Vertrauensdienstrichtlinie für 1&1 EU-Mail

Dokumentenname und Identifizierung

Name:	Vertrauensdienstrichtlinie für 1&1 EU-Mail (1&1 EU-Mail TSPS)
Version:	2.5
Datum:	18.04.2023

Inhaltsverzeichnis

1 Einleitung

Bei dem vorliegenden Dokument handelt es sich um die Vertrauensdienstrichtlinie (engl. Trust Service Practice Statement, kurz TSPS) der Vertrauensdiensteanbieterin (engl. Trust Service Provider, kurz TSP) 1&1 De-Mail GmbH, für deren Vertrauensdienst 1&1 EU-Mail zur Zustellung elektronischer Einschreiben gemäß Artikel 3 Nr. 16 der VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung).

Im Folgenden wird es als die 1&1 EU-Mail TSPS bezeichnet.

Die 1&1 EU-Mail TSPS findet ausschließlich Anwendung für die Zustellung elektronischer Einschreiben (Postfach und Versanddienst für natürliche und juristische Personen) im Rahmen des Vertrauensdiensts 1&1 EU-Mail.

1.1 Überblick

Der 1&1-Konzern - mit seinen Marken GMX, WEB.DE und 1&1 - hat ein Kommunikationssystem aufgebaut, welches nach dem De-Mail Standard zertifiziert und akkreditiert wurde. De-Mail ist ein, auf dem De-Mail-Gesetz basierender, Standard für elektronische, rechtssichere Kommunikation in Deutschland. Der De-Mail-Dienst des 1&1 Konzerns wird von der 1&1 De-Mail GmbH erbracht.

Das System bildet mit einer auf E-Mail basierenden Technik verschiedene Versandoptionen wie Einschreiben, Absender-Bestätigt und Zugangsbestätigte Nachrichten verschlüsselt ab. Darüber hinaus sind alle Teilnehmer eindeutig identifiziert.

Die 1&1 De-Mail GmbH ist seit 2013 nach dem De-Mail-Gesetz akkreditiert und hat zu diesem Zeitpunkt den Betrieb als De-Mail-Diensteanbieter aufgenommen. Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen von De-Mail zeichnet sich der 1&1 De-Mail Diensteanbieter durch einen sehr hohen Sicherheitsstandard aus. Die Vertrauenswürdigkeit des für den Betrieb des De-Mail-Dienstes eingesetzten Personals ist durch öffentliche Stellen überprüft worden. Sowohl die bauliche als auch die organisatorische Infrastruktur erfüllen die strengen Anforderungen des De-Mail-Gesetzes und der Norm ISO/IEC 27001.

Die 1&1 De-Mail GmbH hat diese Infrastruktur zusätzlich nach der eIDAS-Verordnung und dem Vertrauensdienstegesetz zertifizieren lassen, um Ihren Kunden einen qualifizierten europäischen Zustelldienst anbieten zu können. Bei dem durch 1&1 erbrachten qualifizierten Vertrauensdienst 1&1 EU-Mail handelt es sich um einen IT-Service, der für die Zustellung elektronischer Einschreiben zuständig ist und ein europaweit einheitliches Sicherheitsniveau besitzt. Neben der verpflichtenden Identifizierung des Absenders und Empfängers ist die Zustellung des elektronischen Einschreibens garantiert. Der Dienst wird derzeit nur in Deutschland angeboten.

Der Vertrauensdienst 1&1 EU-Mail wird durch die 1&1 De-Mail GmbH betrieben. Der Vertrauensdienst 1&1 EU-Mail ist seit dem 28.06.2016 nach der Verordnung (EU) Nr. 910/2014 (eIDAS) für die Zustellung elektronischer Einschreiben zertifiziert. Dieser Dienst betrifft die Marken WEB.DE EU-Mail, GMX EU-Mail und 1&1 EU-Mail mit den registrierten E-Mail Domains web.de-mail.de, gmx.de-mail.de, 1und1.de-mail.de sowie sec.de-mail.de, wobei die Marken WEB.DE EU-Mail und GMX EU-Mail ausschließlich für natürliche und die Marke 1&1 EU-Mail für juristische Personen angeboten werden.

Die 1&1 EU-Mail TSPS beschreibt die betrieblichen Abläufe und Sicherheitsmaßnahmen des Vertrauensdienstes 1&1 EU-Mail in der Rolle als qualifizierte Dienste für die Zustellung elektronischer Einschreiben (engl. qualified electronic registered delivery services, kurz QERDS). Das vorliegende Dokument dient als Ergänzung der Allgemeinen Geschäftsbedingungen (AGB) für die Nutzung des De-Mail-Kontos der 1&1 De-Mail GmbH.

Im Einzelnen enthält das 1&1 EU-Mail TSPS u.a. die folgenden Aspekte:

- Nutzerkonten und -Adressen

- Identitätsprüfung
- Postfach- und Versanddienst
- Sperrung

1.2 Übertragung von Aufgaben an Dritte

Auf der Grundlage und Maßgabe einer vertraglichen Vereinbarung erfolgt die Übertragung von Aufgaben an Dritte. Die 1&1 De-Mail GmbH hat bei der Vertragsgestaltung gewährleistet, dass die aus der jeweiligen Aufgabenübertragung resultierenden gesetzlichen Anforderungen und die Regelungen der Vertrauensrichtlinie eingehalten werden. Die Verträge mit den Dritten enthalten zudem die Verpflichtung zur Mitwirkung im Falle von internen und externen Audits, sowie dem Einräumen von Kontrollbesuchen der zuständigen Aufsichtsbehörde. Die Aufgaben und Pflichten der Dritten werden in den jeweiligen Verträgen festgelegt.

Dritte verpflichten sich, für den Vertrauensdiensteanbieter 1&1 De-Mail GmbH ausschließlich zuverlässige und ausreichend geschulte, fachkundige Mitarbeiter einzusetzen. Die 1&1 De-Mail GmbH hat das Recht, die beim Dritten vorhandenen Dokumente zur Zuverlässigkeit und Fachkunde des eingesetzten Personals einzusehen. Sie hat die Möglichkeit unzuverlässige Mitarbeiter des beauftragten Dritten aus dem Prozess auszuschließen.

Die 1&1 De-Mail GmbH hat in den folgenden Bereichen Aufgaben an Dritte übertragen:

- **Identdienstleister (IDnow GmbH):** Anbieter der eIDAS konformen Identitätsfeststellung natürlicher Personen. Berechtigt zur Identitätsfeststellung natürlicher Personen für Vertrauensdiensteanbieter (VDA) durch Konformitätsbestätigung nach eIDAS.
- **Rechenzentrumsbetrieb (IONOS SE)**: Hosting und Internet-Konnektivität werden von der IONOS SE erbracht. Der Hostinganbieter ist zur Aufrechterhaltung seiner Zertifizierung nach ISO/IEC 27001 verpflichtet.
- **mTAN-Versender (Deutsche Telekom Security GmbH, kurz TeleSec):** TeleSec ist eine eingetragene Marke des Konzerns Deutsche Telekom. Anbieter von sogenannten Einmalpasswörtern.
- **eID-Servicebetreiber (Governikus GmbH & Co. KG):** Governikus stellt Server- und Client-Komponenten zur Verfügung, um Authentisierungen mittels elektronischer Identitäten sicherzustellen.
- **Support** (soweit externe Dienstleister beauftragt wurden)

Die Gesamtverantwortung für den Betrieb des Vertrauensdienstes 1&1 EU-Mail verbleibt auch bei der Übertragung von Aufgaben an Dritte in der Hand der 1&1 De-Mail GmbH. Alle Unternehmen wurden zur Einhaltung der rechtlichen Anforderungen verpflichtet. Die Umsetzung der Maßnahmen wird von der 1&1 De-Mail GmbH in regelmäßigen Abständen überprüft.

1.3 Teilnehmer

Dieses Kapitel beschreibt die Identitäten oder Arten von Instanzen, die im Rahmen des Vertrauensdienstes die Rolle der Teilnehmer übernehmen.

- **Zertifizierungsstellen:** (Telesec) Austeller von Zertifikaten im qualifizierten Bereich, betreibt komplexe Public Key Infrastrukturen im fortgeschrittenen Bereich, die die Integrität vertrauenswürdiger Kommunikation schützen und sicherstellen.

  Das Trust Center der Deutschen Telekom AG ist seit dem 1.7.2016 konform zu der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste

(eIDAS). Im Bereich nicht qualifizierter Zertifikate wird die Sicherheit und Leistungsfähigkeit durch die ETSI-Zertifizierung bestätigt.

- **Zulassungsstellen**: Identifizierungen und Authentifizierungen der Vertragspartner werden von der 1&1 De-Mail GmbH geprüft.
- **Vertragspartner:** Alle Kunden des VDAs. Dies können natürliche oder juristische Personen sein.
- **Vertrauende Dritte (Relying Party)**: Können sowohl aktive und inaktive Vertragspartner sein, wie auch eine natürliche oder juristische Person, die sich auf die Vertrauenswürdigkeit der von der 1&1 De-Mail GmbH angebotenen Zustellung elektronischer Einschreiben verlassen.

1.4 Organisation zur Verwaltung dieses Dokuments

Diese TSPS wurde von 1&1 De-Mail GmbH herausgegeben.

