Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Freitag, 13. Mai 2022
BAnz AT 13.05.2022 B5

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Bekanntmachung des De-Mail-Kriterienkatalogs für den Datenschutz-Nachweis nach § 18 Absatz 3 Nummer 4 des De-Mail-Gesetzes des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Vom 17. März 2022

Nachstehend gibt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit den folgenden De-Mail-Kriterienkatalog für den Datenschutz-Nachweis bekannt:

De-Mail-Kriterienkatalog für den Datenschutz-Nachweis
Version 3.0

Der De-Mail-Kriterienkatalog für den Datenschutz-Nachweis kann barrierefrei auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter http://www.datenschutz.bund.de abgerufen werden.

Diese Bekanntmachung ergeht im Anschluss an die Bekanntmachung des De-Mail-Kriterienkatalogs für den Datenschutz-Nachweis vom 23. Juni 2020 (BAnz AT 24.07.2020 B3).

Bonn, den 17. März 2022

Der Bundesbeauftragte
für den Datenschutz und die Informationsfreiheit

Im Auftrag
Weber

Die PDF-Datei der amtlichen Veröffentlichung ist mit einer qualifizierten elektronischen Signatur versehen. Siehe dazu Hinweis auf Infoseite.

De-Mail-Kriterienkatalog
für den Datenschutz-Nachweis
nach § 18 Absatz 3 Nummer 4 des De-Mail-Gesetzes

Version 3.0

Stand: 17. März 2022

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Straße 153
D-53117 Bonn

Telefon: +49 (0)22899-7799-0
Telefax: +49 (0)22899-7799-550

E-Mail: de-mail@bfdi.bund.de
De-Mail: poststelle@bfdi.de-mail.de

Internet: http://www.datenschutz.bund.de

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2022)

Inhaltsverzeichnis

I. Einleitung
II. Kriterienkatalog
III. Gestaltung des Gutachtens
IV. Fachliche Eignung für die Gutachtenerstellung
V. Veröffentlichung
VI. Webadressen
VII. Technische Richtlinien
VIII. Abkürzungsverzeichnis

I. Einleitung

Gemäß § 18 Absatz 1 Nummer 4 des De-Mail-Gesetzes ist für die Akkreditierung eines Diensteanbieters der Nachweis erforderlich, dass er bei Gestaltung und Betrieb von De-Mail-Diensten die datenschutzrechtlichen Anforderungen erfüllt. Der Nachweis wird durch ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erbracht (§ 18 Absatz 3 Nummer 4 des De-Mail-Gesetzes).

Das Zertifikat ist formlos zu beantragen. Mit dem Antrag ist die Vorlage eines Gutachtens erforderlich, mit dem die Erfüllung der datenschutzrechtlichen Kriterien nachgewiesen wird. Der De-Mail-Kriterienkatalog[1] dient als Grundlage für die Begutachtung. Er stellt die datenschutzrechtlichen Anforderungen dar, die durch die sachverständigen Stellen für Datenschutz zu prüfen sowie im Gutachten zu erläutern und zu bewerten sind.

In dem Kriterienkatalog sind die typischen Anforderungen und Fragestellungen für die Prüfung aufgelistet. Die sachverständigen Stellen für Datenschutz haben sich hieran zu orientieren und müssen im Einzelfall entsprechend den tatsächlichen Gegebenheiten Anpassungen, Konkretisierungen und Erweiterungen vornehmen.

Im Fall von Re-Zertifizierungen ist der Antrag auf ein Datenschutz-Zertifikat mindestens drei Monate vor Ablauf der Akkreditierung bei dem BfDI zu stellen.

II. Kriterienkatalog

Der Kriterienkatalog gliedert sich nach den Kriteriengruppen:

1. Account-Eröffnung und Verwaltung eines De-Mail-Kontos
2. Postfach- und Versanddienst
3. Identitätsbestätigungsdienst
4. Verzeichnisdienst
5. Dokumentenablage
6. Rechte der betroffenen Person
7. Datenschutzmanagement

Die dem Nachweis zugrunde liegenden Begutachtungen müssen neben den allgemeinen datenschutzrechtlichen Anforderungen explizit auch die für De-Mail und ihre einzelnen Dienste einschlägigen Rechtsvorschriften berücksichtigen. Ausdrücklich müssen insbesondere die im De-Mail-Gesetz für die einzelnen Dienste genannten Anforderungen sowie die Einhaltung datenschutzrechtlicher Vorschriften bei der Umsetzung der technischen Anforderungen behandelt werden. Dies umfasst insbesondere Regelungen von DSGVO und BDSG.

Die Kriterien im Einzelnen sind in der Anlage (in Abschnitt III) aufgeführt.

[1] Es gilt der zum Zeitpunkt der Gutachtenabgabe gültige.

III. Gestaltung des Gutachtens

Für die Erstellung des Gutachtens ist die Anlage zu diesem Kriterienkatalog, in der die Anforderungen niedergelegt sind, verpflichtend als Vorlage zu verwenden (zu finden unter www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/DEMail/AnlageDeMailKriterienkatalog-3-0). Die dort aufgeführten Fragen sind ausführlich zu beantworten. Der jeweils geprüfte Sachverhalt muss hinreichend beschrieben werden. Darüber hinaus muss dargestellt werden, wie die geltenden Anforderungen realisiert wurden und ob es sich dabei um geeignete Maßnahmen zur Umsetzung handelt. Sofern insoweit Mängel identifiziert werden, muss geprüft werden, ob diese auf andere Art ausgeglichen werden (z. B. organisatorische oder technische Lösung).

Der dem Gutachten zugrundeliegende Prüfzeitpunkt des Gutachters beim Diensteanbieter darf nicht älter als drei Monate sein.

IV. Fachliche Eignung für die Gutachtenerstellung

Das Gutachten muss von einer vom Bund oder einem Land anerkannten oder öffentlich bestellten oder beliehenen sachverständigen Stelle für Datenschutz[2] erstellt werden. Da die Begutachtung sowohl rechtliche als auch technische Aspekte betrifft, muss die Anerkennung von sachverständigen Stellen für Datenschutz neben den üblichen Anforderungen an Zuverlässigkeit und Unabhängigkeit auch der fachlichen Eignung in den beiden Bereichen Recht und Technik explizit Rechnung tragen.

Ein Nachweis über die fachliche Eignung der sachverständigen Stelle ist dem Antrag auf Erteilung eines Datenschutz-Zertifikats beizufügen.

V. Veröffentlichung

Der Diensteanbieter veröffentlicht eine Kurzfassung des Nachweises zur Erfüllung der datenschutzrechtlichen Anforderungen (Kurzfassung des Gutachtens) in geeigneter Form (z. B. auf seiner Internetseite).

Wenn ein Diensteanbieter besondere, über die gesetzlichen Verpflichtungen hinausgehende Maßnahmen zur Gewährleistung eines überdurchschnittlich hohen Datenschutzniveaus ergreift, soll dies im Gutachten besonders erwähnt und in die zur Veröffentlichung bestimmte Kurzfassung des Gutachtens aufgenommen werden.

VI. Webadressen

(Stand: 17. März 2022)

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

https://www.bfdi.bund.de/DE/Home/home_node.html

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/

Der Beauftragte der Bundesregierung für Informationstechnik

https://www.cio.bund.de/Web/DE/Startseite/startseite_node.html

IT-Grundschutz

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

VII. Technische Richtlinien

TR-DE-Mail, BSI TR 01201

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/De-Mail/Technische-Richtlinien/technische-richtlinien_node.html

VIII. Abkürzungsverzeichnis

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
De-Mail-G	De-Mail-Gesetz
DSGVO	Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
GG	Grundgesetz
IP	Internet Protocol

[2] Hierzu zählen auch nach Artikel 43 DSGVO akkreditierte Zertifizierungsstellen.

ISP	Internet Service Provider
IT	Informationstechnik
SGB I	Erstes Buch Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TR	Technische Richtlinie
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VwVfG	Verwaltungsverfahrensgesetz

Anlage
zum De-Mail Kriterienkatalog Version 3.0

Gutachten für den Datenschutz-Nachweis
nach § 18 Absatz 3 Nummer 4 des De-Mail-Gesetzes
für
Name und Anschrift des begutachteten De-Mail-Diensteanbieters

Ersteller des Gutachtens:

Name und Adresse der sachverständigen Stelle für den Datenschutz

Name der Prüferin/des Prüfers

Datum des Gutachtens, gegebenenfalls Version

Unterschrift der Prüferin/des Prüfers

I. Erläuterung des Prüfablaufs

(Prüfgegenstand, Prüfgrundlagen, Prüfverfahren, Prüfzeitpunkt)

II. Zusammenfassung

(kurze Darstellung der wesentlichen Ergebnisse)

III. Kriterien im Einzelnen

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1	**Account-Eröffnung (§ 3 des De-Mail-Gesetzes) und Verwaltung eines De-Mail-Kontos**			
	Im Rahmen der Eröffnung eines De-Mail-Kontos ist bei der Prüfung zu trennen zwischen dem De-Mail-Konto und einem gegebenenfalls weiteren Kundenkonto, das zusätzlich für die Erbringung anderer Dienste oder Vertragsverhältnisse desselben Diensteanbieters betrieben wird (z. B. ISP, Web-Mail-Konten, Hosting etc.). Die Prüfung umfasst zwar grundsätzlich nur die Gestaltung und den Betrieb der De-Mail-Dienste, jedoch ist auf die Trennung der insoweit genutzten Daten gegenüber anderen Diensten des Diensteanbieters oder Dritter zu achten.			
1.1	Die personenbezogenen Daten, die für die Account-Eröffnung und Verwaltung eines De-Mail-Kontos verarbeitet werden, sind konkret zu benennen. Die Angaben sollen nach Datenkategorien gebündelt werden (z. B. Daten zur Identitätsfeststellung, Kontodaten, Kontaktdaten, Nutzungsdaten, Abrechnungsdaten, Protokolldaten, Dokumentationsdaten, Daten für Help-Desk). Hier sind keine Daten zu benennen, die im Rahmen des Postfach- und Versanddienstes, des Identitätsbestätigungsdienstes, des Verzeichnisdienstes und der Dokumentenablage anfallen. Die Daten zur Identitätsfeststellung sind getrennt nach natürlichen Personen, juristischen Personen oder Personengesellschaften oder öffentlichen Stellen und juristischen Personen als Mitglied des Vertretungsorgans/gesetzlicher Vertreter aufzuführen.			
	Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten			
1.2	Für alle in Nummer 1.1 genannten personenbezogenen Daten ist die Ermächtigungsgrundlage zu benennen und zu begutachten (z. B. De-Mail-Gesetz, DSGVO, TTDSG). Sofern die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung erfolgt, ist die Wirksamkeit jedes einzelnen Einwilligungsfalls in Nummer 1.3 zu begutachten[3].			
1.3	Für die Wirksamkeit einer Einwilligung sind folgende Punkte zu begutachten (Artikel 4 Nummer 11, Artikel 7 und 8 DSGVO): – Freiwilligkeit und Kopplungsverbot (ohne jeden Druck und Zwang). Die Nutzung von De-Mail darf nicht von der Verarbeitung nicht erforderlicher Daten abhängig gemacht werden. Hierzu sind unter anderem die Pflichtfelder zu begutachten. – vorherige umfassende Information in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache			

[3] Hinweise: Die Daten „Geschlecht“, „Anrede“, und „Titel“ gehören nicht zu den Daten, die im Rahmen der Erstidentifizierung nach § 3 Absatz 2 De-Mail-G zu verarbeiten sind. Gemäß § 3 Absatz 2 Nummer 2 De-Mail-G sind zur Identifizierung juristischer Personen „[...] Namen [...] der gesetzlichen Vertreter [...] zu erheben.“ Dies umfasst Vor- und Nachnamen und das Geburtsdatum der natürlichen Person, die als gesetzlicher Vertreter fungiert. Die Erhebung von Privatanschrift und Geburtsort gesetzlicher Vertreter ist dagegen nicht im De-Mail-Gesetz vorgesehen. Als Rechtsgrundlage für die Verarbeitung von Ordens- und Künstlernamen ist § 5 Absatz 1 Nummer 2 De-Mail-G heranzuziehen. Das Personalausweisgesetz stellt keine Ermächtigungsgrundlage für die Verarbeitung von personenbezogenen Daten im Rahmen von De-Mail dar.

