsalgorithmen werden durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben.

Der Inhalt von De-Mail-Nachrichten ist sowohl beim DMDA als auch bei der Übertragung zu anderen DMDA verschlüsselt. Für diese Inhaltsverschlüsselung wird der S/MIME Standard verwendet.

1.2.2 Ende-zu-Ende Verschlüsselung

Darüber hinaus ist es möglich, eine De-Mail-Nachricht via PGP oder S/MIME Ende-zu-Ende verschlüsselt zu übertragen. Hierbei werden die Daten schon vom Absender verschlüsselt und können nur vom Empfänger wieder entschlüsselt werden. 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, die nicht Gegenstand des De-Mail-Angebotes der Telekom Security ist.

2 Kosten und Rechtsfolgen bei der Nutzung von De-Mail

2.1 Postfach- und Versanddienst

2.1.1 Kosten für die Nutzung von De-Mail

Beim Versand von De-Mails fallen Kosten an. Die Kosten können pro De-Mail-Empfänger je nach gewählter Versandoption unterschiedlich hoch sein. Die verbindlichen Preise für De-Mails und Versandoptionen finden Sie in der aktuellen Preisliste für De-Mail, die unter www.telekom.de/agb/direkt?AGBID=2043 jederzeit abrufbar ist. Sie haben jederzeit die Möglichkeit, Ihren De-Mail-Einzelverbindungsnachweis über Ihren Telekom Security Ansprechpartner anzufordern.

2.1.2 Versandoptionen

Ihnen stehen verschiedene Versandoptionen zur Verfügung. Mit der Option „persönlich/vertraulich"(§ 5 Abs. 4 De-Mail-Gesetz) können Sie bestimmen, dass sich der Empfänger mit hohem Authentisierungsniveau anmelden muss, um die Nachricht zu lesen. Möchten Sie De-Mails mit erhöhter Beweiswirkung versenden, dann stehen Ihnen hierfür die Versandoptionen „Einschreiben" oder „Absenderbestätigung" zur Verfügung. Eine öffentliche Stelle, die nach der Zivilprozessordnung oder dem Verwaltungszustellungsgesetz (VwZG) zur förmlichen Zustellung berechtigt ist, kann nach § 5 Absatz 9 De-Mail-Gesetz eine „Abholbestätigung" anfordern. Mit der „Abholbestätigung" gilt die Zustellung eines elektronischen Dokumentes nach § 5a Absatz 3 VwZG als nachgewiesen. Voraussetzung für eine „Abholbestätigung" ist, dass der Empfänger sich mit Authentisierungsniveau hoch anmeldet.

2.1.3 Schriftformersatz

Bitte beachten Sie, dass die De-Mail alleine für sich nicht das gesetzliche Schriftformerfordernis erfüllt. Hierfür ist grundsätzlich eine qualifizierte elektronische Signatur nach Signaturgesetz erforderlich. Ausnahme: Seit dem 01.07.2014 kann die De-Mail in folgenden Fällen die Schriftform ersetzen:

– Bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die jeweilige Behörde mit der Versandart „absenderbestätigt" nach § 5 Absatz 5 De-Mail-Gesetz (DMDA bestätigt dem Empfänger der De-Mail mittels qualifizierter elektronischer Signatur, dass der Sender mit Authentisierungsniveau hoch angemeldet war).

– Bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail nach § 5 Abs. 5 De-Mail-Gesetz (s.o.), bei der die Bestätigung des DMDA (Provider) die erlassene Behörde als Nutzer des De-Mail-Kontos erkennen lässt (vgl. § 3a Absatz 2 Satz 4 № 2 und 3 VwVfG, § 36 Absatz 2 Satz 4 № 2 und 3 SGB I, § 87a Absatz 3 № 2 und Absatz 4 Satz 3 AO).

2.1.4 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 Mail 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 (das ist eine spezielle Datei), das entweder auf besonderen Karten oder auch auf dem Personalausweis mit Online-Ausweisfunktion gespeichert werden kann. Zum elektronischen „Unterschreiben" fügt man dieses Zertifikat in das zu unterzeichnende Dokument ein.

2.2 De-Mail-Verzeichnisdienst

Jeder De-Mail-Kontoinhaber hat die Möglichkeit, ausgewählte Daten in einem Verzeichnisdienst einzutragen. Dieser funktioniert wie ein öffentliches Verzeichnis, steht allerdings nur angemeldeten De-Mail-Nutzern zur Verfügung. Eine Löschung der Daten aus dem Verzeichnisdienst ist jederzeit über die Kontoverwaltung möglich.

Die Nutzung des De-Mail-Verzeichnisdienstes ist kostenfrei.