Adresse:

1&1 De-Mail GmbH

Brauerstraße 48

76135 Karlsruhe

Telefon:

- GMX: (+49) 0721 960 9992
- WEB.DE: (+49) 0721 960 9800
- 1&1: (+49) 0721 960 9785

E-Mail Adressen:

- GMX: de-mail-kundenservice@gmxnet.de
- WEB.DE: de-mail-kundenservice@web.de
- 1&1: de-mail-kundenservice@1und1.de

WWW:

- GMX: https://www.gmx.net/produkte/de-mail/#.hp.int.footer
- WEB.DE: https://produkte.web.de/de-mail/#.hp.int.footer
- 1&1: https://de-mail-register.1und1.de/1und1-De-Mail

1.5 Definition und Abkürzungen / Akronyme

Dieses Dokument verwendet die folgenden definierten Begriffe:

AGB	Allgemeine Geschäftsbedingungen
BSI	Bundesamtes für Sicherheit in der Informationstechnik
DMDA	De-Mail-Diensteanbieter
eIDAS-VO	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

ISMS	Informationssicherheitsmanagementsystem
QERDS	qualified electronic registered delivery services
SIEM-System	Security Information and Event Management System
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
VDA	Vertrauensdiensteanbieter

2 Veröffentlichung und Verantwortlichkeiten

2.1 Veröffentlichung von Informationen

Der Vertrauensdiensteanbieter 1&1 De-Mail GmbH publiziert Informationen zu dem Wichtigsten der eIDAS-Verordnung (u.a. Was ist ein Vertrauensdienst oder Was ist ein qualifizierter Vertrauensdienst) über die jeweiligen markenspezifischen Webseiten wie folgt:

- GMX: https://www.gmx.net/produkte/eIDAS
- WEB.DE: https://produkte.web.de/eIDAS/
- 1&1: https://hilfe-center.1und1.de/e-mail-c82645/de-mail-c85617/eidas-infoseite-a797697.html

2.2 Update der Informationen / Veröffentlichungsfrequenz

Neu ausgestellte Richtlinien und ggf. weitere Informationen werden zeitnah zur Verfügung gestellt. Es gelten die nachfolgenden Veröffentlichungsfrequenzen:

- Richtlinien werden nach Bedarf aktualisiert

2.3 Zugang zu den Informationen

Der lesende Zugriff auf alle in Kapitel 2.1 aufgeführten Informationen unterliegt keiner Zugangskontrolle. Der schreibende Zugriff auf diese Informationen erfolgt ausschließlich durch berechtigte Mitarbeiter.

3 Betriebliche Anforderungen im Lebenszyklus für die Zustellung elektronischer Einschreiben

3.1 Zustellung elektronischer Einschreiben – Merkmale und Funktionen

Im nachfolgenden werden die betrieblichen Anforderungen für die Zustellung elektronischer Einschreiben, auf Basis des De-Mail-Dienstes beschrieben.

3.1.1 Allgemeines

Die 1&1 De-Mail GmbH ermöglicht ihren Kunden die Nutzung von De-Mail-Diensten gemäß De-Mail-Gesetz vom 28. April 2011.

Die Übertragung und Speicherung von De-Mails erfolgt dabei in einem geschlossenen Nutzerraum, der nur registrierten De-Mail-Nutzern zugänglich ist. Ein Versand von De-Mails an E-Mail-Adressen ist ebenso wenig möglich wie der Empfang von E-Mails in De-Mail-Postfächern.

3.1.2 Voraussetzungen

Technische Voraussetzung für die Nutzung der von 1&1 De-Mail GmbH angebotenen De-Mail-Dienste ist ein Zugang zum Internet, die Verfügbarkeit eines aktuellen Internet-Browsers auf einem geeigneten Endgerät sowie ein ausschließlich vom Nutzer verwendetes Mobiltelefon. Diese Leistungen sind nicht Bestandteil des Vertrages mit der 1&1 De-Mail GmbH.

3.1.3 Identitätsprüfung

Es ist notwendig, dass jeder Nutzer (Absender und Empfänger) einmalig eindeutig identifiziert wird, um die Authentizität der Kommunikation bei De-Mail zu gewährleisten. Auf diese Weise ist jedes Konto einer Person eindeutig zuordenbar.

Die Erstidentifizierung kann über zwei Wege erfolgen:

- Persönliche Prüfung der bei Registrierung angegebenen Daten des Nutzers durch einen zertifizierten Identdienstleister, indem diese Daten mit einem gültigen amtlichen Ausweis, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, verglichen werden,
- anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes.

Die für den Versand von De-Mails mit der Versandoption absenderbestätigt benötigte sichere Anmeldung stellt die Authentifizierung des Absenders auf hohem Niveau sicher.

Die für den Empfang von De-Mails mit der Versandoption persönlich benötigte sichere Anmeldung stellt die Authentifizierung des Empfängers auf hohem Niveau sicher. Erstidentifizierung und Authentifizierung erfolgen in jedem Fall vor dem Abruf der Daten.

Die sichere Anmeldung zu einem De-Mail-Postfach erfordert zwingend eine Anmeldung mit zwei unterschiedlichen Sicherungsmitteln, das bedeutet, dass neben dem Benutzernamen und Passwort noch ein weiteres Sicherungsmittel (Token) oder ein elektronischer Identitätsnachweis nach § 18 Personalausweisgesetz zur Authentisierung benötigt wird.

Nutzer können mit 1&1 De-Mail vereinbaren, dass Ihnen neben dieser sicheren Anmeldung auch eine Anmeldung unter Verwendung nur eines Sicherungsmittels möglich sein soll („einfache Anmeldung“). Für die einfache Anmeldung an einem De-Mail-Postfach wird dann nur der Benutzernamen und das Passwort benötigt. Aufgrund des Verzichts auf ein weiteres unabhängiges Sicherungsmittel bietet die einfache Anmeldung jedoch nicht den gleichen Schutz wie die sichere Anmeldung, weshalb empfohlen wird, ausschließlich die sichere Anmeldung zu verwenden.

Bei einer einfachen Anmeldung stehen einige Funktionen des De-Mail-Postfachs nur begrenzt und andere überhaupt nicht zur Verfügung, z.B. Zugriff auf De-Mails, die eine sichere Anmeldung erfordern oder die Änderung von Identitätsdaten. Zur vollständigen Nutzung ist die sichere Anmeldung zwingend erforderlich.

Die Erstidentifizierung nach § 3 Abs. 3 S.1 Nr. 1 De-Mail-Gesetz erfüllt die Anforderungen nach Art. 24 Abs.1 eIDAS-VO und ist damit als geeignet auch für diesen qualifizierten Vertrauensdienst anzusehen.

Informationen zur Identifizierung für Privatkunden sind in den Leistungsbeschreibungen für den De-Mail-Account geregelt, die unter den folgenden markenspezifischen Webseiten verfügbar sind:

- GMX: https://img.web.de/v/demail/files/leistungsbeschreibung.html
- WEB.DE: https://img.web.de/v/demail/files/leistungsbeschreibung.html

Informationen zur Identifizierung für Geschäftskunden sind in der Leistungsbeschreibung für den De-Mail-Account geregelt, die unter der folgenden Webseite verfügbar ist:

- 1&1: https://dl.1und1.de/de-mail/1und1/De-Mail_Leistungsbeschreibung.pdf

Alle Identifizierungssysteme werden vor der Implementierung von der Konformitätsbewertungs-stelle geprüft.

3.1.4 Nutzerkonten und -Adressen

Für die Nutzung der von 1&1 De-Mail GmbH innerhalb des De-Mail-Dienstes angebotenen Nutzerkonten und -Adressen, muss der Nutzer einen nach De-Mail akkreditierten Registrierungs- und Identifizierungsprozess durchführen (vgl. Kapitel 3.1. Identitätsprüfung).

Informationen zur De-Mail Adresse für Privatkunden sind in den Leistungsbeschreibungen für den De-Mail-Account geregelt, die unter den folgenden markenspezifischen Webseiten verfügbar sind:

- GMX: https://img.web.de/v/demail/files/leistungsbeschreibung.html
- WEB.DE: https://img.web.de/v/demail/files/leistungsbeschreibung.html

Informationen zur Identifizierung für Geschäftskunden sind in der Leistungsbeschreibung für den De-Mail-Account geregelt, die unter der folgenden Webseite verfügbar ist:

- 1&1: https://dl.1und1.de/de-mail/1und1/De-Mail_Leistungsbeschreibung.pdf

3.1.5 Postfach- und Versanddienst

Der Postfach- und Versanddienst ist der zentrale Dienst des Vertrauens- und De-Mail-Diensteanbieters 1&1 De-Mail GmbH. Er gewährleistet zuverlässige und vertrauliche Kommunikation, d.h. eine Nachricht ist beim Versand gegen den Verlust der Vertraulichkeit, gegen Änderungen des Nachrichteninhaltes und der sog. Metadaten (z. B. Absenderadresse, Versandzeit, Versandoptionen) geschützt. Die Sicherung erfolgt durch eine qualifizierte Signatur der Versandbestätigung bzw. Eingangsbestätigung durch den De-Mail-Dienstanbieter (DMDA) und erfüllt die Anforderung nach Art. 44 Abs. 1 d) eIDAS-VO. Der Nachrichtenaustausch erfolgt MIME-konform (RFC 2045-2049).

Im De-Mail System werden übersandte Daten grundsätzlich nicht verändert. Die erstellten Hash-Codes, die auch signiert werden, enthalten nur solche Informationen, die beim Versand einer De-Mail unverändert bleiben. Dadurch bleiben die Hash-Codes unverändert und die entsprechenden Signaturen können von allen Beteiligten geprüft werden, so wie nach Art. 44 Abs. 1 e) eIDAS-VO gefordert.

Die geforderten Zeitstempel sind in der durch den DMDA ausgestellten Versandbestätigung bzw. Eingangsbestätigung enthalten. Die technischen und organisatorischen Anforderungen an qualifizierte Zeitstempel gemäß Artikel 42 der eIDAS-VO, werden durch die Anforderungen

aus der entsprechenden Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR-01201 (De-Mail) abgedeckt.

1&1 De-Mail unterstütz folgende Betriebsart:

- Versendung/Empfang ohne ausdrückliche Annahme (Store and Forward): Die Versendung bzw. der Empfang eines Nachrichteninhaltes erfolgt ohne ausdrückliche Annahme durch den Empfänger

1&1 De-Mail unterstützt folgende Betriebsart nicht:

- Versendung/Empfang erst nach Annahme (Store and Notify): Die Versendung bzw. der Empfang eines Nachrichteninhalts erfolgt erst nachdem der Empfänger dem Empfang einer Nachricht zuvor in Form einer Bestätigung einer Empfangsankündigung zugestimmt hat.