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– Abgabe der Einwilligung nur für einen konkreten Fall – klare textliche Unterscheidung der Einwilligung von anderen Sachverhalten (Hervorhebungspflicht) – Belehrung über das Widerrufsrecht vor Abgabe der Einwilligung – Abgabe der Einwilligung vor der entsprechenden Datenverarbeitung – Einwilligung durch eine eindeutig bestätigende Handlung – Nachweispflicht über erfolgte Einwilligung – bei Minderjährigen unter 16 Jahren: Zustimmung des Trägers der elterlichen Verantwortung – jederzeitige Abrufmöglichkeit des Inhalts der Einwilligung durch die davon betroffene Person – Widerrufsmöglichkeit in einfacher Form entsprechend der Einwilligung			
	Erforderlichkeit/Zweckbindung/Zweckänderung			
1.4	Für alle in Nummer 1.1 genannten personenbezogenen Daten ist zu begutachten, ob diese Daten für die Erfüllung der Aufgaben des Dienste-anbieters im Rahmen der Account-Eröffnung und Verwaltung eines De-Mail-Kontos erforderlich sind und ob die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind [Grundsatz der Zweckbindung und der Erforderlichkeit (vgl. Artikel 5 DSGVO, § 15 Halbsatz 1 des De-Mail-Gesetzes)]. Die jeweiligen Zwecke sind zu nennen. Es ist zu beschreiben, wie sichergestellt wird, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden.			
1.5	Für die Rechtmäßigkeit einer Zweckänderung sind folgende Punkte zu begutachten (Artikel 6 Absatz 4 DSGVO, § 24 BDSG): – Ermächtigungsgrundlage für die Verarbeitung zu dem anderen Zweck (Rechtsvorschrift oder Einwilligung der nutzenden Person) – Vorliegen der Voraussetzungen nach Artikel 6 Absatz 4 DSGVO bzw. § 24 BDSG			
1.6	Erfolgt im Rahmen des Vertragszwecks eine Datenübermittlung, ist zu begutachten, ob die Daten, die nicht von der Zweckbindung erfasst werden, nicht übermittelt werden und ob der Empfänger auf die Zweckbindung der empfangenen Daten hingewiesen bzw. hierauf verpflichtet wird.			
1.7	Es ist zu begutachten, ob eine Kennzeichnung von Datensätzen bezüglich der entsprechenden Zwecke bzw. eine Trennung der Daten nach den verfolgten Zwecken und betroffenen Personen (Trennungsgebot) erfolgt.			
	Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit			
1.8	Nach Erreichen des Zwecks entfällt in der Regel die Erforderlichkeit, so dass die personenbezogenen Daten unverzüglich nach dem Stand der Technik sicher gelöscht werden müssen. Die Aufbewahrungsfristen für die in Nummer 1.1 genannten personenbezogenen Daten (vgl. unter anderem § 13 Absatz 2 des De-Mail-Gesetzes, §§ 9 und 10 TTDSG) sind zu nennen und zu begutachten. Es ist zu beschreiben, durch welche Maßnahmen die Einschränkung der Verarbeitung der personenbezogenen Daten zwischen Wegfall der Erforderlichkeit und der Löschfrist gewährleistet wird. Es ist zudem darzulegen, durch welche Prozesse bzw. Verfahren sichergestellt wird, dass die Daten nach Wegfall der Erforderlichkeit und Ablauf der Aufbewahrungsfristen tatsächlich nach dem Stand der Technik sicher gelöscht werden. In die Begutachtung sind auch Sicherheitskopien und Backups einzubeziehen.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Verarbeitung im Auftrag			
1.9	Für alle in Nummer 1.1 genannten personenbezogenen Daten ist zu begutachten, ob diese durch einen Auftragsverarbeiter verarbeitet werden. Der jeweilige Auftragnehmer sowie die von diesem zu verarbeitenden Daten sind zu benennen. Sofern Auftragsverarbeitung erfolgt, ist die Rechtmäßigkeit jeder einzelnen Auftragsverarbeitung in Nummer 1.10 zu begutachten.			
1.10	Für die Rechtmäßigkeit einer Verarbeitung im Auftrag sind folgende Punkte zu begutachten: – Ist eine Verarbeitung der Daten durch einen Auftragsverarbeiter zulässig? Dies ist nicht der Fall, wenn bei Daten von Berufsgeheimnisträgern durch die Auftragsverarbeitung vom Geheimnisträger ein fremdes Geheimnis im Sinne des § 203 StGB offenbart wird. Zudem darf der Auftragnehmer kein Eigeninteresse an der Datenverarbeitung besitzen. Er darf die personenbezogenen Daten der nutzenden Person nicht für eigene Zwecke verarbeiten. – Werden die Vorgaben des Artikels 28 DSGVO eingehalten? Jede einzelne Vorgabe ist zu prüfen (z. B. Auswahl des Auftragsverarbeiters, Vertrag mit dem Auftragsverarbeiter, Einsatz von Subunternehmern, Dokumentation der Maßnahmen nach Artikel 32 DSGVO, Durchführung von Kontrollen durch den Diensteanbieter, …). – Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf Weisung des Diensteanbieters (Artikel 29 DSGVO)? – Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO? – Welche Meldeprozesse bestehen mit dem Auftragsverarbeiter für den Fall von Datenschutzverstößen nach Artikel 33 Absatz 2 DSGVO? – Erfüllt der Auftragsverarbeiter die Anforderungen nach dem De-Mail-Gesetz? Wie wird dies sichergestellt? – Hat der Auftragsverarbeiter seinen Sitz außerhalb des EU-/EWR-Raums? Wenn ja, werden die zusätzlichen Anforderungen nach Artikel 44 ff. DSGVO (siehe auch Schrems-II-Urteil) erfüllt? Sofern der Auftragnehmer Unterauftragnehmer beauftragt, ist die Anforderung auch bezogen auf die Unterauftragnehmer zu begutachten. – Werden besondere Kategorien von personenbezogenen Daten vom Auftragsverarbeiter verarbeitet? Wenn ja, werden die insoweit einschlägigen rechtlichen Vorgaben beachtet (vgl. Artikel 9 DSGVO, § 22 BDSG)?			
	Aufklärungs- und Informationspflichten (§ 9 des De-Mail-Gesetzes)			
1.11	Der Nutzer ist vor der erstmaligen Nutzung des De-Mail-Kontos gemäß § 9 Absatz 1 des De-Mail-Gesetzes über die Rechtsfolgen und Kosten der Nutzung zu informieren. Dies umfasst nach § 9 Absatz 1 Satz 1 des De-Mail-Gesetzes alle Funktionen von De-Mail wie den Postfach- und Versanddienst, den Verzeichnisdienst, die Dokumentenablage, die Sperrung und Auflösung des Kontos sowie Informationen im Falle der Einstellung der Tätigkeit des Diensteanbieters, der Vertragsbeendigung und der Einsichtnahme in die beim Diensteanbieter vorhandenen personenbezogenen Daten. Besonders relevant sind Informationen: – über die Rechtsfolgen und Kosten der Nutzung des De-Mail-Dienstes (§ 9 Absatz 1 Satz 1 des De-Mail-Gesetzes), – über Maßnahmen, die notwendig sind, um einen unbefugten Zugriff auf das De-Mail-Konto zu verhindern (§ 9 Absatz 1 Satz 1 des De-Mail-Gesetzes), – über die Möglichkeit und Bedeutung einer sicheren Anmeldung (§ 9 Absatz 1 Satz 2 Nummer 1 des De-Mail-Gesetzes),			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– dass ein Zugang zum De-Mail-Konto ohne sichere Anmeldung (d. h. nur mithilfe eines Sicherungsmittels) nicht den gleichen Schutz bietet wie mit einer sicheren Anmeldung (§ 9 Absatz 1 Satz 2 Nummer 1 des De-Mail-Gesetzes), – über den Inhalt und die Bedeutung der Transportverschlüsselung nach § 5 Absatz 3 Satz 2 des De-Mail-Gesetzes sowie der Verschlüsselung nach § 4 Absatz 3 des De-Mail-Gesetzes sowie über die Unterschiede dieser Verschlüsselungen zu einer Ende-zu-Ende-Verschlüsselung nach § 5 Absatz 3 Satz 3 des De-Mail-Gesetzes (§ 9 Absatz 1 Satz 2 Nummer 2 des De-Mail-Gesetzes) und – wie mit Schadsoftware behafteten De-Mail-Nachrichten umgegangen wird (§ 9 Absatz 1 Satz 3 des De-Mail-Gesetzes). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Dabei ist auf jede einzelne Informationspflicht einzugehen.			
1.12	Eine Zulassung der erstmaligen Nutzung des De-Mail-Kontos darf nach § 9 Absatz 2 des De-Mail-Gesetzes erst erfolgen, wenn der Nutzer die erforderlichen Informationen in Textform erhalten und in Textform bestätigt hat, dass er die Informationen erhalten und zur Kenntnis genommen hat. Zur Einhaltung der Textform muss die Erklärung in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben werden, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden (§ 126 Buchstabe b BGB). Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
	Weitere Informationspflichten (§ 9 Absatz 3 des De-Mail-Gesetzes)			
1.13	Nach Artikel 13 DSGVO hat der Diensteanbieter, sobald er personenbezogene Daten bei der nutzenden Person erhebt, dieser zum Zeitpunkt der Erhebung bestimmte Informationen mitzuteilen: 1. den Namen und die Kontaktdaten des Diensteanbieters 2. die Kontaktdaten des Datenschutzbeauftragten 3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung 4. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f DSGVO beruht, die berechtigten Interessen, die von dem Diensteanbieter oder einem Dritten verfolgt werden 5. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten 6. gegebenenfalls die Absicht des Diensteanbieters, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln sowie das Vorhandensein oder Fehlen entsprechender Garantien oder eines Angemessenheitsbeschlusses 7. die Speicherdauer 8. das Bestehen von Betroffenenrechten 9. die Pflicht zur Bereitstellung der Daten 10. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling. Bei Zweckänderung ergeben sich erneute Informationspflichten (Artikel 13 Absatz 3 DSGVO). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Dabei ist auf jede einzelne Informationspflicht einzugehen. Zusätzlich ist zu betrachten, ob die Information in korrekter Form und unentgeltlich erfolgt (Artikel 12 Absatz 1 und 5 DSGVO). § 29 Absatz 2 und § 32 BDSG sind bei der Begutachtung zu berücksichtigen.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1.14	Nach Artikel 14 DSGVO ergeben sich für den Diensteanbieter, sofern er personenbezogene Daten nicht direkt bei der nutzenden Person erhebt, bestimmte weitere Informationspflichten. Es ist zu begutachten, ob solche Datenerhebungen erfolgen und wenn ja, wie die Informationspflichten nach Artikel 14 DSGVO unter Berücksichtigung von Artikel 12 Absatz 1 und 5 DSGVO umgesetzt werden. § 29 Absatz 1 Satz 1 und § 33 BDSG sind bei der Begutachtung zu berücksichtigen.			
1.15	Weitere Informationspflichten gegenüber der nutzenden Person gibt es gemäß allgemeinem Vertragsrecht, insbesondere wenn tatsächliche oder rechtliche Änderungen im laufenden Betrieb bevorstehen. Hier ist zum Beispiel an die Möglichkeit zu denken, dass die nutzende Person nach § 7 Absatz 3 des De-Mail-Gesetzes durch einen geeigneten Zusatz zu seinen im Verzeichnisdienst veröffentlichen Daten gegenüber Behörden den Zugang nach § 3 a Absatz 1 VwVfG, § 36 a Absatz 1 SGB I oder des § 87 a Absatz 1 Satz 1 AO eröffnen kann. Die nutzende Person muss über die Möglichkeit und die Rechtsfolgen der Zugangseröffnung aufgeklärt werden. Weiter muss die nutzende Person darüber informiert werden, dass die De-Mail in den Fällen der § 3 a Absatz 2 Satz 4 Nummer 2 und 3 VwVfG, § 36 Absatz 2 Satz 4 Nummer 2 und 3 SGB I, § 87 a Absatz 3 Nummer 2 und Absatz 4 Satz 3 AO schriftformersetzend eingesetzt werden kann. Es ist zu begutachten, wie diese Informationspflichten umgesetzt werden.			
1.16	Ist der Nutzer zur Sperrung des Zugangs zum De-Mail-Konto berechtigt, so ist ihm eine Rufnummer bekannt zu geben, unter der die Sperrung des Zugangs unverzüglich veranlasst werden kann (§ 10 Absatz 1 Satz 3 des De-Mail-Gesetzes). Es ist zu begutachten, wie bzw. an welcher Stelle diese Bekanntgabe erfolgt.			
1.17	Der Diensteanbieter soll die nutzende Person über die Funktionsweise der qualifizierten elektronischen Signatur in allgemein verständlicher Form unterrichten und entsprechende Dokumente zum jederzeitigen Abruf vorhalten. Es ist zu begutachten, wie bzw. an welcher Stelle diese Unterrichtung erfolgt.			
	Kopplungsverbot			
