KURZGUTACHTEN

ZUM

DE-MAIL GUTACHTEN FÜR DEN DATENSCHUTZ-NACHWEIS NACH § 18 ABS. 3 NR. 4 DE-MAIL-GESETZ

Version:	1.1
Prüfgegenstand:	De-Mail Dienstumgebung der Deutsche Telekom Security GmbH
Verantwortliche Stelle:	Deutsche Telekom Security GmbH Bonner Talweg 100 53113 Bonn
Prüforganisation:	TÜV Informationstechnik GmbH TÜV NORD GROUP Langemarckstr. 20 45141 Essen
Verfasser/Gutachter:	Jörg Schließke, Tobias Mielke
Datum:	18.03.2021

Inhalt

1 Einleitung

Gemäß § 1 Abs. 1 De-Mail-Gesetz sind De-Mail-Dienste definiert als Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen. Dabei dürfen De-Mail-Dienste nur von De-Mail-Diensteanbietern betrieben werden, die nach diesem Gesetz akkreditiert worden sind. Gemäß § 17 Abs. 3 De-Mail-Gesetz ist die Akkreditierung spätestens nach drei Jahren zu erneuern.

Hierzu müssen De-Mail-Diensteanbieter nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz die Erfüllung der datenschutzrechtlichen Anforderungen an das Datenschutzkonzept für die eingesetzten Verfahren und die eingesetzten technischen und organisatorischen Maßnahmen insbesondere der Technischen Richtlinie des BSI TR-01201 nachweisen. Der Nachweis wird schließlich durch ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) geführt, welches ausgestellt wird, wenn sämtliche Anforderungen erfüllt sind, die vom BfDI im Kriterienkatalog für den Datenschutz-Nachweis (De-Mail-Kriterienkatalog) niedergelegt worden sind.

Zum Erhalt bzw. Erneuerung der Akkreditierung hat der De-Mail-Diensteanbieter die entsprechenden Anforderungen aus dem De-Mail-Gesetz zu erfüllen und nachzuweisen.

Seit dem 01.07.2020 hat die **Deutsche Telekom Security GmbH** für den Bereich De-Mail die Gesamtrechtsnachfolge nach dem Umwandlungsgesetz der T-Systems International GmbH angetreten. Die Deutsche Telekom Security GmbH ist eine Ausgründung aus der T-Systems International und hat als bisherige interne Organisationseinheit der T-Systems International das Projekt „De-Mail“ bereits in vollem Umfang verantwortet. Die Deutsche Telekom Security GmbH ist 100%ige Tochtergesellschaft der Deutschen Telekom AG. Zu dem Konzern der Deutschen Telekom AG gehören zwei Tochtergesellschaften, die als De-Mail Diensteanbieter am Markt agieren. Es handelt sich um die Telekom Deutschland GmbH sowie um die Deutsche Telekom Security GmbH. Die Deutsche Telekom Security GmbH bedient im Rahmen des De-Mail Dienstes Großkunden.

Die Deutsche Telekom Security GmbH (ehemals T-Systems International GmbH) bietet seit 2012 De-Mail-Dienste an. Das letzte Datenschutz-Zertifikat wurde der Deutsche Telekom Security GmbH vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 04. Mai 2018 erteilt.

Im Rahmen der Re-Akkreditierung der Deutsche Telekom Security GmbH als De-Mail-Diensteanbieter soll die Erfüllung der datenschutzrechtlichen Kriterien gegenüber dem BfDI auf Basis eines Datenschutznachweises gem. § 18 Abs. 3 Nr. 4 De-Mail-Gesetz erbracht werden, welcher von einer sachverständigen Stelle für Datenschutz zu erstellen ist. Für die Erstellung des entsprechenden De-Mail Datenschutznachweises wurde die TÜV Informationstechnik GmbH (Fachstelle für Datenschutzsachverständige) beauftragt.

Der Begutachtung durch die Fachstelle für Datenschutzsachverständige der TÜV Informationstechnik GmbH wurde hierbei der De-Mail-Kriterienkatalog in der Version 2.1[1] zugrunde gelegt.