Weiterführende Informationen zum Postfach- und Versanddienst und den zusätzlichen Versandoptionen zum qualifizierten versenden einer De-Mail sind in den Leistungsbeschreibungen für den De-Mail-Account geregelt, die unter den folgenden markenspezifischen Webseiten verfügbar sind:

- GMX: https://img.web.de/v/demail/files/leistungsbeschreibung.html
- WEB.DE: https://img.web.de/v/demail/files/leistungsbeschreibung.html
- 1&1: https://dl.1und1.de/de-mail/1und1/De-Mail_Leistungsbeschreibung.pdf

3.1.6 Sperrung

Sollten die Zugangsdaten für die Anmeldung an einem De-Mail Account in falsche Hände geraten sein, so kann der Nutzer jederzeit sein Account bei der 1&1 De-Mail GmbH sperren lassen. Werden mehrfach falsche Authentifizierungsdaten verwendet, wird der betreffende De-Mail-Account automatisch gesperrt.

Sperrungen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Webseiten verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

4 Bauliche und organisatorische Maßnahmen

Die 1&1 De-Mail GmbH hat den gesetzlichen Anforderungen entsprechend bauliche und organisatorische Maßnahmen eingeführt. Die Infrastruktur des Vertrauensdienstes 1&1 EU-Mail ist in einem besonders geschützten Gebäude untergebracht und wird durch das fachkundige Personal der 1&1 De-Mail GmbH betrieben. Alle Arbeitsabläufe des qualifizierten Dienstes für die Zustellung elektronischer Einschreiben sind genau definiert.

4.1 Informationssicherheitsrichtlinien

Die Unternehmensleitung des 1&1 Konzerns hat eine Leitlinie zur Informationssicherheit sowie konkretisierende Richtlinien erlassen, welche die Mindestanforderungen an alle IT-Systeme und IT-gestützte Fachverfahren enthalten (Leitlinie und Richtlinien werden im Folgenden als Informationssicherheitsrichtlinien zusammengefasst), die von dem 1&1 Konzern, der ihr untergeordneten Unternehmensteile und der 1&1 De-Mail GmbH entwickelt und betrieben werden. Die Informationssicherheitsrichtlinien gelten für alle Mitarbeiter des 1&1 Konzerns, der ihr untergeordneten Unternehmensteile sowie von ihr beauftragten Dritten. Die Leitlinie ist schriftlich niedergelegt, von den Vorständen des 1&1 Konzerns akzeptiert, abgenommen und in Kraft gesetzt. Sie wurde den betroffenen Mitarbeitern der 1&1 De-Mail GmbH bekanntgegeben. Sie wird im Bereich der 1&1 De-Mail GmbH und für den angebotenen Vertrauensdienst 1&1 EU-Mail umgesetzt und aufrechterhalten. Die Gesamtverantwortung für die Einhaltung der in seiner Informationssicherheitsrichtlinien vorgeschriebenen Verfahren hat der 1&1 Konzern. Werden Teile der TSP-Funktionalität von Dritten (Outsourcen) erfüllt, werden die Mindestanforderungen an die Informationssicherheit durch regelmäßig Audits überprüft. Im Informationssicherheitsmanagementsystem (ISMS) der 1&1 De-Mail GmbH werden Regelungen beschrieben, die sicherstellen, dass das Sicherheitsniveau der 1&1 durch die Inanspruchnahme externer Dienstleistungen nicht beeinträchtigt wird. Die Anforderungen beginnend mit der Planung und Konzeption über den Betrieb bis hin zu dessen Beendigung wurden beschrieben, freigegeben und im Intranet veröffentlicht. Die Pflichten des Outsourcers und etwaige Haftungsansprüche sind darin ebenfalls geregelt und werden bei Vertragsabschluss bindend. Die Konformität von Dritten zur Informationssicherheitsleitlinie wird von 1&1 mithilfe von Audits und/oder durch die Zertifizierung der Vertragspartner nach ISO/IEC 27001 überprüft.

Die Informationssicherheitsleitlinie wird zusammen mit dem Inventar von Vermögenswerten in regelmäßigen Abständen, mindestens alle 2 Jahre, sowie bei wesentlichen Änderungen überprüft und ggf. aktualisiert. Änderungen bedürfen der Zustimmung der Unternehmensleitung des 1&1 Konzerns. Ebenfalls finden regelmäßige Überprüfungen auf Grundlage des Zertifizierungsprozesses statt.

Dritte, einschließlich Kunden, Vertrauende Dritte, Konformitätsbewertungsstellen sowie Aufsichtsbehörden werden über Änderungen der Informationssicherheitsleitlinie informiert, wenn und soweit dies erforderlich ist.

4.2 Bauliche Sicherheitsmaßnahmen

Die für den Betrieb des Vertrauensdiensteanbieters 1&1 De-Mail GmbH relevanten Systeme und alle sensiblen Daten sind in physisch geschützten Sicherheitsbereichen untergebracht. Durch Zutrittskontrollmechanismen wird sichergestellt, dass keine unberechtigten Personen Zugang zu den Sicherheitsbereichen haben. Alle Zutritte, auch unerlaubte Zutrittsversuche, werden protokolliert. Versuche zur Überwindung der Sicherheitsmechanismen wie Einbruch, Diebstahl und Vandalismus lösen einen Alarm aus. Es existieren Prozesse zur Erteilung, zur Veränderung und zum Entzug von Zutrittsberechtigungen. In regelmäßigen Abständen, mindestens einmal jährlich, findet eine stichprobenartige Überprüfung von Zutrittsberechtigungen statt, um das Risiko von Schäden an Vermögenswerten, Unterbrechung der Geschäftstätigkeit oder Diebstahl von Informationseinrichtungen auszuschließen. Die sicheren, hochverfügbaren und redundanten Rechenzentren werden von der IONOS SE betrieben und sind nach ISO/IEC 27001 zertifiziert und erfüllen somit den aktuellen Stand der Technik.

Um die Vertrauenswürdigkeit des Vertrauensdienstbetriebs sicherzustellen gibt es innerhalb der Rechenzentren einen zusätzlichen physikalischen Sicherheitsbereich für den Schutz der IT-Systeme des Vertrauensdienstes. Der Zutritt zu den Systemen und der Zugriff auf diese sind nur im Vier-Augen-Prinzip möglich. Diese Maßnahmen und die zusätzliche Videoüberwachung bieten einen zusätzlichen Schutz vor Manipulation und Diebstahl. Die Sicherheitsmaßnahmen und das zugrundeliegende Informationssicherheitsmanagementsystem (ISMS) werden regelmäßig durch eine anerkannte Prüf- und Bestätigungsstelle überprüft.

Die Errichtung und der Betrieb der Rechenzentren erfolgten unter Beachtung der entsprechenden Richtlinien TR-01201 (De-Mail) des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Beherrschung von Sicherheitsrisiken nach dem Stand der Technik wird hierbei durch die Zertifizierung entsprechend ISO/IEC 27001 nachgewiesen.

4.3 Verfahrensvorschriften

4.3.1 Rollenkonzept

Das im Informationssicherheitsmanagementsystem (ISMS) dokumentierte und umgesetzte Rollenkonzept sieht eine Aufteilung in operative, administrative und führende Rollen vor. Es genügt den Grundsätzen der Funktionstrennung und erlaubt nur den berechtigten Personen den Zugriff auf IT-Systeme und IT-gestützte Fachverfahren. Alle Mitarbeiter erhalten durch einen definierten Prozess die Rollen, die zum Ausüben der Tätigkeit notwendig sind. Ein Rollenausschlussprinzip garantiert, dass eine einzelne Person keine sicherheitsrelevanten Änderungen vornehmen kann. Der Entzug einer Rolle folgt ebenfalls einem definierten Prozess und wird dokumentiert. Dem Rollenkonzept liegen die folgenden Basisregeln und Rollenausschlüsse zugrunde:

- Leitende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Administrative Rollen dürfen keine operativen Aufgaben übernehmen

Der Zugriff der Administratoren wird entsprechend eines Rollenkonzeptes geregelt und umfasst jeweils den Verantwortungs- bzw. Kompetenzbereich der Rolle und der zugehörigen Gruppe von Administratoren.

Vertrauenswürdige Rollen, wie Sicherheitsmanager, Systemadministratoren, Identity Verification Officer und andere sind vollumfänglich etabliert und im ISMS dokumentiert. Die Rollen sind vom Management und dem Rolleninhaber akzeptiert und anerkannt.

4.3.2 Vier-Augen Prinzip

Sicherheitskritische Vorgänge (z.B. direkte Zugriff auf die Hardware) erfolgen grundsätzlich im Vier-Augen-Prinzip. Dies wird durch technische und organisatorische Maßnahmen sichergestellt.

4.3.3 Sonstige Arbeitsanweisung

Den Mitarbeitern der 1&1 De-Mail GmbH ist es nicht erlaubt, Unterlagen, Medien (mit der Ausnahme von Laptops) und Software, die sensible Daten enthalten, aus dem Sicherheitsbereich der 1&1 De-Mail GmbH zu entfernen.

4.4 Organisatorische Sicherheitsmaßnahmen

Die umgesetzten organisatorischen Maßnahmen basieren auf einer Risikoanalyse und gewähren einen sehr hohen Sicherheitsstandard des Vertrauensdienstes 1&1 EU-Mail. Diese Maßnahmen sind im dokumentierten Informationssicherheitsmanagementsystem (ISMS) niedergelegt, welches nicht öffentlich verfügbar ist. Das ISMS und die darin beschriebenen Maßnahmen werden regelmäßig und kontinuierlich von der 1&1 De-Mail GmbH überprüft. Die Beherrschung von Sicherheitsrisiken nach dem Stand der Technik wird hierbei durch die Zertifizierung entsprechend ISO/IEC 27001 nachgewiesen.

