KURZGUTACHTEN

ZUM

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

Version:	1.0
Prüfgegenstand:	De-Mail Dienstumgebung der 1&1 De-Mail GmbH
Verantwortliche Stelle:	1&1 De-Mail GmbH Elgendorfer Straße 57 56410 Montabaur
Prüforganisation:	TÜV Informationstechnik GmbH TÜV NORD GROUP Am TÜV 1 45307 Essen
Verfasser/Gutachter:	Jörg Schließke, Tobias Mielke
Datum:	11.07.2022

Inhalt

1 EINLEITUNG 3

2 VERFAHREN 4

3 ZUSAMMENFASSUNG DER PRÜFERGEBNISSE 5

3.1 Rechtliche Zulässigkeit 5

3.2 Dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen 6

3.3 Rechte der Betroffenen 7

3.4 Datenschutzmanagement 8

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.

Zur Erneuerung der Akkreditierung hat der DMDA die Voraussetzungen nach § 18 Abs. 1 De-Mail-G zu erfüllen und nachzuweisen. Ein entsprechender Datenschutznachweis gem. § 18 Abs. 3 Nr. 4 De-Mail-G ist hierfür durch den DMDA zu erbringen.

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.

Die **1&1 De-Mail GmbH**[1] bietet seit 2013 De-Mail-Dienste an. Das letzte Datenschutz-Zertifikat wurde der 1&1 vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 09.11.2020 erteilt.

Im Rahmen der Re-Akkreditierung der 1&1 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 TÜV Informationstechnik GmbH ist hierbei der De-Mail-Kriterienkatalog in der Version 2.1 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;

[1] Im Folgenden: 1&1.

- 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 begutachtet.

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 1&1 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 auch die einschlägigen Normen des Telekommunikationsgesetzes, die Datenschutz-Grundverordnung, das Telekommunikation-Telemedien-Datenschutzgesetz sowie das Bundesdatenschutzgesetz berücksichtigt werden.

Ziel dieses Kurzgutachtens ist es, potentiellen Privat- sowie Geschäftskunden das De-Mail Verfahren transparent darzustellen, die Anforderungen dieses Gesetzes zu benennen sowie die Umsetzung durch die 1&1 überblicksartig und zusammenfassend darzustellen.

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 hinaus auf einzelne Anforderungen aus der Technischen Richtlinie De-Mail (BSI TR-01201 De-Mail).

Gegenstand der Begutachtung durch die TÜV Informationstechnik GmbH waren anlass- bzw. themenbezogene Remote-Prüfungen zum De-Mail Dienst. Ferner wurden den Prüfern zahl- und umfangreiche Dokumente zur Begutachtung vorgelegt.

Die Überprüfungen zur Funktionalität und Interoperabilität haben zwischen dem 06.12.2021 – 08.12.2021 stattgefunden. Die Ergebnisse aus dieser Prüfung wurden bei der Erstellung des De-Mail-Datenschutz-Gutachtens berücksichtigt.

Die Überprüfung der Umsetzung von technisch organisatorischen Maßnahmen hat im Rahmen der ISO 27001 Auditierung im Zeitraum vom 29.11.2021 – 08.12.2021 stattgefunden. Themenbereiche waren u.a. Cryptography, Physical and Environmental Security, Zugangssteuerung, Operations Security 1-3, Management Organisation, Compliance, Risiko Management. Die Ergebnisse hieraus wurden bei der vorliegenden Prüfung berücksichtigt.

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 TÜV Informationstechnik GmbH hat dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit empfohlen, das Datenschutz-Zertifikat im Rahmen der Re-Zertifizierung des De-Mail Dienstes weiterhin zu erteilen, da sämtliche Anforderungen aus dem De-Mail-Kriterienkatalog sowie die einschlägigen Anforderungen nach dem De-Mail-Gesetz, der Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes sowie des Telekommunikationsgesetzes durch die 1&1 erfüllt werden.

Der BfDI hat gegenüber der 1&1 das Datenschutz-Zertifikat für die Re-Akkreditierung gem. § 17 Abs. 3 De-Mail-Gesetz am 27.06.2022 erteilt.