1.18	Die Eröffnung eines De-Mail-Kontos bzw. die Anmeldung zu einem De-Mail-Dienst darf nicht von einer Einwilligung in die Nutzung der Daten für andere als für Zwecke des jeweiligen De-Mail-Dienstes abhängig gemacht werden (z. B. Adresshandel oder Werbung). In diesem Rahmen ist auch zu prüfen, ob kein Zwang zur Nutzung anderer Dienste des Diensteanbieters z. B. eines E-Mail-Dienstes, besteht. Es ist zu begutachten, ob diese Anforderung eingehalten wird.			
1.19	Die Eröffnung eines Kontos darf nicht von einer Veröffentlichung im Verzeichnisdienst abhängig gemacht werden (§ 7 Absatz 1 Satz 2 des De-Mail-Gesetzes). Es ist zu begutachten, ob diese Anforderung eingehalten wird.			
	Verfahren zur Identitätsfeststellung			
1.20	Es ist zu begutachten, wie die Identitätsangaben, d. h. die Angaben nach § 3 Absatz 2 des De-Mail-Gesetzes, durch den Diensteanbieter überprüft werden. Hierbei soll auch dargelegt werden, welche in § 3 Absatz 3 genannten Überprüfungsmöglichkeiten genutzt werden.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1.21	Wenn sonstige geeignete technische Verfahren mit gleichwertiger Sicherheit im Sinne des § 3 Absatz 3 Satz 1 Nummer 1 Buchstabe e des De-Mail-Gesetzes angewendet werden, sind diese ausführlich unter Beachtung der nachfolgenden Ausführungen zu beschreiben und zu begutachten. Beim Einsatz von geeigneten technischen Verfahren mit gleichwertiger Sicherheit gemäß § 3 Absatz 3 Satz 1 Nummer 1 Buchstabe e des De-Mail-Gesetzes kann es erforderlich sein, zusätzlich zu den in § 3 Absatz 2 Satz 2 Nummer 1 des De-Mail-Gesetzes genannten Daten vorübergehend weitere Daten zu erheben, um die gleichwertige Sicherheit zur Identifizierung mittels Dokumenten nach § 3 Absatz 3 Satz 1 Nummer 1 Buchstabe a des De-Mail-Gesetzes herzustellen. Dazu kann es ebenfalls erforderlich sein, vollständige Kopien der Ausweise vorübergehend anzufertigen. Die Erforderlichkeit, zusätzliche Daten zur Herstellung der gleichwertigen Sicherheit zu erheben, ist im Einzelfall darzulegen. Da der Zweck in der Herstellung der gleichwertigen Sicherheit liegt, entfällt mit der Zweckerreichung (d. h. Abschluss des Identifizierungsprozesses) der Grund für die Speicherung und Verarbeitung der entsprechenden Daten, so dass sie danach unverzüglich nach dem Stand der Technik sicher zu löschen sind.			
1.22	Wenn die Identitätsfeststellung durch einen Dienstleister erfolgt, sind diese zu benennen und deren Verfahren zu begutachten.			
1.23	Werden im Rahmen der Identitätsfeststellung nach § 3 Absatz 3 des De-Mail-Gesetzes vom Diensteanbieter oder seinem Dienstleister Ausweise kopiert, ist die Rechtmäßigkeit unter Berücksichtigung der folgenden Punkte zu begutachten: – Wie wird sichergestellt, dass die Ausweiskopien sicher aufbewahrt und übermittelt werden? – Wie wird sichergestellt, dass die Ausweiskopien unverzüglich nach der Feststellung der Identität vernichtet werden? – Wie wird sichergestellt, dass nicht erforderliche Daten auf den Ausweiskopien nicht erkennbar sind, also geschwärzt werden?			
1.24	Wenn für die Identitätsfeststellung bereits früher erhobene Daten gemäß § 3 Absatz 3 Satz 4 des De-Mail-Gesetzes verwendet werden, ist zu begutachten, wie sichergestellt wird, dass nur die für die Identitätsfeststellung notwendigen Daten erhoben werden, dass die hierfür erforderlichen Einwilligungen der nutzenden Person in die Verwendung dieser Daten vorliegen und dass die Einwilligungen die Anforderungen der Artikel 7 und 8 DSGVO erfüllen.			
1.25	Der Diensteanbieter hat nach der Freischaltung des De-Mail-Kontos eines Nutzers die Richtigkeit der zu dem Nutzer gespeicherten Identitätsdaten sicherzustellen. Er hat die gespeicherten Identitätsdaten in angemessenen zeitlichen Abständen auf ihre Richtigkeit zu überprüfen und soweit erforderlich zu berichtigen (§ 3 Absatz 5 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderungen umgesetzt werden. Dabei sind die einschlägigen Prozesse zu beschreiben und ist zwischen natürlichen und juristischen Personen zu unterscheiden.			
	Weitere Anforderungen (§ 3 und § 4 des De-Mail-Gesetzes)			
1.26	Es ist zu begutachten, wie sichergestellt wird, dass ein De-Mail-Konto nur genau einer Person zugeordnet ist (§ 3 Absatz 1 Satz 2 des De-Mail-Gesetzes).			
1.27	Es ist zu begutachten, wie sichergestellt wird, dass der Nutzer vor Freischaltung des De-Mail-Kontos eindeutig identifiziert worden ist (§ 3 Absatz 4 Satz 2 Nummer 1 des De-Mail-Gesetzes).			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1.28	Der Diensteanbieter muss vor Freischaltung des De-Mail-Kontos dem Nutzer dessen für die Erstanmeldung notwendigen Anmeldedaten auf geeignetem Wege übermitteln (§ 3 Absatz 4 Satz 2 Nummer 2 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird. Dabei ist auch der Weg der Datenübermittlung zu betrachten.			
1.29	Der Diensteanbieter muss vor Freischaltung des De-Mail-Kontos das Einverständnis des Nutzers in die Prüfung seiner Nachrichten auf Schadsoftware einholen (§ 3 Absatz 4 Satz 2 Nummer 4 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird. Dabei ist auch die Art und Weise sowie der Zeitpunkt der Einholung des Einverständnisses zu betrachten.			
1.30	Das De-Mail-Konto darf erst freigeschaltet werden, nachdem der Nutzer im Rahmen einer Erstanmeldung nachgewiesen hat, dass er die Anmeldedaten erfolgreich nutzen konnte (§ 3 Absatz 4 Satz 2 Nummer 5 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird. Es ist auch zu betrachten, in welcher Art und Weise der Nachweis erfolgt.			
1.31	Für die Anmeldung muss ein geeignetes Verfahren eingesetzt werden (§ 4 Absatz 1 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird. Es ist auch zu betrachten, welche Anmeldevarianten für die nutzende Person möglich sind.			
1.32	Der Diensteanbieter muss dem Nutzer den Zugang zu seinem De-Mail-Konto und den einzelnen Diensten mit einer sicheren Anmeldung oder auf Verlangen des Nutzers auch ohne eine solche sichere Anmeldung ermöglichen (§ 4 Absatz 1 Satz 1 des De-Mail-Gesetzes). Der Nutzer kann verlangen, dass der Zugang zu seinem De-Mail-Konto ausschließlich mit einer sicheren Anmeldung möglich sein soll. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
1.33	Der Nutzer muss zwischen mindestens zwei Verfahren zur sicheren Anmeldung wählen können (§ 4 Absatz 2 des De-Mail-Gesetzes). Ein Verfahren muss unter Nutzung des elektronischen Identitätsnachweises nach § 18 Personalausweisgesetz angeboten werden. Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
1.34	Die Kommunikationsverbindung zwischen dem Nutzer und dem De-Mail-Konto muss verschlüsselt erfolgen (§ 4 Absatz 3 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
	Sperrung eines De-Mail-Kontos			
1.35	Der Diensteanbieter muss in folgenden Fällen das De-Mail-Konto vollständig sperren: – unverzüglich auf Verlangen der nutzenden Person (§ 10 Absatz 1 Satz 1 Nummer 1 des De-Mail-Gesetzes). – wenn Tatsachen die Annahme rechtfertigen, dass die zur eindeutigen Identifizierung der nutzenden Person beim Diensteanbieter gespeicherten Daten nicht ausreichend fälschungssicher sind oder dass die sichere Anmeldung gemäß § 4 des De-Mail-Gesetzes Mängel aufweist (§ 10 Absatz 1 Satz 1 Nummer 2 des De-Mail-Gesetzes).			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– wenn das BSI die Sperrung eines De-Mail-Kontos anordnet (§ 10 Absatz 1 Satz 1 Nummer 3 des De-Mail-Gesetzes). – wenn die Voraussetzungen eines vertraglich zwischen dem Dienste-anbieter und der nutzenden Person vereinbarten Sperrgrundes vorliegen (§ 10 Absatz 1 Satz 1 Nummer 4 des De-Mail-Gesetzes). Bei Eintritt eines vertraglich vereinbarten Sperrgrundes muss der Abruf von Nachrichten möglich bleiben (§ 10 Absatz 1 Satz 2 des De-Mail-Gesetzes), sofern dieses nicht ausgeschlossen wurde. Der Diensteanbieter muss sich vor einer vollständigen Sperrung nach § 10 Absatz 1 des De-Mail-Gesetzes auf geeignete Weise von der Identität des zur Sperrung berechtigten Nutzers überzeugen (§ 10 Absatz 5 des De-Mail-Gesetzes). Nachrichten an ein vollständig gesperrtes De-Mail-Konto dürfen nicht in den Eingang des De-Mail-Postfaches gelangen. Der Absender ist hierüber zu informieren (§ 10 Absatz 6 des De-Mail-Gesetzes). Bei vollständiger Sperrung des De-Mail-Kontos auf Veranlassung des Diensteanbieters oder des BSI ist der Nutzer entsprechend § 10 Absatz 7 De-Mail-G zu informieren. Der Diensteanbieter hat dem Nutzer nach Wegfall des Sperrgrundes den Zugang zum De-Mail-Konto erneut zu gewähren (§ 10 Absatz 3 des De-Mail-Gesetzes). Es ist zu begutachten, in welcher Art und Weise diese Anforderungen umgesetzt werden.			
1.36	Bezüglich der Zugangssperre zu einem De-Mail-Konto sind folgende Fragestellungen zu begutachten: – Wie wird eine Zugangssperre im Fall einer mehrfachen Falscheingabe der Authentisierungsdaten gewährleistet? Wie erfolgt die Entsperrung? – Wird die Zugangssperre in Form des Authentisierungsniveaus der sicheren Anmeldung nach § 4 Absatz 1 De-Mail-Gesetz umgesetzt?			
1.37	Es ist zu begutachten, ob die Möglichkeit einer Sperrung im Sinne einer Nutzungseinschränkung der verschiedenen De-Mail-Dienste existiert. Falls dies bejaht wird, ist darzulegen, ob im Fall der Nutzungseinschränkung der Empfang von Nachrichten und das Herunterladen von Dokumenten weiterhin möglich sind.			
	Auflösen eines De-Mail-Kontos und Vertragsbeendigung (§ 10 Absatz 4 bis 7, § 12 des De-Mail-Gesetzes)			
1.38	Der Diensteanbieter muss ein De-Mail-Konto unverzüglich auflösen, wenn der Nutzer es verlangt oder das BSI die Auflösung anordnet (§ 10 Absatz 4 Satz 1 des De-Mail-Gesetzes). Der Diensteanbieter muss sich vor der Auflösung nach § 10 Absatz 5 des De-Mail-Gesetzes auf geeignete Weise von der Identität der zur Auflösung berechtigten nutzenden Person überzeugen. Nachrichten an ein gesperrtes oder aufgelöstes De-Mail-Konto dürfen nicht in den Eingang des De-Mail-Postfaches gelangen. Der Absender ist hierüber zu informieren (§ 10 Absatz 6 des De-Mail-Gesetzes). Bei Auflösung des De-Mail-Kontos auf Veranlassung des Diensteanbieters oder des BSI ist die nutzende Person entsprechend § 10 Absatz 7 des De-Mail-Gesetzes zu informieren. Es ist zu begutachten, in welcher Art und Weise diese Anforderungen umgesetzt werden.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1.39	Der Diensteanbieter muss dem Nutzer für einen Zeitraum von drei Monaten nach Vertragsende den Zugriff auf die im Postfach und in der Dokumentenablage abgelegten Daten ermöglichen. Der Nutzer muss mindestens einen Monat vor Löschung hierauf in Textform hingewiesen werden (§ 12 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
1.40	Eine Pseudonym-De-Mail-Adresse ist, nachdem sie einem De-Mail-Konto zugeordnet war und die Zuordnung aufgehoben wurde, für eine Verwendung durch eine andere natürliche Person zu sperren und darf auch keinem anderen De-Mail-Konto zugeordnet werden. Es ist zu begutachten, in welcher Art und Weise diese Anforderung umgesetzt ist. Hierbei sollte auch auf die Dauer der Sperrung eingegangen werden.			
1.41	Es ist zu begutachten, ob eine Möglichkeit angeboten wird, eine Pseudonym-De-Mail-Adresse nach einer bestimmten Frist wieder freizugeben.			
	Dokumentation			
1.42	Nach § 13 Absatz 1 des De-Mail-Gesetzes ist die Eröffnung des De-Mail-Kontos, die Änderung der Daten, die hinsichtlich der Führung eines De-Mail-Kontos relevant sind, sowie jede Änderung hinsichtlich des Zustands eines De-Mail-Kontos zu dokumentieren. Die Dokumentation hat so zu erfolgen, dass die Authentizität und Integrität der Daten jederzeit nachprüfbar sind. Es ist zu begutachten, durch welche Prozesse diese Anforderungen umgesetzt werden.			
	Fernmeldegeheimnis			