Der De-Mail-Kriterienkatalog schreibt die Begutachtung aller Dienste und Funktionalitäten vor. Die Struktur des Gutachtens orientiert sich dabei an dem Aufbau des De-Mail Kriterienkatalogs und beinhaltet technische und rechtliche Aspekte, die im Wesentlichen nach vier Kriterien geprüft werden:

- Rechtliche Zulässigkeit unter Angabe der rechtlichen Erlaubnistatbestände sowie Begründung der Erforderlichkeit zur Datenverarbeitung;
- Dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen einschließlich Verschlüsselung, Authentifizierung und Signaturen sowie Speicherbegrenzung;
- Rechte der Betroffenen;
- Datenschutzmanagement.

Die vorgenannten Kriterien wurden vollumfänglich in einem ausführlichen Gutachten der TÜV Informationstechnik GmbH für die Re-Zertifizierung behandelt.

Neben der Begutachtung der vom De-Mail-Gesetz geforderten Dienste und Funktionalitäten sieht der De-Mail-Kriterienkatalog ferner auch die Begutachtung der optionalen Dienste *Dokumentenablage* und *Identitätsbestätigungsdienst* vor, welche von der Deutsche Telekom Security GmbH nicht angeboten werden und folglich im Rahmen der Begutachtung nicht behandelt wurden.

Die für die Akkreditierung erforderliche Erfüllung der datenschutzrechtlichen Anforderungen für die Gestaltung und den Betrieb der De-Mail-Dienste umfasst insbesondere die Beachtung der informationellen Selbstbestimmung der Betroffenen nach Maßgabe der datenschutzrechtlichen Bestimmungen und die Gewährleistung ausreichender Sicherheit für die im Rahmen der De-Mail-Dienste verarbeiteten personenbezogenen Daten.

Neben der Einhaltung der Regelungen des De-Mail-Gesetzes müssen insbesondere die Datenschutz-Grundverordnung sowie das Bundesdatenschutzgesetz berücksichtigt werden.

Ziel dieses Kurzgutachtens ist es, potentiellen Geschäftskunden das De-Mail Verfahren transparent darzustellen, die Anforderungen dieses Gesetzes zu benennen sowie die Umsetzung durch die Deutsche Telekom Security GmbH überblicksartig und zusammenfassend darzustellen.

[1] https://www.bfdi.bund.de/DE/Datenschutz/Themen/Brief_Paket/DeMailInfosAnbieterArtikel/Kriterienkatalog-Nachweis.html (zuletzt besucht: 08.03.2021).

2 Verfahren

Die rechtliche und technische Begutachtung für den Datenschutz-Nachweis hat alle Tatsachen, Bestandteile und Arbeitsabläufe umfasst, die für den Prüfgegenstand gemäß dem detaillierten De-Mail-Kriterienkatalog (Version 2.1) zu begutachten sind. Dieser bezieht sich auf die oben genannten gesetzlichen Anforderungen und darüber auf einzelne Anforderungen aus der Technischen Richtlinie De-Mail (BSI TR-01201 De-Mail).

Im Oktober und November 2020 waren Gegenstand der Begutachtung durch die TÜV Informationstechnik GmbH mehrere anlass- bzw. themenbezogene Remote-Prüfungen zum De-Mail Dienst. Ferner sind in diesem Zeitraum neben dem sog. Datenschutz- und Datensicherheitskonzept (SDSK) des De-Mail-Diensteanbieters zahl- und umfangreiche Dokumente zur Begutachtung vorgelegt worden. Für die Überprüfung der Umsetzung der technisch-organisatorischen Maßnahmen fanden im November und Dezember 2020 zahlreiche Remote Überprüfungen statt (u.a. zu der BSI TR 01201 Teil 6.2 Kap. 11 Schutz vor physischem Zugang und Umwelteinflüssen, Kap. 15 Lieferantenbeziehungen, Kap. 18 Richtlinienkonformität (Kap. 18.1.6 Identifizierung der Nutzer), Kap. 10 Kryptographie, Kap. 12.3 Backup sowie Kap. 13 (Sicherheit in der Kommunikation).

