KURZGUTACHTEN

ZUM

DE-MAIL DATENSCHUTZ-NACHWEIS

Version:	5.0
Prüfgegenstand:	Datenschutzkonzept und dessen Umsetzung für den De-Mail-Dienst der 1 & 1 De-Mail GmbH
Verantwortliche Stelle:	1 & 1 De-Mail GmbH Elgendorfer Str. 57 56410 Montabaur
Prüforganisation:	TÜV Informationstechnik GmbH TÜV NORD GROUP Langemarckstraße 20 45141 Essen http://www.tuvit.de
Verfasser/Gutachter:	Monika Wojtowicz, Ulrich Heitkötter, Dr. Manuel Cebulla
Datum:	03.03.2016

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

Im Rahmen der Akkreditierung der 1 & 1 De-Mail GmbH als De-Mail-Diensteanbieter ist das Datenschutzkonzept und dessen Umsetzung durch eine sachverständige Prüfstelle für Datenschutz zu begutachten.

De-Mail-Diensteanbieter müssen nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz die Erfüllung der datenschutzrechtlichen Anforderungen an das Datenschutzkonzept für die eingesetzten Verfahren und die eingesetzten informationstechnischen Einrichtungen nachweisen. Der Nachweis wird durch ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) geführt, welches ausgestellt wird, wenn die datenschutzrechtlichen Kriterien erfüllt sind, die vom BfDI im Kriterienkatalog für den Datenschutz-Nachweis (De-Mail-Kriterienkatalog) niedergelegt worden sind.

Der Begutachtung durch die Prüfstelle für Datenschutz der TÜV Informationstechnik GmbH wurde der De-Mail-Kriterienkatalog in der Version 1.2 zugrunde gelegt. Das Zertifikat durch den BfDI ist am 28.2.2013 erteilt worden.

Das Zertifikat des BfDI ist am 15.7.2013 um einen weiteren Dienst zur Durchführung der Erstidentifizierung der De-Mail-Nutzer, am 23.08.2013 um das auf Geschäftskunden (juristische Personen, Personengesellschaften und Behörden) ausgeweitete Angebot und am 16.04.2014 um einen weiteren Dienst zur Durchführung der Erstidentifizierung der De-Mail-Nutzer erweitert worden. Der für die letztgenannte Zertifikatserweiterung durchgeführten Begutachtung wurde der De-Mail-Kriterienkatalog in der Version 1.3 zugrunde gelegt.

Gemäß § 17 Abs. 3 De-Mail-Gesetz ist die Akkreditierung spätestens nach drei Jahren zu erneuern. Daher hat die Prüfstelle für Datenschutz der TÜV Informationstechnik GmbH den De-Mail-Dienst nach dem De-Mail-Kriterienkatalog in der Version 1.5 begutachtet. Daraufhin hat die BfDI im Rahmen der 1. Regel-Re-Zertifizierung am 11.02.2016 das Datenschutzzertifikat erneut erteilt.

Der De-Mail-Kriterienkatalog schreibt die Betrachtung aller Dienste und Funktionalitäten vor. Die Begutachtung beinhaltet technische und rechtliche Aspekte, die im Wesentlichen nach vier Kriteriengruppen geprüft werden:

- rechtliche Zulässigkeit unter Angabe der rechtlichen Erlaubnistatbestände;
- dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen einschließlich Verschlüsselung, Authentifizierung und Signaturen sowie Anforderungen an die Datensparsamkeit;
- Rechte der Betroffenen;
- Datenschutzmanagement.

Die vorgenannten Kriteriengruppen wurden im Einzelnen behandelt in den ausführlichen Gutachten der Prüfstelle für die Erstzertifizierung, in den drei oben genannten Ergänzungsgutachten und in den Gutachten für die Re-Zertifizierung.