Die nachfolgende Aufzählung nennt einen Teil der organisatorischen Maßnahmen, aus unterschiedlichen Quellen, die zur Wahrung der Sicherheit getroffen wurden:

- Maßnahmen zur Ermittlung, Bewertung und regelmäßigen Überprüfung von Restrisiken sind im Informationssicherheitsmanagementsystem dokumentiert
- Die Bestimmungen zur Einbindung von externen Dienstleistern stammen aus Festlegungen des De-Mail-Gesetzes und sind in den Verträgen so umgesetzt, dass deren Umsetzung von Sicherheitsmaßnahmen jederzeit durch die 1&1 De-Mail GmbH oder von externen Auditoren überprüft werden kann.
- Alle Mitarbeiter des Rechenzentrums sind verpflichtet die strengen internen Datenschutz- und Sicherheitsrichtlinien der 1&1 De-Mail GmbH einzuhalten.
- Die Systeme des Rechenzentrums werden regelmäßig auf sicherheitsrelevante Veränderungen untersucht. Alle sicherheitsrelevanten Veränderungen müssen vor
- Inbetriebnahme durch das Managementboard für Informationssicherheit und
- Datenschutz der 1&1 De-Mail GmbH freigegeben werden. Aufsichtsstellen werden über alle Änderungen bei der Erbringung des qualifizierten Vertrauensdienstes und über eine beabsichtigte Einstellung dieser Tätigkeiten unterrichtet.
- Grundsätzlich wird auf die vollständige Einhaltung des Art. 24 (2a) eIDAS VO geachtet.
- Alle sicherheitsrelevanten Prozesse sind im Informationssicherheitsmanagement-system dokumentiert und geprüft.
- Die 1&1 De-Mail GmbH ist nach ISO/IEC 27001 zertifiziert und betreibt ein Risikomanagementsystem in Anlehnung an ISO/IEC 27005.

4.5 Personelle Maßnahmen

Die umgesetzten personellen Sicherheitsmaßnahmen gewährleisten einen sehr hohen Sicherheitsstandard des Vertrauensdienstes 1&1 EU-Mail. Die Zuverlässigkeit der Personen, die in den Rechenzentren der 1&1 De-Mail GmbH arbeiten, wird regelmäßig durch interne und externe Audits überprüft. Insbesondere werden die Mitarbeiter der 1&1 De-Mail GmbH klar den definierten Rollen im Vertrauensdienst zugewiesen, für Ihre Aufgaben ausreichend qualifiziert, mit den für Ihre Aufgaben erforderlichen Dokumentationen ausgestattet und auf ihre Zuverlässigkeit hin überprüft.

Im dokumentierten ISMS, das die 1&1 De-Mail GmbH errichtet und eingeführt hat, sind genaue Rollenbeschreibungen enthalten. Dort wird ebenfalls eine Rollentrennung bei kritischen

Prozessen definiert. Bei der täglichen Arbeit wird das Personal von genauen Arbeitsanweisungen unterstützt.

4.5.1 Qualifikation, Erfahrung und Zuverlässigkeit des Personals

Die 1&1 De-Mail GmbH stellt ausschließlich zuverlässiges, qualifiziertes Personal ein. Vor Aufnahme der Tätigkeit im sicherheitskritischen Bereich der 1&1 De-Mail GmbH wird die Fachkunde geprüft und eine initiale Schulung durchgeführt. Dies gilt auch für alle leitenden Rollen der 1&1 De-Mail GmbH. Schulungsmaßnahmen werden dokumentiert. Die 1&1 De-Mail GmbH stellt sicher, dass keine Interessenskonflikte bestehen. Mitarbeiter der 1&1 De-Mail GmbH haben bei Interessenskonflikten ein Tätigwerden abzulehnen. Ihnen drohen in diesem Fall keine arbeitsrechtlichen Konsequenzen.

4.5.2 Sicherheitsüberprüfung

Die 1&1 De-Mail GmbH stellt sicher, dass das für den Vertrauensdienst 1&1 EU-Mail eingesetzte Personal die für einen sicheren Betrieb notwendige Zuverlässigkeit besitzt. Jeder Mitarbeiter, der mit dem sicheren Betrieb betreut wird, muss bei Neueinstellung ein Führungszeugnis nach § 30 Abs. 1 und 5 des Bundeszentralregistergesetzes vorlegen. Die Sicherheitsüberprüfungen dieser Mitarbeiter werden alle 3 Jahre erneuert.

4.5.3 Schulungen und Weiterbildungen

Alle Mitarbeiter werden vor der Aufnahme Ihrer Tätigkeit und bei Bedarf geschult. Die Schulung beinhaltet u.a. eine Einarbeitung/Einweisung in die auszuübende Tätigkeit und eine

Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit sowie der datenschutzrechtlichen Rahmenbedingungen. Nachschulungen der Mitarbeiter finden regelmäßig, im Regelfall alle 2 Jahre statt. Nachschulungen werden zudem dann durchgeführt, wenn Änderungen an den Prozessen, der Technik sowie den Rahmenbedingungen für den Betrieb des Vertrauensdienstes erfolgen oder wenn diese zur Vermittlung oder Aufrechterhaltung der notwendigen Fachkunde eines Mitarbeiters erforderlich sind. Die Schulungsinhalte werden regelmäßig auf Ihre Aktualität überprüft.

Informationen zu aktuellen Gefährdungen,Bedrohungen, sowie zum Stand der Technik in der Informationssicherheit, werden fortlaufend vermittelt. Dies erfolgt bspw. im Rahmen des generellen Risiko-Managements, Vulnerability-Managements, sowie regelmäßig (monatl.) stattfindenter Veranstaltungen zur Informationssicherheit. Des Weiteren stehen den Mitarbeitenden vielfältige interne und externe Schulungsmöglichkeiten zur Verfügung.

4.5.4 Rollenbesetzung, Rollenentzug und Rollenwechsel

Rollenbesetzungen, Rollenentzug und Rollenwechsel erfolgen nach festgelegten internen Verfahren. Sie werden dokumentiert und die entsprechenden Protokolle von Berufendem und Berufenem unterzeichnet. Eine Berufung erfolgt erst, wenn die erforderliche Sicherheitsprüfung und die erforderlichen Schulungen durchgeführt worden sind.

Der Leiter DMDA (De-Mail-Diensteanbieter) wird von der 1&1 Unternehmensleitung berufen und abberufen. Sonstige Personen, die leitende oder kontrollierende Rollen übernehmen, z.B. der stellvertretende Leiter DMDA sowie der Sicherheitsbeauftragte des DMDAs, werden vom Leiter DMDA berufen und abberufen. Durch das umgesetzte Rollenkonzept und die Rollenausschlusskriterien wird gewährleistet, dass jede für die 1&1 De-Mail GmbH tätige Person nur die Zugänge und Zugriffsrechte erhält, die zum Ausüben ihrer Rolle notwendig sind. Die Berufung wird dokumentiert, die berufene Person erklärt ihr Einverständnis mit der Rolle durch Gegenzeichnen des entsprechenden Protokolls.

4.5.5 Anforderungen an externes Personal

Externes Personal, welches temporär im Sicherheitsbereich arbeitet, wird immer von berechtigten Mitarbeitern begleitet und beaufsichtigt. Für dauerhaft eingesetztes Personal von anderen Firmen gelten die gleichen Regelungen wir für internes Personal.

4.5.6 Sanktionen bei unerlaubten Handlungen

Die 1&1 De-Mail GmbH hat Maßnahmen implementiert (z.B. die Durchführung eines internen Revisionsverfahrens), um die Einhaltung der aufgestellten Regeln und Verfahren zum ordnungsgemäßen und sicheren Betrieb des Vertrauensdienstes 1&1 EU-Mail zu kontrollieren. Festgestellte Verstöße werden behoben. Unerlaubte Handlungen werden individuell nach geltenden betrieblichen und rechtlichen Vorschriften und Vereinbarungen geprüft und entsprechend geahndet.

4.6 Protokollereignisse

Sämtliche Änderungen an dem Informationsverbund werden im Rahmen des Change Managements dokumentiert. Folgende Ereignisse werden protokolliert:

- Zutritt zu Sicherheitsabschnitten im Rechenzentrum
- Zugriff auf IT Systeme
- Änderung von IT Verkabelung
- Änderungen der Netzwerktopologie
- Änderungen der Systemarchitektur
- Änderungen von Hardware und Software
- Protokollierungen von Ereignissen im Lebenszyklus von IT Systemen:
- Bestellung/Beschaffung
- Einbau
- Ausbau

- Provisionierung
- Installation
- Inbetriebnahme
- Außerbetriebnahme

Die Protokolle werden fortlaufend überwacht und ggf. geprüft, um potenzielle Schäden oder Fehlfunktionen frühzeitig erkennen zu können.

Alle Protokolle werden von der 1&1 EU-Mail zentralisiert und revisionssicher nach den gesetzlichen Bestimmungen für Aufbewahrung und Speicherfristen vorgehalten.

4.7 Sicherung und Aufzeichnungen

Als rechtliche Vorgaben für die elektronische Archivierung beim Betrieb einer Infrastruktur nach der eIDAS-Verordnung sind die Bestimmungen des De-Mail-Gesetzes und der Technischen Richtlinie BSI TR 01201 identifiziert worden. Die sicher archivierten Daten umfassen u.a. Daten der Identifikation bzw. Verifikation einer zu identifizierenden Person, dokumentationspflichtige Vorgangsdaten wie Änderungsvorgänge, Sende- und Empfangsvorgänge, sowie Protokolle und andere Betriebsdaten, die durch den Dienst entstehen. Der Aufbewahrungszeitraum von archivierten Daten beträgt 10 bzw. 30 Jahre nach Vertragsbeendigung, gem. Technischen Richtlinien. Die elektronischen Archivdaten werden ausschließlich verschlüsselt vorgehalten. Papiergebundene Ident-Formulare werden in einem zutritts- und zugriffsgesicherten Raum archiviert.