2.3 Zugangseröffnung

Für die Kommunikation mit Behörden per De-Mail muss von beiden Seiten eine sogenannte Zugangseröffnung erteilt werden (vgl. § 3a Abs. 1 VwVfG, § 36a Abs. 1 SGB I sowie § 87a Abs. 1 Satz 1 AO), d. h. die Erlaubnis, die behördliche Kommunikation über De-Mail abzuwickeln. Behörden und öffentliche Stellen sind gesetzlich verpflichtet, den Zugang für die De-Mail-Kommunikation zu eröffnen, wobei die Zugangseröffnung in der Regel durch die Veröffentlichung der De-Mailadresse auf der Web-Seite der Behörde oder öffentlichen Stelle erfolgt.

Die Veröffentlichung Ihrer Unternehmensdaten bzw. Behördendaten im De-Mail-Verzeichnisdienst stellt ebenso wie die Veröffentlichung auf einer Web-Seite eine Zugangseröffnung im o. g. Sinne dar (konkludente Zugangseröffnung). Die Erklärung der Zugangseröffnung hat zur Folge, dass elektronische Dokumente rechtsverbindlich an den Empfänger zugestellt werden können. Ein elektronisches Dokument gilt als zugegangen, wenn es im De-Mail-Postfach des Empfängers in bearbeitbarer Weise vorliegt. Die Zustellung ist durch die Behörde mit der Versandoption „Abholbestätigung" nachweisbar (s. o.). Versand und Empfang werden bei jeder De-Mail mit einem Zeitstempel versehen und sind je nach genutzter Versandoption auch durch Sie nachprüfbar. Dies ist insbesondere bei der Einhaltung von Fristen und dem entsprechenden Nachweis relevant.

2.4 Sperrung und Auflösung des De-Mail-Kontos

Auf Verlangen des Kontoinhabers kann der Zugang zum Konto temporär gesperrt werden. Ein Zugriff auf das De-Mail-Konto und die darin gespeicherten Nachrichten ist dann nicht mehr möglich. Haben Sie einen Missbrauchsverdacht, dann erreichen Sie den Sperr-Notruf zur kostenfreien Sperrung Ihres Kontos jederzeit (24/7) unter der Rufnummer +49 116 116.

Wichtige Informationen zu De-Mail
Informationsblatt gemäß § 9 De-Mail-Gesetz

2.5 Die Sperrung eines De-Mail-Kontos kann auch erfolgen, wenn
– Tatsachen die Annahme rechtfertigen, dass die zur Anmeldung gespeicherten Daten nicht ausreichend fälschungssicher sind oder dass die sichere Anmeldung (hohes Authentisierungsniveau) Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung des Anmeldevorgangs zulassen,
– eine Anordnung der zuständigen Behörde erfolgt,
– ein Sperrgrund gemäß den Allgemeinen Geschäftsbedingungen De-Mail vorliegt.

2.6 Ein aktives De-Mail-Konto kann aufgelöst werden durch
– Kündigung oder
– behördliche Anordnung.

2.7 Einstellung der Tätigkeit
Im Falle einer Einstellung des De-Mail-Dienstes seitens der Telekom Security werden wir Sie hierüber im Vorfeld benachrichtigen und Ihnen die die daraus resultierenden Folgen und Maßnahmen erläutern. Übernimmt kein anderer Diensteanbieter das De-Mail-Konto, wird sichergestellt, dass die in den Postfächern gespeicherten Daten für mindestens drei Monate ab dem Zeitpunkt der Benachrichtigung für Sie abrufbar und exportierbar bleiben.

2.8 Vertragsbeendigung
Nach Vertragsende können Sie für einen Zeitraum von drei Monaten noch auf Nachrichten in Ihrem De-Mail-Postfach zugreifen. Der Empfang oder Versand neuer De-Mail-Nachrichten ist nach Vertragsende jedoch nicht mehr möglich.

2.9 Einsichtnahme/Auskunftsanspruch
Auf Verlangen erhalten Sie Einsicht in die Sie betreffenden Daten, die die Telekom Security zwecks ihrer Dokumentationspflicht gemäß § 13 De-Mail-Gesetz speichern muss. Auf Verlangen muss die Telekom Security nach § 16 De-Mail-Gesetz auch Dritten Auskunft über Name und Anschrift eines De-Mail-Nutzers erteilen, sofern der Dritte einen Rechtsanspruch gegen den Nutzer glaubhaft macht. Weitere Informationen zur Auskunft finden Sie in den Datenschutzhinweisen zu De-Mail.

3 Umgang mit Schadsoftware
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 werden die Nachrichten über einen transportverschlüsselten Kanal ohne Inhaltsverschlüsselung an ein Virenprüftool innerhalb des De-Mail-Systems übermittelt. 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 Absender 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.