Es fanden zusätzlich regelmäßige Telefonkonferenzen mit fachverantwortlichen Mitarbeiterinnen und Mitarbeitern sowie regelmäßige E-Mail-Kommunikationen und Interviews statt, um konkret ausgewählte Themenkomplexe zu behandeln, die folglich im Datenschutz Gutachten ihre Berücksichtigung fanden.

3 Zusammenfassung der Prüfergebnisse

Die Fachstelle für Datenschutzsachverständige der TÜV Informationstechnik GmbH hat dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit empfohlen, das Datenschutz-Zertifikat im Rahmen der Re-Zertifizierung weiterhin zu erteilen, da sämtliche Anforderungen aus dem De-Mail-Kriterienkatalog sowie die einschlägigen Anforderungen nach dem De-Mail-Gesetz, der Datenschutz-Grundverordnung sowie des Bundesdatenschutzgesetzes durch die Deutsche Telekom Security GmbH erfüllt werden.

Der BfDI hat gegenüber der Deutsche Telekom Security GmbH das Datenschutz-Zertifikat für die Re-Akkreditierung gem. § 17 Abs. 3 De-Mail-Gesetz am 01.03.2021 erteilt.

3.1 Rechtliche Zulässigkeit

Die Anforderungen des De-Mail-Kriterienkatalogs zur rechtlichen Zulässigkeit und zur Erforderlichkeit der Datenverarbeitung werden von der Deutsche Telekom Security GmbH erfüllt.

Dies betrifft die allgemeinen datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung sowie die im De-Mail-Gesetz für die einzelnen Dienste und Funktionalitäten genannten speziellen Anforderungen und die weiteren im De-Mail-Kriterienkatalog genannten einschlägigen Rechtsvorschriften. Die eingehende Begutachtung hat insbesondere Folgendes ergeben:

Für jede Art der Verarbeitung personenbezogener Daten liegt stets eine gesetzliche Ermächtigung oder Einwilligung der betroffenen Personen vor. Dabei wird bei der Verarbeitung personenbezogener Daten stets der Grundsatz der Erforderlichkeit und der Datensparsamkeit berücksichtigt, sodass nur erforderliche Daten im Rahmen ihrer Zweckbestimmung erhoben und verarbeitet werden. Nach Wegfall der Erforderlichkeit werden die personenbezogenen Daten nach dem Stand der Technik sicher gelöscht. Löschfristen sämtlicher verarbeiteten personenbezogenen Daten werden berücksichtigt und anhand entsprechender Maßnahmen und Prozesse umgesetzt.

Die Deutsche Telekom Security GmbH setzt andere Unternehmen als Auftragsverarbeiter ein. Die datenschutzrechtlichen Anforderungen der Auftragsverarbeitung werden vollumfänglich erfüllt. Das Fernmeldegeheimnis wird gewahrt.

Die Deutsche Telekom Security GmbH kommt ihren Aufklärungs- und Informationspflichten gemäß dem De-Mail-Gesetz und der DSGVO bzw. BDSG vollumfänglich nach. Den De-Mail-Nutzern werden den gesetzlichen Anforderungen entsprechende detaillierte Informationen über die De-Mail-Dienste, über Datenschutz und Datensicherheit und über die Rechte der Betroffenen zur Verfügung gestellt.

Die Nutzung der De-Mail-Dienste wird gemäß dem gesetzlichen Kopplungsverbot nicht vom Abschluss anderer Verträge oder von der Einwilligung in die Nutzung anderer Dienste der Deutsche Telekom Security GmbH abhängig gemacht. Die erhobenen Daten der Nutzer werden ferner nicht für Adresshandel oder Werbung verwendet.

Um die Vertraulichkeit, Integrität und Authentizität der Nachrichten zu gewährleisten, werden diese transportverschlüsselt und inhaltsverschlüsselt nach dem Stand der Technik übertragen. Eine Ende-zu-Ende-Verschlüsselung der Nachrichten, welche vom Nutzer eingerichtet werden kann, wird vom System unterstützt.

Die De-Mail-Kunden können, wenn sie sicher an ihrem De-Mail-Konto angemeldet sind, automatische Weiterleitungen für die an sie gerichteten De-Mails einrichten und jederzeit zurücknehmen.