1.43	Es ist zu begutachten, ob das Fernmeldegeheimnis nach § 3 TTDSG gewährleistet ist. Zu begutachten ist neben der Vertraulichkeit der Kommunikation auch die Einhaltung der gesetzlichen Grenzen für staatliche Überwachungsmaßnahmen unter anderem nach den §§ 170 ff TKG, § 5 und § 8 des Artikel-10-Gesetzes, § 100 b StPO sowie die Gewährleistung des vom Bundesverfassungsgericht 2008 formulierten Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (Urteil vom 27. Februar 2008 – 1 BvR 370/07; 1 BvR 595/07). Das Gutachten soll folgende Punkte umfassen:
	– Verpflichtung der Mitarbeiter sowohl des Diensteanbieters als auch gegebenenfalls von Auftragnehmern auf das Fernmeldegeheimnis
	– Erforderlichkeit einer internen Regelung von Zugriffs- bzw. Kontrollrechten betreffend Verkehrs- und Protokolldaten
	– Technischer Schutz (vor Viren und anderer Malware)
	– Einhaltung der Bestimmungen der §§ 170 ff. TKG mit den Vorgaben der Bundesnetzagentur, der TKÜV sowie der einschlägigen Vorschriften des achten Abschnitts der StPO
	– Bereitstellung entsprechender Schnittstellen und Prozesse:
	– Dabei ist auch zu betrachten:
	  – Wie wird sichergestellt, dass die Zugriffsmöglichkeiten des Diensteanbieters auf De-Mails und Inhalte der Dokumentenablage auf die Umsetzung dieser Vorgaben beschränkt sind?
	  – Welche Prozesse zur Überprüfung der Berechtigung entsprechender Kontrollen durch berechtigte Stellen, insbesondere nach der StPO, sind vorhanden?
	  – Wie wird die nachträgliche Unterrichtungspflicht eingehalten?
	  – Welche Maßnahmen zur Gewährleistung der Integrität der Daten werden umgesetzt?
	  – Wie werden die Verkehrs-, Inhalts- und Protokolldaten gegen unberechtigte interne und externe Zugriffe geschützt?			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Auskunftsanspruch von öffentlichen Stellen			
1.44	Manuelle Auskünfte an ersuchende öffentliche Stellen (z. B. Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes) dürfen nur nach Maßgabe des § 174 TKG im Einzelfall erteilt werden, sofern die ersuchende Stelle die gesetzliche Bestimmung hierfür angibt. Es ist zu begutachten, wie die Anforderungen des § 174 TKG umgesetzt werden.			
1.45	§ 173 TKG regelt das automatisierte Auskunftsverfahren. Es ist zu begutachten, ob beim Diensteanbieter ein automatisertes Abrufverfahren eingerichtet ist und in welcher Art und Weise die Anforderungen des § 173 TKG umgesetzt werden.			
	Auskunftsanspruch (§ 16 des De-Mail-Gesetzes)			
1.46	Der Diensteanbieter muss Auskunft über Name und Anschrift einer nutzenden Person an private Dritte bzw. an öffentliche Stellen erteilen, sofern die in § 16 Absatz 1 des De-Mail-Gesetzes genannten Voraussetzungen erfüllt sind. Vor Erteilung einer Auskunft muss der Diensteanbieter die Einhaltung dieser Vorgaben überprüfen. Dies beinhaltet auch eine Überprüfung der eingereichten Unterlagen (§ 16 Absatz 2 Satz 1 des De-Mail-Gesetzes). Die nutzende Person muss vom Diensteanbieter unverzüglich über das Auskunftsersuchen unter Benennung des Dritten informiert werden und es muss der nutzenden Person Gelegenheit zur Stellungnahme gewährt werden, soweit dies die Verfolgung des Rechtsanspruchs des Dritten nicht im Einzelfall gefährdet (§ 16 Absatz 2 Satz 2 des De-Mail-Gesetzes). Es ist zu begutachten, in welcher Art und Weise diese Anforderungen umgesetzt werden. Es sind auch die Prozesse bei Anfragen nach Pseudonym-De-Mail-Adressen einschließlich der Prüfung der Berechtigung zur Aufdeckung zu betrachten.			
1.47	Der Diensteanbieter muss die Auskunftserteilung nach § 16 Absatz 1 des De-Mail-Gesetzes dokumentieren (Antrag zur Auskunftserteilung, Angabe des Dritten, Identitätsdaten des Mitarbeiters etc.) und die nutzende Person von der Erteilung der Auskunft zu informieren (§ 16 Absatz 5 Satz 1 des De-Mail-Gesetzes). Die Dokumentation der Auskunftserteilung muss der Diensteanbieter drei Jahre aufbewahren und danach nach dem Stand der Technik sicher löschen bzw. vernichten. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
	Help-Desk			
1.48	Die nutzenden Personen, die den Help-Desk in Anspruch nehmen, sind über die hierbei gegebenenfalls erfolgte Datenverarbeitung (z. B. Speicherung) zu informieren. Es ist zu begutachten, ob diese Anforderung erfüllt ist.			
1.49	Der Zugriff der Help-Desk-Mitarbeiter ist auf die für ihre definierte Tätigkeit erforderlichen Daten zu beschränken. Es ist zu begutachten, wie diese Anforderung umgesetzt ist.			
1.50	Die Authentifizierung des Anfragenden muss in geeigneter Art und Weise erfolgen. Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
1.51	Maßnahmen oder Änderungen durch die Help-Desk-Mitarbeiter sind im Rahmen der Erforderlichkeit zu dokumentieren. Hierbei darf keine vollständige Überwachung der Mitarbeitertätigkeit erfolgen. Es ist zu begutachten, wie diese Anforderungen umgesetzt sind. Dabei ist auch die Dauer der Speicherung dieser Dokumentation zu betrachten.			
1.52	Die vom Help-Desk erhobenen Daten sind von denen des De-Mail-Dienstes zu trennen. Es ist zu begutachten, wie diese Anforderung umgesetzt ist.			
	Standortbestimmung			
1.53	Eine Geolokalisierung zu Statistikzwecken oder zur Profilerstellung auf Basis von IP-Adressen darf nur anhand einer anonymisierten IP-Adresse erfolgen. Standortdaten dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die nutzende Person dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. Im Übrigen sind die Vorgaben von § 13 TTDSG zu beachten, der die datenschutzgerechte Verarbeitung und Nutzung von Standortdaten regelt. Wenn keine Standortdaten verarbeitet werden, soll die nutzende Person an geeigneter Stelle darauf hingewiesen werden, dass keine Standortdaten verarbeitet werden bzw. dass IP-Adressen jedenfalls nicht für derartige Zwecke gespeichert werden. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
	Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung			
1.54	Der Diensteanbieter hat nach Artikel 32 Absatz 2 DSGVO durch technische und organisatorische Maßnahmen die Sicherheit der Verarbeitung der in Nummer 1.1 genannten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen betreffen unter anderem Folgendes: – die Pseudonymisierung und Verschlüsselung personenbezogener Daten, – die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, – die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen und – ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Es ist zu begutachten, ob die Sicherheit der Verarbeitung gewährleistet ist. Dabei sind auch zu betrachten: – Zutritts- und Zugangskontrolle zu allen IT-Einrichtungen – Kopplung mit weiteren technischen Systemen, z. B. Strom- und Netzversorgung – Art und Qualität der Verschlüsselung – Trennung von Daten über die Nutzung von De-Mail-Diensten von Daten über andere Nutzungen beim Diensteanbieter – Zugriffskontrolle (Zugriffe der nutzenden Person, Zugriffsmöglichkeiten der Diensteanbieter auf Konfigurationsdaten)			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Es ist davon auszugehen, dass die Sicherheit der Verarbeitung gewährleistet ist, wenn ein Testat die Konformität zu den Prüfgrundlagen BSI TR-01201, Teil 1 – Modul IT-Basisinfrastruktur, BSI TR-01201, Teil 2 – Modul Accountmanagement bestätigt und das Zertifikat zu BSI TR-01201 Teil 6 – Modul Informationssicherheit vorgelegt wird. Diese Nachweise dürfen zum Zeitpunkt des Gutachtens nicht älter als drei Monate sein.			
	Protokollierung			
1.55	Die im Rahmen der Account-Eröffnung und Verwaltung eines De-Mail-Kontos erfolgten Protokollierungen sind zu benennen und zu begutachten. Es sind hierbei auch die Rechtsgrundlage, Erforderlichkeit, Zweckbindung, Speicherdauer, Löschfristen, Löschverfahren, Revisionssicherheit und Überprüfungsmöglichkeiten zu betrachten, sofern die Protokollierungen personenbezogene Daten beinhalten. Es ist zu beachten, dass sowohl dynamische IP-Adressen mit Zeitstempel als auch statische IP-Adressen als personenbezogene Daten anzusehen sind. Bei der Begutachtung soll zwischen Protokollierung der Nutzeraktivitäten und Protokollierung der internen Aktivitäten (Administratorentätigkeit, Help-Desk-Tätigkeit etc.) unterschieden werden. Protokolle, die die internen Aktivitäten (wann, durch wen und in welcher Weise Daten gespeichert oder verändert) speichern, müssen in der Regel nach zehn Jahren nach dem Stand der Technik sicher gelöscht werden.			
2	**Postfach- und Versanddienst (§ 5 des De-Mail-Gesetzes)**			
2.1	Die personenbezogenen Daten, die für den Postfach- und Versanddienst verarbeitet werden, sind konkret zu benennen. Die Angaben sollen nach Datenkategorien gebündelt werden (z. B. Kundendaten, Nutzungsdaten, Verkehrsdaten, Protokolldaten).			
	Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten			
2.2	Für alle in Nummer 2.1 genannten personenbezogenen Daten ist die Ermächtigungsgrundlage zu benennen und zu begutachten. Sofern die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung erfolgt, ist die Wirksamkeit jedes einzelnen Einwilligungsfalls in Nummer 2.3 zu begutachten.			
2.3	Für die Wirksamkeit einer Einwilligung sind folgende Punkte zu begutachten (Artikel 4 Nummer 11, Artikel 7 und 8 DSGVO): – Freiwilligkeit und Kopplungsverbot (ohne jeden Druck und Zwang) – vorherige umfassende Information in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache – Abgabe der Einwilligung nur für einen konkreten Fall – klare textliche Unterscheidung der Einwilligung von anderen Sachverhalten (Hervorhebungspflicht) – Belehrung über das Widerrufsrecht vor Abgabe der Einwilligung – Abgabe der Einwilligung vor der entsprechenden Datenverarbeitung – Einwilligung durch eine eindeutig bestätigende Handlung – Nachweispflicht über erfolgte Einwilligung – bei Minderjährigen unter 16 Jahren: Zustimmung des Trägers der elterlichen Verantwortung – jederzeitige Abrufmöglichkeit des Inhalts der Einwilligung durch die davon betroffene Person – Widerrufsmöglichkeit in einfacher Form entsprechend der Einwilligung			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Erforderlichkeit/Zweckbindung/Zweckänderung			