Neben der Begutachtung der vom De-Mail-Gesetz geforderten Dienste und Funktionalitäten sieht der De-Mail-Kriterienkatalog auch die Begutachtung der optionalen Dienste *Dokumentenablage* und *Identitätsbestätigungsdienst* vor. Diese Dienste werden von der 1 & 1 De-Mail GmbH nicht angeboten und wurden somit auch nicht begutachtet.

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 über die De-Mail-Dienste verarbeiteten personenbezogenen Daten.

Neben der Einhaltung der gesetzlichen Regelungen des De-Mail-Gesetzes müssen insbesondere auch die einschlägigen Normen des Telekommunikationsgesetztes, des Telemediengesetzes und die Einhaltung anderer auf die einzelnen Dienste und Funktionalitäten anwendbarer Datenschutzbestimmungen sowie des Bundesdatenschutzgesetzes begutachtet werden.

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 zu begutachten sind. Dieser bezieht sich auf die oben genannten gesetzlichen Anforderungen und darüber hinaus auf den Baustein 1.5 der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der vollumfänglich in die Begutachtung einbezogen worden ist, sowie auf einzelne Anforderungen aus der Technischen Richtlinie De-Mail (BSI TR-01201 De-Mail).[1]

Gegenstand der Begutachtung durch die Prüfstelle für Datenschutz der TÜV Informationstechnik GmbH waren das Datenschutzkonzept der 1 & 1 De-Mail GmbH und die darin referenzierten zahl- und umfangreichen Dokumente, die zur Begutachtung vorgelegt worden sind. In Vor-Ort-Terminen wurden Aspekte aus dem Kriterienkatalog geprüft, indem sie in Augenschein genommen wurden und Gespräche mit Verantwortlichen bzw. Interviews mit Mitarbeitern geführt wurden. Zusatzinformationen wurden zudem per elektronischer Post oder in Form von Telefonkonferenzen bei verantwortlichen Mitarbeiterinnen und Mitarbeitern eingeholt.

Die Erstbegutachtung fand zwischen Oktober 2012 und Februar 2013 statt. Die Ergänzungsbegutachtungen wurden im Mai bis Juli 2013 bzw. im Juli bis August 2013 bzw. Feb-

[1] Neben der Begutachtung für den Datenschutz-Nachweis ist für die Akkreditierung der 1 & 1 De-Mail GmbH als De-Mail-Diensteanbieter von De-Mail-Auditoren der TÜV Informationstechnik GmbH testiert worden, dass der Diensteanbieter die in der Technischen Richtlinie festgelegten umfangreichen Anforderungen an die Informationssicherheit, an die Funktionalität und an die Interoperabilität erfüllt.

ruar bis April 2014 durchgeführt. Die Begutachtung für die Re-Zertifizierung erfolgte zwischen Oktober 2015 und Januar 2016.

3 Zusammenfassung der Prüfergebnisse

Die Prüfstelle für Datenschutz der TÜV Informationstechnik GmbH hat dem bzw. der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit[2] empfohlen, das Zertifikat zu erteilen und um die in der Folge begutachteten Ergänzungen zu erweitern sowie das Datenschutz-Zertifikat im Rahmen der Re-Zertifizierung weiterhin zu erteilen, da alle Anforderungen aus dem De-Mail-Kriterienkatalog durch die 1 & 1 De-Mail GmbH erfüllt werden.

3.1 Rechtliche Zulässigkeit

Die Anforderungen des De-Mail-Kriterienkatalogs aus der Kriteriengruppe *Rechtliche Zulässigkeit* werden von der 1 & 1 De-Mail-GmbH erfüllt. Dies betrifft die allgemeinen datenschutzrechtlichen Anforderungen 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 Verarbeitung personenbezogener Daten (Speichern, Verändern, Übermitteln, Sperren und Löschen) liegt eine gesetzliche Ermächtigung oder Einwilligung der Betroffenen vor. Es werden nur erforderliche Daten im Rahmen ihrer Zweckbestimmung erhoben und verwendet und nach Wegfall der Erforderlichkeit werden sie gelöscht. Somit wird auch dem Erfordernis der Datensparsamkeit Genüge getan. Die 1 & 1 De-Mail GmbH setzt andere Unternehmen als Auftragnehmer ein. Die gesetzlichen Vorschriften an die Datenverarbeitung im Auftrag werden eingehalten. Das Fernmeldegeheimnis wird gewahrt.