Auf ausdrückliches Verlangen der Nutzer können ihre De-Mail-Adressen, ihre hinterlegten Identitätsdaten und ihre öffentlichen Schlüssel für die zusätzliche Verschlüsselung von Nachrichten (Ende-zu-Ende-Verschlüsselung) in einem Verzeichnisdienst veröffentlicht und auf Verlangen der Nutzer wieder aus dem Verzeichnisdienst gelöscht werden. Daneben wird Großkunden die Möglichkeit einer Zugangseröffnung angeboten, um die Kommunikation mit

Behörden per De-Mail durchführen zu können.

3.2 Dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen

Die Anforderungen des De-Mail-Kriterienkatalogs zur Dienstespezifischen Umsetzung der technisch-organisatorischen Anforderungen werden von der Deutsche Telekom Security GmbH erfüllt.

Für sämtliche von der Deutsche Telekom Security GmbH angebotenen De-Mail-Dienste sind geeignete und erforderliche technische und organisatorische Maßnahmen implementiert und umgesetzt worden. Sämtliche Anforderungen an die Sicherheit der Verarbeitung i.S.d. Art. 32 DSGVO (insb. Pseudonymisierung, Verschlüsselung personenbezogener Daten, Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, Rasche Wiederherstellbarkeit) werden vollumfänglich erfüllt. Durch regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen wird die Sicherheit der Verarbeitung durch die Deutsche Telekom Security GmbH gewährleistet.

Ferner wird die Einhaltung der technischen Anforderungen durch Zertifizierungen nach ISO 27001 geprüft.

Sämtliche Mitarbeiter der Deutsche Telekom Security GmbH werden zur Einhaltung der Datenschutzanforderungen auf die Vertraulichkeit und das Fernmeldegeheimnis verpflichtet. Ferner werden die Mitarbeiter regelmäßig im Hinblick auf den Datenschutz geschult und sensibilisiert.

Die zum Einsatz kommenden Verschlüsselungstechniken entsprechen dem Stand der Technik und halten den gesetzlichen Anforderungen der Datenschutz-Grundverordnung stand.

Die wesentlichen in der Datenschutz-Grundverordnung genannten Zielvorgaben der IT-Sicherheit, insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, sind vollumfänglich von den standardmäßigen technischen und organisatorischen Maßnahmen der Telekom abgedeckt. Zudem wird zur grundsätzlichen Umsetzung der Sicherheit der Verarbeitung eine Datenschutz Schulung zu den technischen und organisatorischen Maßnahmen durchgeführt. Das Informationssicherheitsmanagementsystem wird unter anderem in der Informationssicherheitsleitlinie erläutert und ausführlich dargestellt.

3.3 Rechte der Betroffenen

Die Anforderungen des De-Mail-Kriterienkatalogs zu den Betroffenenrechten werden von der Deutsche Telekom Security GmbH ebenfalls erfüllt. Sämtliche Dokumentationen und Prozesse im Umgang mit Betroffenenrechten der Deutsche Telekom Security GmbH wurden einer Begutachtung unterzogen.

Die sich aus dem De-Mail-Gesetz, der Datenschutz-Grundverordnung sowie dem Bundesdatenschutzgesetz ergebenden Rechte der Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Widerruf der Einwilligung, Recht auf Datenübertragbarkeit) werden durch geeignete organisatorische Verfahren, insbesondere durch ausführliche Datenschutzhinweise, Konzernrichtlinien sowie Organisationsanweisungen gewährleistet.

Darüber hinaus können De-Mail-Nutzer zahlreiche Aktionen, wie z.B. Änderungen und Löschungen ihrer personenbezogenen Daten, über Accounteinstellungen in ihrem De-Mail-Konto selbstständig vornehmen, was zu einer zusätzlichen Benutzerfreundlichkeit beiträgt.

Die Kontaktdaten des Datenschutzbeauftragten (Name, Adresse, E-Mail-Adresse) können über die Datenschutzhinweise aufgerufen werden. Folglich haben die betroffenen Personen bei Fragen und Beschwerden stets die Möglichkeit, sich an den Datenschutzbeauftragten zu wenden.