2.4	Für alle in Nummer 2.1 genannten personenbezogenen Daten ist zu begutachten, ob diese Daten für die Erfüllung der Aufgaben des Dienste-anbieters im Rahmen des Postfach- und Versanddienstes erforderlich sind und ob die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind [Grundsatz der Zweckbindung und der Erforderlichkeit (vgl. Artikel 6 DSGVO, § 15 Halbsatz 1 des De-Mail-Gesetzes)]. Die jeweiligen Zwecke sind zu nennen. Es ist zu beschreiben, wie sichergestellt wird, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden.			
2.5	Für die Rechtmäßigkeit einer Zweckänderung sind folgende Punkte zu begutachten (Artikel 6 Absatz 4 DSGVO, § 24 BDSG): – Ermächtigungsgrundlage für die Verarbeitung zu dem anderen Zweck (Rechtsvorschrift oder Einwilligung der nutzenden Person) oder – Vorliegen der Voraussetzungen nach Artikel 6 Absatz 4 DSGVO bzw. § 24 BDSG			
2.6	Erfolgt im Rahmen des Vertragszwecks eine Datenübermittlung, ist zu begutachten, ob die Daten, die nicht von der Zweckbindung erfasst werden, nicht übermittelt werden und ob der Empfänger auf die Zweck-bindung der empfangenen Daten hingewiesen bzw. hierauf verpflichtet wird.			
2.7	Es ist zu begutachten, ob eine Kennzeichnung von Datensätzen bezüglich der entsprechenden Zwecke bzw. eine Trennung der Daten nach den verfolgten Zwecken und betroffenen Personen (Trennungsgebot) erfolgt.			
	Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit			
2.8	Nach Erreichen des Zwecks entfällt in der Regel die Erforderlichkeit und die personenbezogenen Daten müssen unverzüglich nach dem Stand der Technik sicher gelöscht werden. Die Aufbewahrungsfristen für die in Nummer 2.1 genannten personenbe-zogenen Daten (vgl. unter anderem § 13 Absatz 2 des De-Mail-Gesetzes, §§ 9 und 10 TTDSG) sind zu nennen und zu begutachten. Es ist zu beschreiben, durch welche Maßnahmen die Einschränkung der Verarbeitung der personenbezogenen Daten zwischen Wegfall der Er-forderlichkeit und der Löschfrist gewährleistet wird. Es ist zudem darzulegen, durch welche Prozesse bzw. Verfahren sicher-gestellt wird, dass die Daten nach Wegfall der Erforderlichkeit und Ablauf der Aufbewahrungsfristen tatsächlich nach dem Stand der Technik sicher gelöscht werden. In die Begutachtung sind auch Sicherheitskopien und Backups einzubeziehen.			
	Verarbeitung im Auftrag			
2.9	Für alle in Nummer 2.1 genannten personenbezogenen Daten ist zu begutachten, ob diese durch einen Auftragsverarbeiter verarbeitet werden. Der jeweilige Auftragnehmer sowie die von diesem zu verarbeitenden Daten sind zu benennen. Sofern Auftragsverarbeitung erfolgt, ist die Rechtmäßigkeit jeder einzelnen Auftragsverarbeitung in Nummer 2.10 zu begutachten.			
2.10	Für die Rechtmäßigkeit einer Verarbeitung im Auftrag sind folgende Punkte zu begutachten: – Ist eine Verarbeitung der Daten durch einen Auftragsverarbeiter zu-lässig? Dies ist nicht der Fall, wenn bei Daten von Berufsgeheimnisträgern durch die Auftragsverarbeitung vom Geheimnisträger ein fremdes Geheimnis im Sinne des § 203 StGB offenbart wird. Zudem darf der Auftragnehmer kein Eigeninteresse an der Daten-verarbeitung besitzen. Er darf die personenbezogenen Daten der nutzenden Person nicht für eigene Zwecke verarbeiten.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– Werden die Vorgaben des Artikels 28 DSGVO eingehalten? Jede einzelne Vorgabe ist zu prüfen (z. B. Auswahl des Auftragsverarbeiters, Vertrag mit dem Auftragsverarbeiter, Einsatz von Subunternehmern, Dokumentation der Maßnahmen nach Artikel 32 DSGVO, Durchführung von Kontrollen durch den Diensteanbieter etc). – Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf Weisung des Diensteanbieters (Artikel 29 DSGVO)? – Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO? – Welche Meldeprozesse bestehen mit dem Auftragsverarbeiter für den Fall von Datenschutzverstößen nach Artikel 33 Absatz 2 DSGVO? – Erfüllt der Auftragsverarbeiter die Anforderungen nach dem De-Mail-Gesetz? Wie wird dies sichergestellt? – Hat der Auftragsverarbeiter seinen Sitz außerhalb des EU-/EWR-Raums? Wenn ja, werden die zusätzlichen Anforderungen nach Artikel 44 ff. DSGVO (siehe auch Schrems-II-Urteil) erfüllt? Sofern der Auftragnehmer Unterauftragnehmer beauftragt, ist die Anforderung auch bezogen auf die Unterauftragnehmer zu begutachten. – Werden besondere Kategorien von personenbezogenen Daten vom Auftragsverarbeiter verarbeitet? Wenn ja, werden die insoweit einschlägigen rechtlichen Vorgaben beachtet (vgl. Artikel 9 DSGVO, § 22 BDSG)?			
	Informationspflichten			
2.11	Werden im Rahmen des Postfach- und Versanddienstes personenbezogene Daten bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 13 DSGVO Informationspflichten (vgl. Nummer 1.13). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. Zusätzlich ist zu betrachten, ob die Information in korrekter Form und unentgeltlich erfolgt (Artikel 12 Absatz 1 und 5 DSGVO). § 29 Absatz 2 und § 32 BDSG sind bei der Begutachtung zu berücksichtigen.			
2.12	Werden im Rahmen des Postfach- und Versanddienstes personenbezogene Daten nicht direkt bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 14 DSGVO Informationspflichten. Es ist zu begutachten, wie diese Informationspflichten unter Berücksichtigung von Artikel 12 Absatz 1 und 5 DSGVO umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. § 29 Absatz 1 Satz 1 und § 33 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Weitere Anforderungen (§ 5 des De-Mail-Gesetzes)			
2.13	Auf Wunsch müssen pseudonyme De-Mail-Adressen für Nutzer bereitgestellt werden, bei denen es sich um natürliche Personen handelt (§ 5 Absatz 2 des De-Mail-Gesetzes). Die Inanspruchnahme eines Dienstes durch den Nutzer unter Pseudonym muss für Dritte erkennbar sein. Eine Pseudonym-De-Mail-Adresse darf nur einem De-Mail-Konto zugewiesen werden. Es ist zu begutachten, in welcher Art und Weise diese Anforderungen umgesetzt werden. Hierbei sollte auch auf die Fragen eingegangen werden, ob eine nutzende Person selbst Pseudonym-De-Mail-Adressen verwalten (d. h. einrichten, verändern und löschen) kann und ob eine Überprüfung der einzurichtenden Pseudonym-De-Mail-Adressen gegen eine Liste gesperrter Pseudonym-De-Mail-Adressen (z. B. schon vorher verwendete Adressen, Prominentennamen) erfolgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
2.14	Vertraulichkeit, Integrität und Authentizität der Nachrichten hat der Diensteanbieter zu gewährleisten (§ 5 Absatz 3 des De-Mail-Gesetzes) durch: – Transportverschlüsselung (§ 5 Absatz 3 Satz 2 Nummer 1 des De-Mail-Gesetzes) und – Inhaltsverschlüsselung (§ 5 Absatz 3 Satz 2 Nummer 2 des De-Mail-Gesetzes) Eine Ende-zu-Ende-Verschlüsselung muss bei eigener Aktivität des Nutzers möglich sein. Der Diensteanbieter hat dies zu unterstützen. Es ist zu begutachten, in welcher Art und Weise diese Anforderungen umgesetzt werden.			
2.15	Der Sender muss eine sichere Anmeldung nach § 4 des De-Mail-Gesetzes für den Abruf der Nachricht durch den Empfänger bestimmen können (§ 5 Absatz 4 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
2.16	Der Nutzer muss die Möglichkeit haben, seine sichere Anmeldung bestätigen zu lassen (vgl. § 5 Absatz 5 des De-Mail-Gesetzes). Die Bestätigung muss durch eine qualifizierte elektronische Signatur erfolgen. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
2.17	Der Diensteanbieter muss dem Sender einer Nachricht gemäß § 5 Absatz 7 des De-Mail-Gesetzes auf Antrag den Versand mit den dort in den Nummern 1 bis 4 genannten Daten (Absender- und Empfängeradresse, Datum und Uhrzeit des Versands, Identifizierungsdaten des Diensteanbieters, Prüfsumme der Nachricht) bestätigen (Versandbestätigung). Er hat die Versandbestätigung mit einer qualifizierten elektronischen Signatur zu versehen. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
2.18	Der Diensteanbieter des Empfängers muss auf Antrag des Senders einer Nachricht den Eingang in das Postfach des Empfängers gemäß § 5 Absatz 8 des De-Mail-Gesetzes mit den dort in den Nummern 1 bis 4 von Satz 2 genannten Daten (Absender- und Empfängeradresse, Datum und Uhrzeit des Eingangs, Identifizierungsdaten des Diensteanbieters, Prüfsumme der Nachricht) bestätigen (Eingangsbestätigung). Er hat die Eingangsbestätigung mit einer qualifizierten elektronischen Signatur zu versehen. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
2.19	Der Diensteanbieter des Empfängers muss dem Empfänger ebenfalls die Eingangsbestätigung zusenden (§ 5 Absatz 8 Satz 5 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
2.20	Die Löschfristen sowie die Zugriffs- bzw. Weitergabekontrolle sind für die Versandbestätigung (§ 5 Absatz 7 des De-Mail-Gesetzes) und die Eingangsbestätigung (§ 5 Absatz 8 des De-Mail-Gesetzes) zu begutachten. Dabei ist Folgendes zu berücksichtigen: – Die Protokolle über die Versand- und die Eingangsbestätigung sind in der Regel nach ihrer Auslieferung nach dem Stand der Technik sicher zu löschen. – Nachrichten, für die eine Eingangsbestätigung (§ 5 Absatz 8 des De-Mail-Gesetzes) oder eine Abholbestätigung (§ 5 Absatz 9 des De-Mail-Gesetzes) erteilt wurde, dürfen durch den Empfänger ohne eine sichere Anmeldung an seinem De-Mail-Konto erst 90 Tage nach ihrem Eingang gelöscht werden können (§ 5 Absatz 10 des De-Mail-Gesetzes).			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
2.21	Berechtigten öffentlichen Stellen muss eine Abholbestätigung nach § 5 Absatz 9 des De-Mail-Gesetzes zur Verfügung gestellt werden können. Der Diensteanbieter des Empfängers muss die Abholbestätigung mit einer qualifizierten elektronischen Signatur versehen. Die öffentliche Stelle muss zur förmlichen Zustellung nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, berechtigt sein. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
2.22	Der Diensteanbieter des Empfängers muss dem Empfänger ebenfalls die Abholbestätigung zusenden (§ 5 Absatz 9 Satz 7 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
2.23	Es ist zu begutachten, ob die Daten, die zur Verifikation der dabei verwendeten elektronischen Signaturen genutzt werden, für die Empfänger der Nachrichten verfügbar sind. Wenn eine automatisierte Verifikation der Signaturen angeboten wird, ist darzulegen, wie dies den Empfängern der Bestätigungen dargestellt wird.			