3.1 Rechtliche Zulässigkeit

Die Anforderungen des De-Mail-Kriterienkatalogs zur rechtlichen Zulässigkeit und zur Erforderlichkeit der Datenverarbeitung werden von der 1&1 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 Ermächtigungsgrundlage vor. Dabei wird bei der Verarbeitung personenbezogener Daten 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 1&1 setzt andere Unternehmen als Auftragsverarbeiter ein. Die datenschutzrechtlichen Anforderungen der Auftragsverarbeitung werden hierbei vollumfänglich erfüllt. Das Fernmeldegeheimnis gemäß dem Telekommunikation-Telemedien-Datenschutzgesetz wird gewahrt.

Die 1&1 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 1&1 abhängig gemacht. Die erhobenen Daten der Nutzer werden ferner nicht für Adresshandel oder Werbung verwendet.

Ferner wird Privatkunden angeboten, pseudonyme De-Mail-Adressen einzurichten und für die De-Mail Kommunikation zu verwenden.

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 Nutzern auf ausdrückliches Verlangen 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 1&1 erfüllt.

Für sämtliche von der 1&1 angebotenen De-Mail-Dienste sind geeignete und erforderliche technische und organisatorische Maßnahmen implementiert und umgesetzt worden. Sämt-

liche 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 1&1 gewährleistet.

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

Sämtliche Mitarbeiter der 1&1 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 1&1 abgedeckt.

3.3 Rechte der Betroffenen

Die Anforderungen des De-Mail-Kriterienkatalogs zu den Betroffenenrechten werden von der 1&1 ebenfalls erfüllt. Sämtliche Dokumentationen und Prozesse im Umgang mit Betroffenenrechten der 1&1 wurden einer Begutachtung unterzogen.

Die sich aus dem De-Mail-Gesetz, der Datenschutz-Grundverordnung und 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, Richtlinien sowie Konzepte 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 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 1&1 erfüllt.

Das von der 1&1 De-Mail GmbH für den De-Mail-Service vorgesehene Datenschutzmanagementsystem ermöglicht die Umsetzung eines gesetzeskonformen Datenschutzmanagements, mit dem die Erfüllung der datenschutzrechtlichen Vorgaben im Wirkbetrieb sichergestellt wird.

Das Datenschutzmanagementsystem ist als dauerhafter Datenschutzprozess angelegt (sogenannter Plan-Do-Check-Act-Zyklus), um bei geänderten Umfeldbedingungen die Einhaltung des Datenschutzrechts kontinuierlich sicherstellen zu können.

Es sind Verfahren zum Management von IT-Sicherheitsvorfällen, Management der Lebenszyklen von IT-Verfahren unter Datenschutzgesichtspunkten, Management von Änderungen im Datenschutzrecht, zum Technologie-Monitoring und zum Monitoring und Management von Änderungen in den IT-Grundschutz-Katalogen vorhanden.

Die Verantwortlichkeiten im Bereich Datenschutz sind bei der 1&1 De-Mail GmbH klar geregelt. Ein betrieblicher Datenschutzbeauftragter ist gemäß den gesetzlichen Anforderungen bestellt. Er kann seine Aufgaben gesetzeskonform ausführen und erhält die erforderliche Unterstützung von den Fachabteilungen. Er wird frühzeitig in Sachverhalte eingebunden, die datenschutzrechtliche Themen tangieren (können). De-Mail-Nutzer und andere Interessenten können sich direkt an den Datenschutzbeauftragten wenden.

Die 1&1 De-Mail GmbH verfügt über ein den Anforderungen entsprechendes Datenschutzkonzept, Datenschutzmanagementkonzept und weitere erforderliche Dokumentationen wie z.B. Verfahrensbeschreibungen, Anforderungskonzepte, Verzeichnis von Verarbeitungstätigkeiten etc. Die Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit werden gemäß einer Schutzbedarfsfeststellung ergriffen.

Die Mitarbeiter der 1&1 und die Mitarbeiter der eingesetzten Dienstleister werden auf Wahrung der Vertraulichkeit und auf das Fernmeldegeheimnis verpflichtet und umfassend und regelmäßig zu Datenschutz und zur Datensicherheit geschult bzw. sensibilisiert.

Die 1&1 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.

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 1&1 überprüft wird.