4.8 Wiederherstellung des Betriebes im Katastrophenfall

Es existiert ein übergreifendes Notfall-Handbuch sowie Notallpläne pro Komponente. Außerdem besteht ein systemübergreifendes Datensicherungskonzept. Zur Sicherstellung der Wiederherstellbarkeit bei Störungen werden anfallende Daten aus der Datenbank und aus dem Dateisystem sowie die Konfigurationsdaten der IT Systeme dediziert gesichert.

Für eine Wiederherstellung existiert ein genereller Wiederanlaufplan für das Gesamtsystem, für die einzelnen Systeme und Dienste ist dies zusätzlich im Detail beschrieben.

Sämtliche Störungen werden im Rahmen des Incident Managements (vgl. Kapitel 5.9) bearbeitet und analysiert. Dies umfasst auch eine Ursachenanalyse, um gleichartige, wiederkehrende Störungen zu vermeiden.

Grundsätzlich sind ausreichende finanzielle, technische und personelle Ressourcen vorhanden.

4.9 Einstellung des Betriebes

Die 1&1 De-Mail GmbH verfügt über einen fortlaufend aktualisierten Beendigungsplan für die Einstellung des De-Mail Betriebes, welcher nicht öffentlich verfügbar ist. Dort sind die Einzelheiten für den Fall der Einstellung des Betriebes niedergelegt. Der Beendigungsplan wird in regelmäßigen Abständen von der zuständigen Behörde überprüft und freigegeben.

Die 1&1 De-Mail GmbH benachrichtigt Kunden und Dritte, einschließlich Vertrauender Dritte und die zuständige Aufsichtsbehörde, rechtzeitig, soweit möglich jedoch mindestens drei Monate vorher, über die Einstellung ihrer Tätigkeit und der sich hieraus ergebenden Folgen.

Alle Verträge mit externen Dienstleistern und weiteren Dritten werden fristgerecht gekündigt. Soweit erforderlich, werden alle Verträge mit internen Dienstleistern gekündigt.

Die 1&1 De-Mail GmbH versucht eine Übernahme des Vertrauensdienstes durch einen anderen qualifizierten Vertrauensdiensteanbieter zu erreichen, kann dies aber nicht gewährleisten. Für den Fall, dass ein anderer qualifizierter Vertrauensdiensteanbieter die Kundendaten übernimmt, hält die 1&1 De-Mail GmbH alle Informationen vor, bis nachgewiesen werden kann, dass der andere VDA diese nicht mehr benötigt.

Übernimmt kein anderer Diensteanbieter die Konten muss die 1&1 De-Mail GmbH sicherstellen, dass die gespeicherten Daten für mindestens drei Monate, ab dem Zeitpunkt der Beendigungsbenachrichtigung, abrufbar bleiben.

4.10 Asset Management

Die 1&1 De-Mail GmbH stellt ein ausreichendes Sicherheitslevel seiner Assets, einschließlich der Information Assets, sicher. Die Verfahren zum Schutz der Information Assets sind im ISMS dokumentiert und durch die Zertifizierung entsprechend ISO/IEC 27001 nachgewiesen. Die eingesetzten IT-Systeme sind in einer Komponentenliste vermerkt. Das jeweilige Sicherheitslevel entspricht den gesetzlichen Bestimmungen.

Es bestehen Kontrollmechanismen um Verlust, Beschädigung oder Kompromittierung der eingesetzten Komponenten sowie die Unterbrechung des Geschäftsbetriebs und den Diebstahl, oder die Kompromittierung von sensiblen Informationen zu verhindern.

Sämtliche Medien werden sicher aufbewahrt. Sensible Daten, die auf zu entsorgenden Medien enthalten sind, werden nach einem sicheren Verfahren (z.B. US Department of Defense Sanitizing DoD 5220.22-M) gelöscht.

5 Technische Sicherheitsmaßnahmen

Im Rahmen des Aufbaus und der Installation der De-Mail-Infrastruktur werden die Systeme mehrfach aufgesetzt. Grundlegende Vorgaben für die Installation und den Betrieb eines Servers sind in der Richtlinie „Sicherer Betrieb“ beschrieben. Die Richtlinie ist für alle Mitarbeiter verfügbar und wird regelmäßig aktualisiert. Serverdienste sind so konfiguriert, dass nur die für die Erbringung des Dienstes notwendigen Hardwareressourcen verwendet werden (z.B. Netzwerkschnittstellen). Alle nicht benötigten Soft- und Hardwareressourcen sind deaktiviert. Darüber hinaus werden vor dem Aufbau, Änderungen und Erweiterungen von Systemen sowie bei Softwareentwicklungsprojekten die Anforderungen an die Sicherheit erhoben, um diese bereits in der Konzeptionsphase berücksichtigen zu können.

Die IT-Systeme werden in einer sicheren Umgebung betrieben (vgl. Kapitel 4.2), um sie vor unberechtigten Zugriffen, Modifikationen und Diebstahl zu schützen. Zudem erfolgt regelmäßig zentral eine Datensicherung (Back-Up) zur Vermeidung von Datenverlust. Die Daten werden auf Festplatten gesichert, die ausgetauscht werden, sobald sie funktionsunfähig sind oder gemäß Herstellerangaben nicht mehr betrieben werden dürfen. Datenverluste wegen alternder Datenträger werden durch redundante Speicherung der Daten vermieden.

Das Sicherheitsniveau eines Servers richtet sich nach dem Schutzbedarf der Daten auf dem Server. Angesichts der regelmäßig bei den eIDAS-Diensten verwendeten Daten kann grundsätzlich von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ausgegangen werden.

Es gibt einen definierten und verbindlichen Change- und Patch-Management Prozess, der gewährleistet, dass sicherheitsrelevante Patches und Updates zeitnah und geordnet in die Systeme eingepflegt werden. Geeignete Informations- und Bezugsquellen sowie Verfahren zur Identifizierung und Behebung technischer Schwachstellen sind definiert und festgelegt.

Bei der 1&1 De-Mail GmbH existiert ein an der IT Infrastructur Library (ITIL) orientiertes Change Management. Die Entscheidung, ob aus einer Änderungsanfrage (Request for Change) eine Änderung (Change) generiert wird, trifft der Betriebsverantwortliche, der einen Change Manager mit der weiteren Bearbeitung und der Abstimmung der Durchführungsmodalitäten beauftragt. Der vorhandene Prozess des Change Managements stellt mit Hilfe des Vier-Augen-Prinzips sicher, dass alle Änderungsanforderungen erfasst, bearbeitet und dokumentiert werden. Änderungen werden mit Ausnahme definierter Minimaländerungen systemintern auswertbar dokumentiert. Die Einzelheiten für den Change Management Prozess sind definiert und dokumentiert. Das Change Management und der darin beschriebene Prozess werden regelmäßig und kontinuierlich von der 1&1 De-Mail GmbH überprüft und durch die Zertifizierung entsprechend ISO/IEC 27001 nachgewiesen.

Alle Sicherheitsupdates und Patches unterliegen dem Change Management Prozess und werden innerhalb einer angemessenen Zeit behoben. Patches werden vor dem Einspielen in einer Testumgebung auf ihre Verwendbarkeit für den Produktiveinsatz überprüft. Patches werden nicht eingespielt, wenn sich daraus Nachteile und Instabilität ergeben, die schwerwiegender sind als die Vorteile des Patches. Das Nichteinspielen solcher Updates sowie der Grund dafür werden dokumentiert. Dringende sicherheitskritische Patches sind zeitnah einzuspielen und dürfen den Change Management Prozess nachträglich durchlaufen. Maßnahmen zur Aufrechterhaltung der Verfügbarkeit von Komponenten, wie z. B. die redundante Auslegung von Serversystemen, sind generell im Verfügbarkeitskonzept beschrieben.

Alle Systemänderungen werden geloggt und sind damit, z.B. über das Security Information and Event Management (SIEM) System, auswertbar. Im Rahmen der turnusmäßigen „Selbstaudits“ finden darüber hinaus Überprüfungen statt, bei denen die Systeme und Systemzustände kontrolliert werden.

Redundante Loadbalancer verteilen Anfragen auf die redundanten Serversysteme. Diese sind verteilt über redundante Rechenzentren. Datenhaltende Systeme werden entsprechend repliziert. Alle Systeme und Dienste sind so konfiguriert, dass eine Übernahme zwischen den Redundanten Partnerkomponenten automatisch erfolgt. Dazu testen die Loadbalancer die Verfügbarkeit der Dienste und reagieren gemäß Konfiguration auf Änderungen des Zustandes. Es existiert daneben ein umfassendes Monitoring der Services im 24/7-Betrieb.

Es existieren sowohl ein Datensicherungskonzept für Server als auch Notfallpläne für Serverausfälle und für andere Systeme, die zum Betrieb eines Servers benötigt werden. Störungen werden im Rahmen des Incident Managements behandelt. Regelmäßige Tests der Störungs- und Notfallprozeduren sind vorgesehen.

Die geregelte Außerbetriebnahme von IT-Systemen und Datenträgern ist in der Richtlinie „Server“ beschrieben. Administratoren sind verpflichtet die technischen und organisatorischen Prozesse im Rahmen des Lebenszyklus der betreuten IT Systeme einzuhalten.

Der Nachweis erfolgt jährlich im Rahmen einer Auditierung nach ISO/IEC 27001.

5.1 Netzwerktechnische Sicherheitsmaßnahmen

Der Betrieb erfolgt in zwei physikalisch getrennten Rechenzentren, die jeweils über redundante Systeme (Multiplexverfahren) miteinander verbunden sind. Alle Kommunikationsverbindungen – bis hin zu den Hauseinführungen – sind redundant vorhanden und werden ständig an aktuelle Gegebenheiten angepasst. Für aktive Netzkomponenten (Switche, Router, Firewalls) existieren Vorgaben hinsichtlich ihrer Konfiguration, Administration, der erlaubten und zu deaktivierenden bzw. zu filternden Protokolle. Die Übertragung zwischen den Rechenzentren erfolgt verschlüsselt.