2.24	Es ist zu begutachten, welche Verfahren es für die Empfänger der Bestätigungen gibt, die Prüfsummen der zu bestätigenden Nachricht (§ 5 Absatz 7 Nummer 4, Absatz 8 Satz 2 Nummer 4 und Absatz 9 Satz 3 Nummer 5 des De-Mail-Gesetzes) mit den Prüfsummen der übermittelten Nachrichten zu vergleichen. Erfolgt eine solche Verifikation automatisch? Es ist darzulegen, ob überprüft wurde, dass das Vergleichsverfahren von Prüfsummen im Fall unverändert übermittelter Nachrichten ein positives Ergebnis ergibt und ob das Vergleichsverfahren von Prüfsummen im Fall verändert übermittelter Nachrichten (oder beim Vergleich mit Nachrichten, die nach dem Empfang verändert wurden) ein negatives Ergebnis ergibt.			
2.25	Falls der Diensteanbieter Mechanismen zur Erhaltung des Beweiswertes qualifiziert elektronisch signierter Bestätigungen bereithält (z. B. Übersignatur nach Zeitablauf) ist zu begutachten, in welcher Art und Weise diese ausgestaltet sind.			
2.26	Es ist zu begutachten, ob Kopien von Versandbestätigungen beim Dienstanbieter unmittelbar nach dem Stand der Technik sicher gelöscht werden.			
2.27	Nutzern (natürlichen Personen) muss eine automatische Weiterleitung angeboten werden (§ 5 Absatz 11 des De-Mail-Gesetzes). Der Nutzer muss ausschließen können, dass im Sinne des § 5 Absatz 4 des De-Mail-Gesetzes an ihn gesendete Nachrichten weitergeleitet werden. Der Nutzer muss die automatische Weiterleitung jederzeit zurücknehmen können. Die automatische Weiterleitung darf nur nutzbar sein, wenn der Nutzer sicher an seinem De-Mail-Konto angemeldet ist. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden.			
	Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung			
2.28	Der Diensteanbieter hat nach Artikel 32 Absatz 2 DSGVO durch technische und organisatorische Maßnahmen die Sicherheit der Verarbeitung der in Nummer 2.1 genannten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen betreffen unter anderem Folgendes: – die Pseudonymisierung und Verschlüsselung personenbezogener Daten, – die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, – die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Es ist zu begutachten, ob die Sicherheit der Verarbeitung gewährleistet ist. Dabei sind auch zu betrachten: – Zutritts- und Zugangskontrolle zu allen IT-Einrichtungen – Kopplung mit weiteren technischen Systemen, z. B. Strom- und Netzversorgung – Art und Qualität der Verschlüsselung einschließlich a) Datenspeicherung beim Diensteanbieter – Sicherstellung der dauerhaften Lesbarkeit von Nachrichten bei turnusmäßigem Wechsel der Domänen-Verschlüsselung – Verschlüsslung von Sicherungs- und Backup-Dateien – Schlüsselmanagement (Zugriff auf Schlüssel oder Parametrisierung) – Verfügbarkeit von Schlüsseln auch bei Ausfall von Hardware b) Ende-zu-Ende-Verschlüsselung der nutzenden Person – Veröffentlichung der Verschlüsselungszertifikate durch den Diensteanbieter – Änderung und Zurückziehung des Zertifikats durch die nutzende Person – Verfahren für die Übertragung der Zertifikate zum Diensteanbieter und Verwendung einer sicheren Authentisierung hierfür – keine Unterdrückung von verschlüsselten Dateien mangels Prüffähigkeit auf Malware und Viren – Trennung von Daten über die Nutzung von De-Mail-Diensten von Daten über andere Nutzungen beim Diensteanbieter – Zugriffskontrolle (Zugriffe der nutzenden Person, Zugriffe der Diensteanbieter auf Nachrichteninhalte, Verkehrsdaten sowie auf Daten, die mittelbar der Kommunikation zuzuordnen sind, wie z. B. persönliche Adressbücher) Es ist davon auszugehen, dass die Sicherheit der Verarbeitung gewährleistet ist, wenn ein Testat die Konformität zu den Prüfgrundlagen BSI TR-01201, Teil 1 – Modul IT-Basisinfrastruktur, BSI TR-01201, Teil 3 – Modul Postfach- und Versanddienst bestätigt und das Zertifikat zu BSI TR-01201 Teil 6 – Modul Informationssicherheit vorgelegt wird. Diese Nachweise dürfen zum Zeitpunkt des Gutachtens nicht älter als 3 Monate sein.			
	Interne Protokollierungen			
2.29	Es ist zu begutachten, welche Daten bezüglich nicht zugestellter oder nicht versendeter De-Mails protokolliert werden (z. B. bei Fund von Malware).			
2.30	Es ist zu begutachten, wie die Begrenzung der Anzahl der bereits versendeten Mails bei Authentisierungsniveau „normal“ erfolgt (vgl. Abschnitt 3.1.1.1 der TR De-Mail Postfach- und Versanddienst Funktionalitätsspezifikation, BSI TR-01201 Teil 3.1). Es ist darzulegen, ob es einen spezifischen tagesaktuellen Zähler für die Anzahl der an diesem Tag bereits versandten De-Mails gibt. Falls die Anzahl der an diesem Tag bereits versandten De-Mails durch die Analyse eines Sendeprotokolls bestimmt wird, ist zu erläutern, wie sich dies mit den Anforderungen nach sofortiger Löschung der technischen Protokolle über Versand und Empfang verträgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
2.31	Es ist zu begutachten, ob sichergestellt ist, dass bei Fehlern lediglich Fehlermeldungen, aber keine Protokolle erzeugt werden. Falls Protokolleinträge erzeugt werden, ist darzulegen, welche Aufbewahrungsfristen es gibt und wer unter welchen Bedingungen Zugriff auf diese Protokolldaten hat.			
	Löschung von Nachrichten			
2.32	Es ist zu begutachten, wie sichergestellt wird, dass Nachrichten, für die eine Eingangsbestätigung oder eine Abholbestätigung (§ 5 Absatz 8 und 9 des De-Mail-Gesetzes) erzeugt wird, durch den Empfänger ohne eine sichere Anmeldung an seinem De-Mail-Konto erst 90 Tage nach ihrem Eingang gelöscht werden können (§ 5 Absatz 10 des De-Mail-Gesetzes). Es ist hierbei auch zu betrachten, wie sichergestellt ist, dass die nutzende Person jederzeit alle Nachrichten, für die die zuvor genannte Einschränkung nicht gilt, löschen kann.			
2.33	Es ist zu begutachten, ob es eine „Papierkorb-Funktion“ oder eine explizite Nachfrage gegen unbeabsichtigtes Löschen von Nachrichten gibt.			
2.34	Es ist zu begutachten, mit welcher zeitlichen Verzögerung Nachrichten von Backup-Medien nach dem Stand der Technik sicher gelöscht werden.			
2.35	Es ist zu begutachten, ob es einen Wiederherstellungsprozess gibt, mit dem die nutzende Person eine irrtümliche Löschung durch Recovery-Prozesse aus dem Backup anstoßen kann und ob in diesen Fällen eine sichere Authentisierung der nutzenden Person sichergestellt ist.			
3	**Identitätsbestätigungsdienst (§ 6 des De-Mail-Gesetzes)**			
3.1	Die personenbezogenen Daten, die für den Identitätsbestätigungsdienst verarbeitet werden, sind konkret zu benennen. Die Angaben sollen nach Datenkategorien gebündelt werden (z. B. Kundendaten, Identitätsdaten, Protokolldaten).			
	Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten			
3.2	Für alle in Nummer 3.1 genannten personenbezogenen Daten ist die Ermächtigungsgrundlage zu benennen und zu begutachten. Sofern die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung erfolgt, ist die Wirksamkeit jedes einzelnen Einwilligungsfalls in Nummer 3.3 zu begutachten.			
3.3	Für die Wirksamkeit einer Einwilligung sind folgende Punkte zu begutachten (Artikel 4 Nummer 11, Artikel 7 und 8 DSGVO): – Freiwilligkeit und Kopplungsverbot (ohne jeden Druck und Zwang) – vorherige umfassende Information in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache – Abgabe der Einwilligung nur für einen konkreten Fall – klare textliche Unterscheidung der Einwilligung von anderen Sachverhalten (Hervorhebungspflicht) – Belehrung über das Widerrufsrecht vor Abgabe der Einwilligung – Abgabe der Einwilligung vor der entsprechenden Datenverarbeitung – Einwilligung durch eine eindeutig bestätigende Handlung – Nachweispflicht über erfolgte Einwilligung – bei Minderjährigen unter 16 Jahren: Zustimmung des Trägers der elterlichen Verantwortung – jederzeitige Abrufmöglichkeit des Inhalts der Einwilligung durch die davon betroffene Person – Widerrufsmöglichkeit in einfacher Form entsprechend der Einwilligung			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Erforderlichkeit/Zweckbindung/Zweckänderung			
3.4	Für alle in Nummer 3.1 genannten personenbezogenen Daten ist zu prüfen, ob diese Daten für die Erfüllung der Aufgaben des Diensteanbieters im Rahmen des Identitätsbestätigungsdienstes erforderlich sind und ob die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind [Grundsatz der Zweckbindung und der Erforderlichkeit (vgl. Artikel 6 DSGVO, § 15 Halbsatz 1 des De-Mail-Gesetzes)]. Die jeweiligen Zwecke sind zu nennen. Es ist zu beschreiben, wie sichergestellt wird, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden.			
3.5	Für die Rechtmäßigkeit einer Zweckänderung sind folgende Punkte zu prüfen (Artikel 6 Absatz 4 DSGVO, § 24 BDSG): – Ermächtigungsgrundlage für die Verarbeitung zu dem anderen Zweck (Rechtsvorschrift oder Einwilligung der nutzenden Person) oder – Vorliegen der Voraussetzungen nach Artikel 6 Absatz 4 DSGVO bzw. § 24 BDSG.			
3.6	Erfolgt im Rahmen des Vertragszwecks eine Datenübermittlung, ist zu begutachten, ob die Daten, die nicht von der Zweckbindung erfasst werden, nicht übermittelt werden und ob der Empfänger auf die Zweckbindung der empfangenen Daten hingewiesen bzw. hierauf verpflichtet wird.			
3.7	Es ist zu begutachten, ob eine Kennzeichnung von Datensätzen bezüglich der entsprechenden Zwecke bzw. eine Trennung der Daten nach den verfolgten Zwecken und betroffenen Personen (Trennungsgebot) erfolgt.			
	Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit			
3.8	Nach Erreichen des Zwecks entfällt in der Regel die Erforderlichkeit und die personenbezogenen Daten müssen unverzüglich nach dem Stand der Technik sicher gelöscht werden. Die Aufbewahrungsfristen für die in Nummer 3.1 genannten personenbezogenen Daten (vgl. unter anderem § 13 Absatz 2 des De-Mail-Gesetzes, §§ 9 und 10 TTDSG) sind zu nennen und zu begutachten. Es ist zu beschreiben, durch welche Maßnahmen die Einschränkung der Verarbeitung der personenbezogenen Daten zwischen Wegfall der Erforderlichkeit und der Löschfrist gewährleistet wird. Es ist zudem darzulegen, durch welche Prozesse bzw. Verfahren sichergestellt wird, dass die Daten nach Wegfall der Erforderlichkeit und Ablauf der Aufbewahrungsfristen tatsächlich nach dem Stand der Technik sicher gelöscht werden. In die Begutachtung sind auch Sicherheitskopien und Backups einzubeziehen.			
	Verarbeitung im Auftrag			