Die 1 & 1 De-Mail GmbH kommt ihren Aufklärungs- und Informationspflichten 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 De-Mail-fremde Datenverarbeitungen abhängig gemacht. Die erhobenen Daten der Nutzer werden nicht für Adresshandel oder Werbung verwendet.

Auf Wunsch können die Nutzer (Privatkunden) pseudonyme De-Mail-Adressen benutzen.

[2] Seit Januar 2014 ist es die Bundesbeauftragte für Datenschutz und Informationsfreiheit.

Die Vertraulichkeit, Integrität und Authentizität der Nachrichten werden durch Transportverschlüsselung und Inhaltsverschlüsselung gewährleistet. Eine Ende-zu-Ende-Verschlüsselung der Nachrichten, welche vom Nutzer eingerichtet werden kann, wird vom System unterstützt.

Der Sender kann bestimmen, dass sich der Empfänger für den Abruf der Nachricht an seinem De-Mail-Konto sicher anmeldet. Der Nutzer kann sich die sichere Anmeldung bestätigen lassen. Die Bestätigung erfolgt mit einer qualifizierten Signatur. Die Versandbestätigung und die Eingangsbestätigung werden durch den akkreditierten De-Mail-Diensteanbieter des Senders mit einer qualifizierten elektronischen Signatur versehen. Die gesetzlichen Anforderungen an die Löschungsfristen und an die Zugriffs- bzw. Weitergabekontrolle werden hinsichtlich der Versandbestätigung und der Eingangsbestätigung erfüllt. Berechtigten öffentlichen Stellen kann für von ihnen versendete De-Mails eine mit einer qualifizierten Signatur versehene Abholbestätigung zur Verfügung gestellt werden.

Die De-Mail-Nutzer 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. Die internen Prozesse der 1 & 1 De-Mail GmbH gewährleisten zudem, dass eine Löschung auch dann erfolgt, wenn die Daten auf Grund falscher Angaben ausgestellt wurden oder die zuständige Behörde die Löschung aus dem Verzeichnisdienst anordnet.

3.2 Dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen

Die Anforderungen des De-Mail-Kriterienkatalogs aus der Kriteriengruppe *Dienstespezifische Umsetzung der technisch-organisatorischen Anforderungen* werden von der 1 & 1 De-Mail-GmbH erfüllt. Dies hat die eingehende Begutachtung ergeben.

Für jeden von der 1 & 1 De-Mail GmbH angebotenen De-Mail-Dienst sind geeignete, erforderliche und angemessene technische und organisatorische Maßnahmen implementiert worden zur Erfüllung der Anforderungen nach der Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes (Zutritts-, Zugangs-, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren) sowie für die Authentifizierung und für die zum Einsatz kommenden elektronischen Signaturen. Darüber hinaus werden das Gebot der Datensparsamkeit (§ 3a Satz 1 BDSG) und die Möglichkeit der pseu-

donymen Nutzung (§ 3a Satz 2 BDSG) umgesetzt. Die besonderen, sich aus anderen Gesetzen ergebenden Anforderungen an Datensicherheit, Datenvermeidung und Datensparsamkeit werden ebenfalls erfüllt.

Die Art und Qualität der zum Einsatz kommenden Verschlüsselung entsprechen den gesetzlichen Anforderungen und dem Stand der Technik. Dies gilt für die Datenspeicherung bei der 1 & 1 De-Mail GmbH und ihren Auftragnehmern und für den Transport der De-Mails zwischen den Diensteanbietern.