Änderungen von Hard- und Software unterliegen eigenen Prozessvarianten im Change Management.

Das Netzwerk ist in verschiedene Zonen aufgeteilt, um eine Trennung der Netze zu gewährleisten. Die Kommunikation zu und zwischen diesen Zonen ist jeweils über Firewalls abgesichert. Das etablierte Firewall-Regelwerk wird regelmäßig geprüft und angepasst. Nur die Systeme, die direkt zur Dienstnutzung benötigt werden, dürfen aus dem Internet erreichbar sein. Produktiv- und Testumgebung sind voneinander getrennt. Ebenfalls wurde die Administrationsumgebung von der Produktivumgebung im Netzwerk separiert.

Der Betrieb der Komponenten und die Einhaltung der vorgegebenen Betriebsparameter werden fortlaufend mit Hilfe eines Monitoring Systems überwacht. Hierbei werden laufend Performancemessungen und Verkehrsflussanalysen vorgenommen. Beim Erreichen definierter Schwellenwerte oder der Entdeckung sicherheitsrelevanter Ereignisse entsteht Handlungs- und Entscheidungsbedarf. Dabei wird sichergestellt, dass über diesen Weg, keine sensiblen Daten ausgeleitet werden. Die Monitoring Daten dienen zusätzlich zur Kapazitätsplanung.

Alle sicherheitsrelevanten Prozesse und Störungen sowie Zugriffe der Mitarbeiter werden protokolliert. In diesem Zusammenhang – sofern sicherheitsrelevant – werden insbesondere Start und Beendigung der IT-Systeme, Start und Beendigung der Logging-Funktionalität der relevanten IT-Systeme, Systemabstürze, Ausfälle der Hardware, Aktivitäten der Firewall und der Router protokolliert. Die Log-Files werden auf zusätzlich gesicherten Log-Servern gesichert. Diese sind gegen unautorisiertes Löschen oder Datenvernichtung ausreichend nach dem Stand der Technik gesichert. Der Zugriff kann nur über autorisiertes Personal erfolgen. Näheres wird im Rollenkonzept der 1&1 De-Mail GmbH beschrieben.

Zur Protokollierung von Ereignissen im IT Verbund wird ein Security Information and Event Management System (SIEM-System) genutzt. Dieses bietet eine zusammenfassende Datensammlung, Normalisierung, Analyse, Korrelation und Darstellung (Reporting) unterschiedlicher Logevents und Networkflows, welche das SIEM von unterschiedlichsten Loggingsources empfangen bzw. abholen kann. Das SIEM System ist als „Distributed Enviroment“ aufgebaut und installiert, d.h. Management und Event/Flow-Collector sind getrennt auf unterschiedlichen Maschinen implementiert. Das SIEM-System ist als Hochverfügbarkeitslösung implementiert.

Zusätzlich findet eine automatische Protokollanalyse statt, um Angriffsversuche und Fehler frühzeitig zu erkennen. Diese Maßnahme wird durch regelmäßige manuelle Kontrollen ergänzt. Neben den Protokollen werden insbesondere auch die Audit Logs geprüft.

Bei der 1&1 De-Mail GmbH existieren klar definierte Abläufe und Regeln für die Behandlung von Störungen in IT-Bereichen. Der gesamte organisatorische und technische Prozess der Reaktion auf eine erkannte oder vermutete Störung, wird im Rahmen des Incident Managements behandelt. Störungen der Hardware oder Software, Angriffsversuche, Verstöße gegen die Sicherheitsregeln und Meldungen des Monitoring-Systems werden an die Administratoren gemeldet, die sich unverzüglich um die Behebung des Fehlers bzw. eine Eingrenzung möglicher sicherheitsrelevanter Ereignisse kümmern. Sicherheitsrelevante Vorfälle und offene Sicherheitslücken werden unverzüglich an den Sicherheitsbeauftragten der 1&1 De-Mail GmbH gemeldet, der die Umsetzung aller zur Behebung des Sicherheitsvorfalls notwendigen Maßnahmen bewertet und dann ggf. umsetzen lässt und den Vorgang dokumentiert.

Relevante Sicherheitsvorfälle werden innerhalb von 24 Stunden an die aufsichtführende Stelle gemeldet. Sofern zutreffend, werden auch von dem Sicherheitsvorfall betroffene Personen und Firmen unverzüglich informiert.

Kritische Schwachstellen, die nicht anderweitig adressiert worden sind, werden innerhalb von 48 Stunden nach deren Entdeckung adressiert. Auf Basis einer Bewertung des mit derartigen Schwachstellen verbundenen Risikos wird die 1&1 De-Mail GmbH diese beheben oder – wenn dies im Verhältnis zu den Auswirkungen nicht mit wirtschaftlich vertretbarem Aufwand möglich ist – dokumentiert, warum diese nicht behoben werden.

Des Weiteren finden in regelmäßigen Abständen (mind. 1x jährlich) sogenannte Penetrationstests statt. Ebenso wird eine regelmäßige Schwachstellenüberprüfung (mind. 4x jährlich) durchgeführt. IT-Systeme und eingesetzte Software werden dabei auf Schwachstellen untersucht die Ergebnisse werden dokumentiert und im ISMS verwaltet. Etwaige Mängel werden gemäß dem zuvor beschriebenen Prozess behandelt.

Penetrationstest werden durch interne oder externe Dienstleister durchgeführt. Die regelmäßigen Schwachstellenprüfungen werden durch einen internen DL durchgeführt. Bei Auswahl der Dienstleister wird darauf geachtet, dass die Dienstleister über die erforderlichen Qualifikationen und Fachkenntnisse verfügen.

5.2 Backup- und Wiederherstellung

Ziel ist es einen Datenverlust von Nutzerdaten zu vermeiden. Die Rechenzentren verfügen daher über redundante Standorte. Backup- und Wiederherstellungspläne liegen vor und sind den Verantwortlichen vollumfänglich bekannt. Es werden regelmäßige Wiederherstellungstests durchgeführt.

5.3 Zutrittskontrolle

Die für De-Mail verwendeten Systeme befinden sich in physikalisch getrennten Rechenzentrumsbereichen. Die verwendeten Racks sind besonders gesichert.

Zutritt zu den Räumen der datenverarbeitenden Systeme wird mittels eines Vier-Augen-Prinzips durch einen Mitarbeiter der 1&1 De-Mail GmbH und einem Mitarbeiter der IONOS SE gewährleistet.

5.4 Zugriffskontrolle

Zugänge zu IT-Systemen werden erst nach erfolgreicher Authentisierung gewährt. Die Benutzerrechte für Zugriffe auf Dateien und Programme sind abhängig von der jeweiligen Rolle und nach dem Need-to-Know-Prinzip definiert. Rollen und Berechtigungen sind im ISMS dokumentiert.

Im De-Mail Verbund haben alle Systeme den Schutzbedarf hoch oder sehr hoch. Entsprechend des Bedarfs erfolgt die Authentisierung nach einem Mehrfaktor-Prinzip. Zusätzlich zu Username und Passwort kommt ein Einmaltoken als Merkmal zum Einsatz, dieses wird auf seine Gültigkeit geprüft. Es gibt nur einen einzigen Zugriffsweg zu den IT-Systemen. Dort werden außerdem rollengebundene Restriktionen umgesetzt, als auch Kontrollmechanismen wie das 4-Augen-Prinzip erzwungen.

Die Kommunikation von Authentisierungsinformationen findet ausschließlich verschlüsselt statt.

Benutzer werden nach ihren Rollen in entsprechende Gruppen eingeteilt. Benutzer werden nur auf Systemen ausgerollt auf denen sie auch administrative Tätigkeiten ausüben.

Eine Führungskraft ist verantwortlich für die Beantragung, Änderungen, und Sperrung von Accounts. Dieser Lebenszyklus ist im ISMS modellierten Prozesse zu Vergabe, Änderung, Sperrung nachvollziehbar dokumentiert. Alle Rolleninhaber sind sich Ihrer Verantwortung bewusst und akzeptieren Ihre Rolle.

Es bestehen keine dauerhaften oder unbeaufsichtigten Wartungszugriffsmöglichkeiten durch Externe.

5.5 Verfügbarkeitskontrolle

Es existieren drei Backups, welche eine Lebensdauer von je sieben Tagen haben. Die Backups sind zweifach verschlüsselt, sowohl auf Dateisystem- als auch auf Dateiebene.

Zwei der Backups werden im Rechenzentrum aufbewahrt, ein drittes wird in einer feuerfesten Kassette in einem nur eingeschränkt zugänglichen feuerfesten Tresor aufbewahrt. Die Funktionsfähigkeit der Backupsysteme wird quartalsweise geprüft.

5.6 Trennungskontrolle

Die De-Mail-Systeme befinden sich in physikalisch und logisch vollständig getrennten Netzwerksegmenten.

5.7 Zeitservice

Zeitquelle für den Zeitservice ist die gesetzliche Zeit (MEZ/MESZ), die von der Physikalisch Technischen Bundesanstalt (PTB) als UTC (PTB) + 1 (2) realisiert und verbreitet (DFC77, Telefonzeitdienst der PTB, NTP) wird.

Die Uhrzeiten aller im De-Mail-System eingesetzten Komponenten werden über einen dedizierten Zeitserver, der über die oben geforderte gesetzliche Zeit verfügt, synchronisiert. Die Zeit wird über ein separates Management-Netz verbreitet. Das Management-Netz ist ein getrenntes Netz und dient unabhängig vom Netz der Nutzdaten der Administration der Systeme.