3.9	Für alle in Nummer 3.1 genannten personenbezogenen Daten ist zu begutachten, ob diese durch einen Auftragsverarbeiter verarbeitet werden. Der jeweilige Auftragnehmer sowie die von diesem zu verarbeitenden Daten sind zu benennen. Sofern Auftragsverarbeitung erfolgt, ist die Rechtmäßigkeit jeder einzelnen Auftragsverarbeitung in Nummer 3.10 zu begutachten.			
3.10	Für die Rechtmäßigkeit einer Verarbeitung im Auftrag sind folgende Punkte zu begutachten: – Ist eine Verarbeitung der Daten durch einen Auftragsverarbeiter zulässig? Dies ist nicht der Fall, wenn bei Daten von Berufsgeheimnisträgern durch die Auftragsverarbeitung vom Geheimnisträger ein fremdes Geheimnis im Sinne des § 203 StGB offenbart wird. Zudem darf der Auftragnehmer kein Eigeninteresse an der Datenverarbeitung besitzen. Er darf die personenbezogenen Daten der nutzenden Person nicht für eigene Zwecke verarbeiten.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	– Werden die Vorgaben des Artikels 28 DSGVO eingehalten? Jede einzelne Vorgabe ist zu prüfen (z. B. Auswahl des Auftragsverarbeiters, Vertrag mit dem Auftragsverarbeiter, Einsatz von Subunternehmern, Dokumentation der Maßnahmen nach Artikel 32 DSGVO, Durchführung von Kontrollen durch den Diensteanbieter etc.) – Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf Weisung des Diensteanbieters (Artikel 29 DSGVO)? – Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO? – Welche Meldeprozesse bestehen mit dem Auftragsverarbeiter für den Fall von Datenschutzverstößen nach Artikel 33 Absatz 2 DSGVO? – Erfüllt der Auftragsverarbeiter die Anforderungen nach dem De-Mail-Gesetz? Wie wird dies sichergestellt? – Hat der Auftragsverarbeiter seinen Sitz außerhalb des EU-/EWR-Raums? Wenn ja, werden die zusätzlichen Anforderungen nach Artikel 44 ff. DSGVO (siehe auch Schrems-II-Urteil) erfüllt? Sofern der Auftragnehmer Unterauftragnehmer beauftragt, ist die Anforderung auch bezogen auf die Unterauftragnehmer zu begutachten. – Werden besondere Kategorien von personenbezogenen Daten vom Auftragsverarbeiter verarbeitet? Wenn ja, werden die insoweit einschlägigen rechtlichen Vorgaben beachtet (vgl. Artikel 9 DSGVO, § 22 BDSG)?			
	Informationspflichten			
3.11	Werden im Rahmen des Identitätsbestätigungsdienstes personenbezogene Daten bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 13 DSGVO Informationspflichten (vgl. Nummer 1.13). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. Zusätzlich ist zu betrachten, ob die Information in korrekter Form und unentgeltlich erfolgt (Artikel 12 Absatz 1 und 5 DSGVO). § 29 Absatz 2 und § 32 BDSG sind bei der Begutachtung zu berücksichtigen.			
3.12	Werden im Rahmen des Identitätsbestätigungsdienstes personenbezogene Daten nicht direkt bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 14 DSGVO Informationspflichten. Es ist zu begutachten, wie diese Informationspflichten unter Berücksichtigung von Artikel 12 Absatz 1 und 5 DSGVO umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. § 29 Absatz 1 Satz 1 und § 33 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Weitere Anforderungen (§ 6 des De-Mail-Gesetzes)			
3.13	Es ist zu begutachten, ob die vom Identitätsbestätigungsdienst genutzten Identitätsdaten den in § 3 des De-Mail-Gesetzes genannten Identitätsdaten entsprechen.			
3.14	Die De-Mail-Nachricht zur Identitätsbestätigung muss mit einer qualifizierten elektronischen Signatur versehen sein (§ 6 Absatz 1 Satz 4 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
3.15	Der Diensteanbieter hat Vorkehrungen dafür zu treffen, dass Identitätsdaten nicht unbemerkt gefälscht oder verfälscht werden können (§ 6 Absatz 2 des De-Mail-Gesetzes). Dies können sein: – wiederholte interne Kontrollen, – dokumentierter stichprobenartiger Vergleich der Daten mit den jeweiligen Anträgen, – Anwendung elektronischer Signaturen und Zeitstempel bei der Datenspeicherung und Datenübermittlung.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Es ist zu begutachten, in welcher Art und Weise diese Anforderung umgesetzt wird.			
3.16	Es ist zu begutachten, welche Prozesse eingerichtet wurden, um eine Anordnung der Sperrung eines nach § 3 des De-Mail-Gesetzes hinterlegten Identitätsdatums durch das BSI umzusetzen (§ 6 Absatz 3 des De-Mail-Gesetzes). Es ist hierbei darzulegen, wie die Authentizität einer solchen Anordnung geprüft wird.			
3.17	Es ist zu begutachten, ob genau die Daten eines Ident-Auftrages übermittelt werden, die die nutzende Person freigegeben hat.			
3.18	Es ist zu begutachten, ob eine Verwendung des Identitätsbestätigungsdienstes nur mit sicherer Anmeldung (§ 4 des De-Mail-Gesetzes) möglich ist.			
3.19	Es ist zu begutachten, welche Maßnahmen ergriffen werden, um die Integrität der Identitätsdaten zu überprüfen (Kontrolle der Protokolle, Vergleich von Identitätsdaten mit Anträgen).			
	Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung			
3.20	Der Diensteanbieter hat nach Artikel 32 Absatz 2 DSGVO durch technische und organisatorische Maßnahmen die Sicherheit der Verarbeitung der in Nummer 3.1 genannten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen betreffen unter anderem Folgendes: – die Pseudonymisierung und Verschlüsselung personenbezogener Daten, – die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, – die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, – ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Es ist zu begutachten, ob die Sicherheit der Verarbeitung gewährleistet ist. Dabei sind auch zu betrachten: – Zutritts- und Zugangskontrolle zu allen IT-Einrichtungen – Kopplung mit weiteren technischen Systemen, z. B. Strom- und Netzversorgung – Art und Qualität der Verschlüsselung – Trennung von Daten über die Nutzung von De-Mail-Diensten von Daten über andere Nutzungen beim Diensteanbieter – Zugriffskontrolle (Zugriffe der nutzenden Person, Zugriffe der Diensteanbieter) Es ist davon auszugehen, dass die Sicherheit der Verarbeitung gewährleistet ist, wenn ein Testat die Konformität zu den Prüfgrundlagen BSI TR-01201, Teil 1 – Modul IT-Basisinfrastruktur, BSI TR-01201, Teil 4 – Modul Identitätsbestätigungsdienst bestätigt und ein Zertifikat zur BSI TR-01201 Teil 6 – Modul Informationssicherheit vorgelegt wird. Diese Nachweise dürfen zum Zeitpunkt des Gutachtens nicht älter als drei Monate sein.			
	Protokollierung			
3.21	Es ist zu begutachten, welche Daten bezüglich Erstellung, Versand, Überprüfung durch die nutzende Person und gegebenenfalls Verwerfen eines Ident-Auftrages protokolliert werden, welche Aufbewahrungsfristen es gibt es und ob der Zugriff auf diese Protokolldaten eingeschränkt ist.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
4	**Verzeichnisdienst (§ 7 des De-Mail-Gesetzes)**			
4.1	Die personenbezogenen Daten, die für den Verzeichnisdienst verarbeitet werden, sind konkret zu benennen. Die Angaben sollen nach Datenkategorien gebündelt werden (z. B. Kundendaten, Protokolldaten).			
	Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten			
4.2	Für alle in Nummer 4.1 genannten personenbezogenen Daten ist die Ermächtigungsgrundlage zu benennen und zu begutachten. Sofern die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung erfolgt, ist die Wirksamkeit jedes einzelnen Einwilligungsfalls in Nummer 4.3 zu begutachten.			
4.3	Für die Wirksamkeit einer Einwilligung sind folgende Punkte zu begutachten (Artikel 4 Nummer 11, Artikel 7 und 8 DSGVO): – Freiwilligkeit und Kopplungsverbot (ohne jeden Druck und Zwang) – vorherige umfassende Information in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache – Abgabe der Einwilligung nur für einen konkreten Fall – klare textliche Unterscheidung der Einwilligung von anderen Sachverhalten (Hervorhebungspflicht) – Belehrung über das Widerrufsrecht vor Abgabe der Einwilligung – Abgabe der Einwilligung vor der entsprechenden Datenverarbeitung – Einwilligung durch eine eindeutig bestätigende Handlung – Nachweispflicht über erfolgte Einwilligung – bei Minderjährigen unter 16 Jahren: Zustimmung des Trägers der elterlichen Verantwortung – jederzeitige Abrufmöglichkeit des Inhalts der Einwilligung durch die davon betroffene Person – Widerrufsmöglichkeit in einfacher Form entsprechend der Einwilligung			
	Erforderlichkeit/Zweckbindung/Zweckänderung			
4.4	Für alle in Nummer 4.1 genannten personenbezogenen Daten ist zu prüfen, ob diese Daten für die Erfüllung der Aufgaben des Diensteanbieters im Rahmen des Verzeichnisdienstes erforderlich sind und ob die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind [Grundsatz der Zweckbindung und der Erforderlichkeit (vgl. Artikel 6 DSGVO, § 15 Halbsatz 1 des De-Mail-Gesetzes)]. Die jeweiligen Zwecke sind zu nennen. Es ist zu beschreiben, wie sichergestellt wird, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden.			
4.5	Für die Rechtmäßigkeit einer Zweckänderung sind folgende Punkte zu begutachten (Artikel 6 Absatz 4 DSGVO, § 24 BDSG): – Ermächtigungsgrundlage für die Verarbeitung zu dem anderen Zweck (Rechtsvorschrift oder Einwilligung der nutzenden Person) oder – Vorliegen der Voraussetzungen nach Artikel 6 Absatz 4 DSGVO bzw. § 24 BDSG.			
4.6	Erfolgt im Rahmen des Vertragszwecks eine Datenübermittlung, ist zu begutachten, ob die Daten, die nicht von der Zweckbindung erfasst werden, nicht übermittelt werden und ob der Empfänger auf die Zweckbindung der empfangenen Daten hingewiesen bzw. hierauf verpflichtet wird.			
4.7	Es ist zu begutachten, ob eine Kennzeichnung von Datensätzen bezüglich der entsprechenden Zwecke bzw. eine Trennung der Daten nach den verfolgten Zwecken und betroffenen Personen (Trennungsgebot) erfolgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit			
4.8	Nach Erreichen des Zwecks entfällt in der Regel die Erforderlichkeit und die personenbezogenen Daten müssen unverzüglich nach dem Stand der Technik sicher gelöscht werden. Die Aufbewahrungsfristen für die in Nummer 4.1 genannten personenbezogenen Daten (vgl. unter anderem § 13 Absatz 2 des De-Mail-Gesetzes, §§ 9 und 10 TTDSG) sind zu nennen und zu begutachten. Es ist zu beschreiben, durch welche Maßnahmen die Einschränkung der Verarbeitung der personenbezogenen Daten zwischen Wegfall der Erforderlichkeit und der Löschfrist gewährleistet wird. Es ist zudem darzulegen, durch welche Prozesse bzw. Verfahren sichergestellt wird, dass die Daten nach Wegfall der Erforderlichkeit und Ablauf der Aufbewahrungsfristen tatsächlich nach dem Stand der Technik sicher gelöscht werden. In die Begutachtung sind auch Sicherheitskopien und Backups einzubeziehen.			