3.4 Datenschutzmanagement

Die Anforderungen des De-Mail-Kriterienkatalogs zum Datenschutzmanagement werden von der Deutsche Telekom Security GmbH erfüllt.

Das Datenschutzmanagementsystem ist bei der Deutsche Telekom Security GmbH als dauerhafter Datenschutzprozess angelegt, welcher einen kontinuierlichen Prozess zum Ziel hat.

Das sog. Privacy & Security Assessment (PSA-Verfahren) stellt das Kernelement zur Wahrung von Sicherheit und Datenschutz bei der Deutsche Telekom Security GmbH dar. Grundsätzlich müssen alle Produkte, Dienstleistungen und IT-Systeme der Deutsche Telekom Security GmbH, die eine Verarbeitung personenbezogener Daten zum Gegenstand haben, das PSA-Verfahren durchlaufen. Das Prinzip des PSA-Verfahrens ist ebenso für Betroffene frei zugänglich im Internet erläutert.[2]

Mithilfe des PSA-Verfahrens wird frühzeitig die technische Sicherheit und der Datenschutz in den Entwicklungsprozessen bei der Deutsche Telekom Security GmbH verankert. Es stellt ein standardisiertes Verfahren dar, welches Sicherheits- und Datenschutzanforderungen in die Produkt- und Systementwicklung integriert und dadurch ein angemessenes Schutzniveau der Telekom Services und Anwendungen gewährleistet.

Ferner basiert das PSA-Verfahren auf einem standardisierten Datenschutz- und Sicherheitskonzept (SDSK), welches sich aus Systembeschreibungen, Berechtigungskonzepten, Datenschutzinformationen, Anforderungskatalogen, Maßnahmenplänen, Systemkategorisie-

[2] https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/details/privacy-and-security-assessment-verfahren-342724 (zuletzt aufgerufen am 09.03.2021).

rungen und Datenschutz Rahmenfreigaben zusammensetzt. Somit bildet das PSA-Verfahren insgesamt die Anforderungen der Datenschutz-Grundverordnung ab und gewährleistet, dass Systeme laufend überprüft sowie ein einheitliches und angemessenes Sicherheits- und Datenschutzniveau aufrechterhalten wird.

Schließlich erfolgen zur Einhaltung der Vorgaben der Konzernrichtlinie Kontrollen, die vom Konzerndatenschutzbeauftragen anhand eines jährlichen Kontrollplans durchgeführt werden.

Die Verantwortlichkeiten im Bereich Datenschutz sind bei der Deutsche Telekom Security GmbH klar geregelt. Ein Konzerndatenschutzbeauftragter ist bestellt, auch eine Vertretung ist vorgesehen. Der Konzerndatenschutzbeauftragte kann seine Aufgaben gesetzeskonform ausführen und erhält hierzu die erforderliche Unterstützung durch den Konzerndatenschutz. Er wird umfassend und frühzeitig eingebunden, wenn Fragen des Datenschutzes berührt sind bzw. sein können. De-Mail-Nutzer und andere Interessenten können sich direkt an den Konzerndatenschutzbeauftragten wenden.

Die Deutsche Telekom Security GmbH verfügt folglich über ein den Anforderungen entsprechendes Datenschutzmanagement, welches sich aus zahlreichen erforderlichen Dokumenten wie z.B. Verfahrensbeschreibungen, Konzernrichtlinien zum Datenschutz, Datenschutzkonzept, Datenschutz-Folgenabschätzungen, Verzeichnis von Verarbeitungstätigkeiten etc. zusammensetzt.

Die Mitarbeiter der Deutsche Telekom Security GmbH werden auf die Vertraulichkeit und auf das Fernmeldegeheimnis verpflichtet sowie umfassend und regelmäßig zum Datenschutz und zur Datensicherheit geschult bzw. sensibilisiert. Im Rahmen von Auftragsverarbeitungsverhältnissen wird vertraglich sichergestellt, dass ein angemessenes Maß an Datenschutz und Datensicherheit bei Auftragsverarbeitern besteht, was zusätzlich durch regelmäßige Kontrollen seitens der Deutsche Telekom Security GmbH überprüft wird.