Die NTP-Server stellen anderen Assets die aktuelle Zeit zur Verfügung und gewährleisten dadurch die synchrone gesetzliche Zeit auf allen Servern. Der 1&1 Konzern betreibt hierfür drei Stratum 1 Zeitquellen.

Dieses Zeitsignal wird von 4 Zeitservern georedundant über ein Anycast Protokoll zur Verfügung gestellt.

Pro De-Mail Rechenzentrum stehen jeweils zwei NTP Appliances zur Verfügung. Diese holen das Zeitsignal von den Servern, und bieten das - gemäß dem NTP Algorithmus - beste der erhaltenen Signale im De-Mail Leistungssystem an.

Auf jedem De-Mail Server ist ein NTP-Dienst installiert, der sich mit den oben genannten Zeitservern synchronisiert.

Die Zeitsynchronisation über gesicherte Kanäle erfolgt auf allen unterstützenden Assets mehrmals täglich. Die Zeitinformation, die der Zeitserver zur Verfügung stellt, darf max. 1 Sekunde von der gesetzlichen Zeit abweichen.

Die Betriebssysteme und die Anwendungssoftware der IT-Systeme, die den Zeitservice für die jeweilige De-Mail-Infrastruktur zur Verfügung stellen, werden durch den Administrator regelmäßig, mindestens einmal täglich, auf Integrität geprüft.

5.8 Kryptographische Verfahren und sichere Protokolle

Um die Vertraulichkeit und Integrität der Informationen in den datenverarbeitenden Systemen zu gewährleisten, ist es u.a. notwendig, kryptographische Verfahren und sichere Protokolle einzusetzen.

Es werden ausschließlich Protokolle und kryptographische Verfahren verwendet, deren Sicherheit nach aktuellem Kenntnisstand der Fachwelt als ausreichend für den jeweiligen Einsatzzweck und der jeweiligen Einsatzdauer bewertet sind. (Starke Verschlüsselung nach Stand der Technik). Insbesondere wird bei kryptographischen Algorithmen auf eine hinreichende Stärke des Algorithmus und eine ausreichend große Schlüssellänge geachtet. Die Beurteilung des Stands der Technik basiert dabei auf den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), gemäß Technischer Richtlinien (TR)

- TR 01201 Teil 1.4 IT-Basisinfrastruktur Interoperabilitätsspezifikation

- TR 03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen

Die Technischen Richtlinien werden regelmäßig durch das BSI auf Aktualität und Angemessenheit geprüft.

Bei Daten mit einem hohen Schutzbedarf werden zertifizierte Produkte zur sicheren Verschlüsselung eingesetzt (z.B. nach Common Criteria oder FIPS).

Die technischen und organisatorischen Maßnahmen sind im ISMS der IONOS SE und 1&1 De-Mail GmbH dokumentiert und werden in regelmäßigen Abständen geprüft und bei Bedarf angepasst.

5.9 Incident Management

Für die Sicherstellung und Aufrechterhaltung des Dienstes wurde ein Incident Management Prozess nach ISO/IEC 27001 etabliert. Die Systeme werden rund um die Uhr von qualifiziertem Personal überwacht. Auf Sicherheitsvorfälle kann schnell reagiert werden – Erkannte Angriffe können somit frühzeitig abgewehrt werden. Im Rahmen des Incident Managementprozesses erfolgt bei Bedarf eine Ursachenanalyse (Root Cause Analysis). Die Ursachenanalyse dient dazu wiederkehrende Störung zu vermeiden, die auf der gleichen Ursache beruhen.

Die 1&1 EU-Mail benachrichtigt zuständige Parteien im Einklang mit den geltenden Regulierungsvorschriften bei Verletzung der Sicherheit oder Verlust der Integrität, die einen erheblichen Einfluss auf den Vertrauensdienst oder auf personenbezogene Daten haben können.

Grundsätzlich wird auf die vollständige Einhaltung des Art. 19.2 eIDAS VO geachtet. Die Aufsichtsbehörde wird innerhalb von 24h über jeden erheblichen Sicherheitsvorfall informiert.

6 Audits und andere Bewertungsanforderungen

6.1 De-Mail

Als akkreditierter De-Mail-Diensteanbieter wird die 1&1 De-Mail GmbH alle 3 Jahre von einer unabhängigen Organisation auditiert. Bei diesen Audits wird überprüft, ob die 1&1 De-Mail GmbH die Anforderungen des De-Mail-Gesetzes erfüllt.

Die Akkreditierung umfasst die Prüfung von Nachweisen zu technischen und organisatorischen Anforderungen, zur Erfüllung der datenschutzrechtlichen Vorgaben, zur Zuverlässigkeit und Fachkunde für den Betrieb von De-Mail-Diensten und zur geeigneten Deckungsvorsorge.

Darüber hinaus wird jede wesentliche Änderung bei der zuständigen Behörde angezeigt und ebenfalls von einer unabhängigen Organisation überprüft und bestätigt.

Die durch 1&1 De-Mail GmbH beauftragten Identdienstleister werden regelmäßig geschult. Zusätzlich werden diese einem regelmäßigen Audit unterzogen.

Der Leiter des De-Mail-Diensteanbieters ist verantwortlich für die korrekte Umsetzung der Bestimmungen aus den einschlägigen Gesetzen, internationalen Standards, dem Sicherheitskonzept und den internen Verfahrens- und Arbeitsanweisungen. Er prüft diese Umsetzung regelmäßig durch die Beauftragung von internen Audits, deren Ergebnisse alle 3 Jahre bei externen Audits vorgelegt werden.

6.2 eIDAS

Die 1&1 De-Mail GmbH betreibt den Vertrauensdienst 1&1 EU-Mail im Einklang mit dem geltenden Recht.

Als akkreditierter Vertrauensdiensteanbieter wird die 1&1 De-Mail GmbH alle 2 Jahre von einer unabhängigen Organisation auditiert. Bei diesen Audits wird überprüft, ob die 1&1 De-Mail GmbH die Anforderungen der eIDAS-VO erfüllt.

Wie die 1&1 De-Mail GmbH als De-Mail-Diensteanbieter die Anforderungen an qualifizierte Dienste zur Zustellung elektronischer Einschreiben nach eIDAS-Verordnung erfüllen, können Sie auf der nachfolgenden Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) und dem dort veröffentlichten Dokument nachlesen:

- https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-Verordnung/Zustellung-elektronischer-Einschreiben/zustellung-elektronischer-einschreiben_node.html

Die Ergebnisse der Prüfungen sind nicht öffentlich verfügbar. Werden bei den Audits Mängel festgestellt, so werden diese in Abstimmung zwischen der 1&1 De-Mail GmbH und dem Auditor beseitigt.

Der Vertrauensdienst wird durch für ihre Aufgaben geschulte und autorisierte Mitarbeiter innerhalb einer baulich, organisatorisch und systemtechnisch abgesicherten Umgebung betrieben. Darüber hinaus wird jede sicherheitsrelevante Änderung bei der zuständigen Behörde angezeigt und ebenfalls von einer unabhängigen Organisation überprüft und bestätigt.

Die 1&1 De-Mail GmbH führt regelmäßig, mindestens jedoch alle 12 Monate eine Risikoanalyse durch, um die Risiken für den angebotenen Vertrauensdienst 1&1 EU-Mail zu identifizieren, zu analysieren und zu bewerten. Dabei werden sowohl technische als auch betriebliche Anforderungen berücksichtigt. Dies umfasst auch eine Betrachtung der Information Assets.

Zuständig sind die leitenden Rollen der 1&1 De-Mail GmbH. Insbesondere bei einer wesentlichen Änderung der Bedrohungslage, erfolgt eine erneute Risikoanalyse. Die 1&1 De-Mail GmbH ergreift unter Berücksichtigung der Risikoanalyse angemessene Gegenmaßnahmen. Es wird sichergestellt, dass das Sicherheitslevel dem Risikolevel entspricht. Die im Rahmen der Risikoanalyse identifizierten Restrisiken werden bewertet und von den leitenden Rollen der 1&1 De-Mail GmbH akzeptiert.

Einzelheiten sind im Informationssicherheitsmanagementsystem der 1&1 De-Mail GmbH dokumentiert. Darin sind insbesondere die erforderlichen Sicherheitsanforderungen und die betrieblichen Abläufe der 1&1 De-Mail GmbH festgelegt. Das ISMS wird fortlaufend angepasst und insbesondere, wenn die Risikoanalyse zum Ergebnis kommt, dass neue Risiken entstanden sind und weitere Gegenmaßnahmen erforderlich sind.

Die 1&1 De-Mail GmbH legt zur Prüfung der Einhaltung seiner Verpflichtungen der Aufsichtsstelle auf deren Verlangen die in Betracht kommenden Aufzeichnungen, Belege, Bücher, Schriftstücke und sonstigen Unterlagen zur Einsicht vor, auch soweit sie in elektronischer Form geführt werden.

7 Sonstige geschäftliche und rechtlichen Angelegenheiten

Im nachfolgenden werden die geschäftlichen und rechtlichen Angelegenheiten für die Zustellung elektronischer Einschreiben, auf Basis des De-Mail-Dienstes beschrieben. Hierbei werden u.a. auf die markenspezifischen Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account verwiesen, die über ein dauerhaftes Kommunikationsmittel (markenspezifische Webseiten) zur Verfügung gestellt werden. Die Informationen sind dort in einer leicht verständlichen Sprache verfügbar und werden elektronische übermittelt.

7.1 Preise

Die aktuelle Preisliste ist auf den jeweiligen markenspezifischen Webseiten wie folgt verfügbar:

- GMX: https://hilfe.gmx.net/de-mail/setup-costs.html
- WEB.DE: https://hilfe.web.de/de-mail/setup-costs.html
- 1&1: https://dl.1und1.de/de-mail/1und1/Preisliste_De-Mail.pdf

7.2 Finanzielle Verantwortung

Die 1&1 De-Mail GmbH verfügt über die notwendigen Mittel, um den Betrieb des Vertrauensdienstes 1&1 EU-Mail ordnungsgemäß durchzuführen. Die notwendigen Mittel werden durch die Erhebung der Gebühren für die Bereitstellung und Nutzung des Vertrauensdienstes der 1&1 De-Mail GmbH erzielt.