Die 1 & 1 De-Mail GmbH ermöglicht, dass die Benutzer über die dienstseitig eingesetzte Transportverschlüsselung hinaus eine von ihnen selbst gewählte Ende-zu-Ende-Verschlüsselung einsetzen können. Zudem stellt die 1 & 1 De-Mail GmbH den Nutzern ein Browser-Plugin für eine PGP-Verschlüsselung zur Verfügung.

Die 1 & 1 De-Mail GmbH hat über die gesetzlichen Verpflichtungen hinaus weitere technische Maßnahmen implementiert, um das Niveau von Datenschutz und Datensicherheit weiter zu steigern (datenschutzfördernde Gestaltung): Verschlüsselung auf Dateisystemebene des Betriebssystems, verschlüsselte Kommunikation auf Transportebene auch bei interner Kommunikation, Verschlüsselung der Kommunikationsverbindung zwischen den Rechenzentren, Verschlüsselung auf Datenbankebene. Es kann keine Vermischung mit Datenbeständen aus anderen Angeboten der 1 & 1 stattfinden.

3.3 Rechte der Betroffenen

Die Anforderungen des De-Mail-Kriterienkatalogs aus der Kriteriengruppe *Rechte der Betroffenen* werden von der 1 & 1 De-Mail-GmbH erfüllt. Die Dokumente und Verfahren der 1 & 1 De-Mail GmbH wurden begutachtet.

Die sich aus De-Mail-Gesetz, Telekommunikationsgesetz, Telemediengesetz und Bundesdatenschutzgesetz ergebenden Rechte der Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten (Recht auf Benachrichtigung und Auskunft, Löschung und Sperrung, Berichtigung, Widerspruch gegen die Verarbeitung, Rücknahme einer Einwilligung) werden durch geeignete organisatorische Verfahren gewährleistet.

Die De-Mail-Nutzer können Änderungen und Löschungen ihrer personenbezogenen Daten über Einstellungen in ihrem De-Mail-Konto selbst vornehmen. Der Kundenservice hat – was aus Gründen des Datenschutzes sinnvoll ist – nur beschränkte Möglichkeiten, auf Kundendaten zuzugreifen, sondern leistet im Wesentlichen nur Hilfe zur Selbsthilfe.

Zum Zwecke der Aufklärung der Nutzer stellt die 1 & 1 De-Mail GmbH detailliertes und verständliches Informationsmaterial zur Verfügung.

3.4 Datenschutzmanagement

Die Anforderungen des De-Mail-Kriterienkatalogs aus der Kriteriengruppe *Datenschutzmanagement* werden von der 1 & 1 De-Mail-GmbH erfüllt.

Die betriebliche Organisation zur Gewährleistung der rechtlichen und technischen Vorschriften für den Datenschutz hinsichtlich der von der 1 & 1 De-Mail GmbH angebotenen De-Mail-Dienste wurde auf der Grundlage des IT-Grundschutz-Bausteins B 1.5 Datenschutz eingehend begutachtet. Die Begutachtung hat insbesondere Folgendes ergeben:

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 eingerichtet 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.

Die Verantwortlichkeiten im Bereich Datenschutz sind bei der 1 & 1 De-Mail GmbH klar geregelt. Ein betrieblicher Datenschutzbeauftragter ist gemäß den gesetzlichen Anforderungen des Bundesdatenschutzgesetzes bestellt. Er kann seine Aufgaben gesetzeskonform ausführen und erhält die erforderliche Unterstützung. 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 Datenschutzbeauftragten wenden.

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

Die Mitarbeiter der 1 & 1 De-Mail GmbH und die Mitarbeiter der von dieser eingesetzten Dienstleister werden auf das Datengeheimnis und auf das Fernmeldegeheimnis verpflichtet und umfassend und regelmäßig zu Datenschutz und Datensicherheit geschult bzw. sensibilisiert.