Darüber hinaus verfügt die 1&1 De-Mail GmbH über eine angemessene Deckungsvorsorge gemäß der eIDAS-VO Art. 24 Absatz 2 Buchstabe c.

Für den Fall einer Insolvenz ist durch eine Organschaft mit der 1&1 Mail&Media GmbH sichergestellt, dass die gesetzlichen Anforderungen an einen De-Mail Diensteanbieter/eIDAS Vertrauensdiensteanbieter erbracht werden können. Hierzu zählen:

- Einleitung der Einstellung der Tätigkeiten als De-Mail Diensteanbieter/eIDAS Vertrauensdiensteanbieter
- Dem Nutzer für einen Zeitraum von drei Monaten nach Vertragsende den Zugriff auf die im Postfach und in der Dokumentenablage abgelegten Daten zu ermöglichen und ihn auf ihre Löschung mindestens einen Monat vor dieser in Textform hinzuweisen
- Bemühung, dass das De-Mail-Konto von einem anderen akkreditierten Diensteanbieter übernommen werden kann
- Sofern kein anderer De-Mail Diensteanbieter das Konto übernimmt:
    - Sicherstellung, dass die im Postfach und in der Dokumentenablage gespeicherten Daten für wenigstens drei Monate ab dem Zeitpunkt der Benachrichtigung des Nutzers abrufbar bleiben,
    - Übergabe der Dokumentation nach §13 De-Mail Gesetz an die zuständige Behörde

7.3 Datenschutz

Die personenbezogenen Informationen werden gemäß der EU- Datenschutz-Grundverordnung (DSGVO) und des De-Mail-Gesetzes (De-Mail- Kriterienkatalog für den Datenschutz-Nachweis / De-Mail Datenschutz-Zertifikat) geschützt. Weitere Informationen sind unter den folgenden markenspezifischen Datenschutzhinweisen verfügbar:

- GMX: https://img.ui-portal.de/demail/privacy/data_privacy_gmx.html
- WEB.DE: https://img.ui-portal.de/demail/privacy/data_privacy_webde.html
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_Datenschutzhinweise.pdf

7.4 Urheberrecht

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von 1&1 De-Mail GmbH unzulässig.

7.5 Gewährleistung

Gewährleistung bzgl. der Verfügbarkeit des Dienstes sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Adressen verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

7.6 Haftungsausschlüsse- und Beschränkungen

Haftungsfragen sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Webseiten verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

7.7 Schadenersatz

Schadenersatzansprüche sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Adressen verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

7.8 Fristen und Beendigung

Fristen und Beendigung sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Webseiten verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

7.9 Änderungen der TSPS

Die 1&1 De-Mail GmbH behält sich das Recht vor, Änderungen und Anpassungen an dieser TSPS durchzuführen, um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren. Änderungen der TSPS werden auf den jeweiligen markenspezifischen Webseiten

- GMX: https://www.gmx.net/produkte/eIDAS
- WEB.DE: https://produkte.web.de/eIDAS/
- 1&1: https://hilfe-center.1und1.de/e-mail-c82645/de-mail-c85617/eidas-infoseitea797697.html

angekündigt und gelten von dem Moment an, in dem die TSPS in Kraft tritt. Die TSPS tritt in zwei Wochen nach Veröffentlichung der Änderungen in Kraft, außer für den Fall, dass die Veröffentlichung einen anderen Zeitraum vorsieht.

Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Die aktuelle TSPS wird mindestens einmal jährlich von 1&1 De-Mail GmbH einem Review unterzogen. Nutzer elektronischer Einschreiben oder andere an dem Vertrauensdienst 1&1 EU-Mail beteiligte Personen bzw. Organisationen können Kommentare zu dem Inhalt der TSPS an 1&1 De-Mail GmbH melden. Die Entscheidungsbefugnis für Änderungen der TSPS bleibt bei 1&1 De-Mail GmbH.

Änderungen dieser TSPS werden durch die Mitarbeiter der 1&1 De-Mail GmbH vorgenommen. Nach Durchführung der Änderungen wird das Dokument dem Managementboard Informationssicherheit und Datenschutz De-Mail der 1&1 De-Mail GmbH, zu welchem unter anderem der Leiter des Vertrauensdienstes 1&1 EU-Mail gehört, vorgelegt. Das

Managementboard Informationssicherheit und Datenschutz De-Mail überprüft die Änderung und gibt die TSPS zur Veröffentlichung frei.

Änderungen der TSPS, welche nur Rechtschreibfehler beheben oder redaktioneller Natur sind, treten auch ohne vorherige Ankündigung in Kraft.

Bei jeder Änderung der TSPS wird deren Versionsnummer und Datum erneuert.

7.10 Anwendbares Recht

Die eIDAS-VO sowie das Vertrauensdienstegesetz regeln generell den Versand von elektronischen Einschreiben und die Anforderungen an Vertrauensdiensteanbieter. Ferner gilt das Recht der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Montabaur.

Der 1&1 Vertrauensdienst EU-Mail wird im Einklang mit den Bestimmungen des Allgemeinen Gleichbehandlungsgesetztes betrieben.

7.11 Einhaltung geltendes Recht

Der 1&1 Vertrauensdienst macht seine Vertrauensdienste und zur Erbringung der Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar, soweit dies möglich ist. Hiervon sind nachfolgende Punkte betroffen:

- Es besteht Wahlfreiheit des verwendeten Zugangs (Browser oder Outlook Add-In) zu De-Mail. Die Funktionalität zur Barrierefreiheit innerhalb Browser und Outlook sind voll nutzbar.
- Dargestellte Grafiken sind je Marke farboptimiert (gelb und blau) für seheingeschränkte Personen.
- Durch Nutzung von Zeichenketten in der Darstellung ist der Einsatz von Screenreadern möglich.

Diskriminierung und Rassismus sind mit einem ordnungsgemäßen Geschäftsbetrieb nicht zu vereinbaren. Wer Kunden, Geschäftspartner oder Mitarbeiterinnen und Mitarbeiter zum Beispiel aus Gründen der ethnischen Herkunft ungerechtfertigt benachteiligt, verletzt das Allgemeine Gleichbehandlungsgesetz. Der 1&1 Vertrauensdienst EU-Mail richtet sich nach diesem Grundsatz und wird grundsätzlich keinerlei Einschränkungen wegen der der ethnischen Herkunft oder aus sonstigen diskriminierenden Gründen vornehmen.

7.12 Beschwerden, Empfehlungen und Eskalation

Beschwerden und Eskalation sind in den Allgemeinen Geschäftsbedingungen (AGB) für den De-Mail-Account geregelt, diese sind unter den folgenden markenspezifischen Webseiten verfügbar:

- GMX: https://agb-server.gmx.net/de-mail
- WEB.DE: https://agb-server.web.de/de-mail
- 1&1: https://dl.1und1.de/de-mail/1und1/1und1_De-Mail_AGB.pdf

Empfehlungen können an eine der unter Kapitel 1.4 *Organisation zur Verwaltung dieses Dokuments* angegebenen E-Mail Adressen eingereicht werden.

1&1 De-Mail GmbH freut über jegliche Beteiligung und wird jede Empfehlung berücksichtigen. Aufgrund der Menge der Anfragen kann eine Bearbeitung etwas Zeit in Anspruch nehmen – Wir bitten um Verständnis.

7.13 Geschäftsbedingungen

In den Allgemeinen Geschäftsbedingungen (AGB) für Geschäftskunden der 1&1 De-Mail GmbH sind Angaben zu folgenden Aspekten enthalten:

1. Geltungsbereich
2. Vertragsgegenstand und Technische Voraussetzungen
3. Nutzerkreis
4. Zustandekommen des Vertrages
5. Beginn der Leistungserbringung
6. Identifizierung
7. Beachtung von Urheberrechten
8. Rechte und Pflichten des Nutzers
9. Freistellung
10. Vergütung und Zusatzkosten
11. Registrierungsdaten des Nutzers
12. Inhalt von De-Mail-Nachrichten
13. Zeitkritische De-Mail-Nachrichten
14. Löschung von Daten
15. Einsicht in die Daten nach De-Mail-Gesetz
16. Sperrung des De-Mail-Accounts
17. Auflösung des De-Mail-Accounts
18. Gewährleistung
19. Haftung
20. Vertragsbeendigung
21. Vertragsübertragung
22. Datenschutz
23. Schlussbestimmungen

In den Allgemeinen Geschäftsbedingungen (AGB) für Privatkunden der Produkte WEB.DE De-Mail und GMX De-Mail sind Angaben zu folgenden Aspekten enthalten:

1. Geltungsbereich
2. Vertragsgegenstand und Technische Voraussetzungen
3. Nutzerkreis
4. Zustandekommen des Vertrags
5. Beginn der Leistungserbringung
6. Identifizierung
7. Beachtung von Urheberrechten
8. Rechte und Pflichten des Nutzers
9. Freistellung
10. Vergütung und Zusatzkosten
11. Registrierungsdaten des Nutzers
12. Nutzung von Pseudonymen
13. Zeitkritische De-Mail-Nachrichten

14. Löschung von Daten
15. Einsicht in die Daten
16. Sperrung des De-Mail-Accounts
17. Auflösung des De-Mail-Accounts
18. Gewährleistung
19. Haftung
20. Vertragsbeendigung
21. Datenschutz
22. Schlussbestimmungen
23. Widerrufsbelehrung

Die AGBs beinhalten die Bedingungen für die Nutzung elektronischer Einschreiben der 1&1 De-Mail GmbH. Grundlage für die Allgemeinen Geschäftsbedingungen ist das deutsche Recht.