	Verarbeitung im Auftrag			
4.9	Für alle in Nummer 4.1 genannten personenbezogenen Daten ist zu begutachten, ob diese durch einen Auftragsverarbeiter verarbeitet werden. Der jeweilige Auftragnehmer sowie die von diesem zu verarbeitenden Daten sind zu benennen. Sofern Auftragsverarbeitung erfolgt, ist die Rechtmäßigkeit jeder einzelnen Auftragsverarbeitung in Nummer 4.10 zu begutachten.			
4.10	Für die Rechtmäßigkeit einer Verarbeitung im Auftrag sind folgende Punkte zu begutachten: – Ist eine Verarbeitung der Daten durch einen Auftragsverarbeiter zulässig? Dies ist nicht der Fall, wenn bei Daten von Berufsgeheimnisträgern durch die Auftragsverarbeitung vom Geheimnisträger ein fremdes Geheimnis im Sinne des § 203 StGB offenbart wird. Zudem darf der Auftragnehmer kein Eigeninteresse an der Datenverarbeitung besitzen. Er darf die personenbezogenen Daten der nutzenden Person nicht für eigene Zwecke verarbeiten. – Werden die Vorgaben des Artikels 28 DSGVO eingehalten? Jede einzelne Vorgabe ist zu prüfen (z. B. Auswahl des Auftragsverarbeiters, Vertrag mit dem Auftragsverarbeiter, Einsatz von Subunternehmern, Dokumentation der Maßnahmen nach Artikel 32 DSGVO, Durchführung von Kontrollen durch den Diensteanbieter, …). – Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf Weisung des Diensteanbieters (Artikel 29 DSGVO)? – Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO? – Welche Meldeprozesse bestehen mit dem Auftragsverarbeiter für den Fall von Datenschutzverstößen nach Artikel 33 Absatz 2 DSGVO? – Erfüllt der Auftragsverarbeiter die Anforderungen nach dem De-Mail-Gesetz? Wie wird dies sichergestellt? – Hat der Auftragsverarbeiter seinen Sitz außerhalb des EU-/EWR-Raums? Wenn ja, werden die zusätzlichen Anforderungen nach Artikel 44 ff. DSGVO (siehe auch Schrems-II-Urteil) erfüllt? Sofern der Auftragsverarbeiter Unterauftragnehmer beauftragt, ist die Anforderung auch bezogen auf die Unterauftragnehmer zu begutachten. – Werden besondere Kategorien von personenbezogenen Daten vom Auftragsverarbeiter verarbeitet? Wenn ja, werden die insoweit einschlägigen rechtlichen Vorgaben beachtet (vgl. Artikel 9 DSGVO, § 22 BDSG)?			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Informationspflichten			
4.11	Werden im Rahmen des Verzeichnisdienstes personenbezogene Daten bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 13 DSGVO Informationspflichten (vgl. Nummer 1.13). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. Zusätzlich ist zu betrachten, ob die Information in korrekter Form und unentgeltlich erfolgt (Artikel 12 Absatz 1 und 5 DSGVO). § 29 Absatz 2 und § 32 BDSG sind bei der Begutachtung zu berücksichtigen.			
4.12	Werden im Rahmen des Verzeichnisdienstes personenbezogene Daten nicht direkt bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 14 DSGVO Informationspflichten. Es ist zu begutachten, wie diese Informationspflichten unter Berücksichtigung von Artikel 12 Absatz 1 und 5 DSGVO umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. § 29 Absatz 1 Satz 1 und § 33 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Weitere Anforderungen (§ 7 des De-Mail-Gesetzes)			
4.13	Bei dem Verzeichnisdienst handelt es sich um ein Verzeichnis, welches ausschließlich für De-Mail-Nutzer angelegt ist, damit diese die für eine De-Mail-Kommunikation notwendigen Informationen erhalten. Das Verzeichnis wird nicht in Form eines öffentlichen Telefonbuches mit der Möglichkeit einer Einsichtnahme durch beliebige Dritte geführt. Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
4.14	Die De-Mail-Adressen, die hinterlegten Identitätsdaten sowie die für die Verschlüsselung von Nachrichten notwendigen Informationen dürfen vom Dienstanbieter in einem Verzeichnisdienst im De-Mail-Verbund veröffentlicht werden. Dies darf nur auf ausdrückliches Verlangen des Nutzers erfolgen (§ 7 Absatz 1 Satz 1 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderungen umgesetzt werden. Sollten in dem Verzeichnisdienst zusätzlich Freitextfelder mit nicht verifizierten Daten aufgenommen sein, ist zu begutachten, ob klar (in einer einfachen und leicht verständlichen Sprache) sowie deutlich (durch eine entsprechende Darstellung) erkennbar ist, dass es sich um keine verifizierten Daten handelt.			
4.15	Der Diensteanbieter hat eine De-Mail-Adresse, ein Identitätsdatum oder die für die Verschlüsselung von Nachrichten an den Nutzer notwendige Informationen aus dem Verzeichnisdienst nach § 7 Absatz 2 des De-Mail-Gesetzes unverzüglich nach dem Stand der Technik sicher zu löschen, wenn – der Nutzer dies verlangt, – die Daten aufgrund falscher Angaben ausgestellt wurden, – der Diensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen akkreditierten Diensteanbieter fortgeführt wird oder – das BSI die Löschung aus dem Verzeichnisdienst anordnet. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden. Wenn Replikationen von Verzeichnisdienstinformationen an weitere Verzeichnisdienste innerhalb des De-Mail-Verbundes erfolgen, ist zusätzlich zu betrachten, wie sichergestellt ist, dass die Löschung auch in diesen Diensten erfolgt.			
4.16	Auf Verlangen des Nutzers muss der Diensteanbieter durch einen geeigneten Zusatz die Erklärung des Nutzers im Verzeichnisdienst veröffentlichen, den Zugang im Sinne von § 3 a VwVfG, § 36 a Absatz 1 SGB I und des § 87 a Absatz 1 AO öffnen zu wollen (§ 7 Absatz 3 Satz 2 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
4.17	Auf Verlangen des Nutzers ist der Zusatz für die Zugangseröffnung nach § 7 Absatz 3 Satz 4 des De-Mail-Gesetzes zurückzunehmen. Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
4.18	§ 18 TTDSG (Bereitstellung von Teilnehmerdaten) ist entsprechend zu beachten. Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
4.19	Es ist zu begutachten, wie das System im Rahmen der Suche auf unvollständige Vornamen (es könnte bei mehreren registrierten Vornamen nur nach einem Vornamen gesucht werden) reagiert und ob eine Ähnlichkeitssuche (Meyer/Meier/Mayer/Maier) vorhanden ist.			
	Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung			
4.20	Der Diensteanbieter hat nach Artikel 32 Absatz 2 DSGVO durch technische und organisatorische Maßnahmen die Sicherheit der Verarbeitung der in Nummer 4.1 genannten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen betreffen unter anderem Folgendes: – die Pseudonymisierung und Verschlüsselung personenbezogener Daten, – die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, – die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, – ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Es ist zu begutachten, ob die Sicherheit der Verarbeitung gewährleistet ist. Dabei sind auch zu betrachten: – Zutritts- und Zugangskontrolle zu allen IT-Einrichtungen – Kopplung mit weiteren technischen Systemen, z. B. Strom- und Netzversorgung – Art und Qualität der Verschlüsselung – Trennung von Daten über die Nutzung von De-Mail-Diensten von Daten über andere Nutzungen beim Diensteanbieter – Zugriffskontrolle (Zugriffe der nutzenden Person, Zugriffe der Diensteanbieter) Es ist davon auszugehen, dass die Sicherheit der Verarbeitung gewährleistet ist, wenn ein Testat die Konformität zu den Prüfgrundlagen BSI TR-01201, Teil 1 – Modul IT-Basisinfrastruktur bestätigt und ein Zertifikat zur BSI TR-01201 Teil 6 – Modul Informationssicherheit vorgelegt wird. Diese Nachweise dürfen zum Zeitpunkt des Gutachtens nicht älter als drei Monate sein.			
	Interne Protokollierungen			
4.21	Es ist zu begutachten, ob Abfragen aus dem Verzeichnisdienst angemessen protokolliert werden, welche Aufbewahrungsfristen es gibt und ob der Zugriff auf diese Protokolldaten eingeschränkt ist.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
5	**Dokumentenablage (§ 8 des De-Mail-Gesetzes)**			
5.1	Die personenbezogenen Daten, die für die Dokumentenablage verarbeitet werden, sind konkret zu benennen. Die Angaben sollen nach Datenkategorien gebündelt werden (z. B. Kundendaten, Protokolldaten).			
	Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten			
5.2	Für alle in Nummer 5.1 genannten personenbezogenen Daten ist die Ermächtigungsgrundlage zu benennen und zu begutachten. Sofern die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung erfolgt, ist die Wirksamkeit jedes einzelnen Einwilligungsfalls in Nummer 5.3 zu begutachten.			
5.3	Für die Wirksamkeit einer Einwilligung sind folgende Punkte zu begutachten (Artikel 4 Nummer 11, Artikel 7 und 8 DSGVO): – Freiwilligkeit und Kopplungsverbot (ohne jeden Druck und Zwang) – vorherige umfassende Information in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache – Abgabe der Einwilligung nur für einen konkreten Fall – klare textliche Unterscheidung der Einwilligung von anderen Sachverhalten (Hervorhebungspflicht) – Belehrung über das Widerrufsrecht vor Abgabe der Einwilligung – Abgabe der Einwilligung vor der entsprechenden Datenverarbeitung – Einwilligung durch eine eindeutig bestätigende Handlung – Nachweispflicht über erfolgte Einwilligung – bei Minderjährigen unter 16 Jahren: Zustimmung des Trägers der elterlichen Verantwortung – jederzeitige Abrufmöglichkeit des Inhalts der Einwilligung durch die davon betroffene Person – Widerrufsmöglichkeit in einfacher Form entsprechend der Einwilligung			
	Erforderlichkeit/Zweckbindung/Zweckänderung			
5.4	Für alle in Nummer 5.1 genannten personenbezogenen Daten ist zu begutachten, ob diese Daten für die Erfüllung der Aufgaben des Diensteanbieters im Rahmen der Dokumentenablage erforderlich sind und ob die Verarbeitung für die Zwecke erfolgt, für die die Daten erhoben worden sind (Grundsatz der Zweckbindung und der Erforderlichkeit (vgl. Artikel 6 DSGVO, § 15 Halbsatz 1 des De-Mail-Gesetzes). Die jeweiligen Zwecke sind zu nennen. Es ist zu beschreiben, wie sichergestellt wird, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden.			
5.5	Für die Rechtmäßigkeit einer Zweckänderung sind folgende Punkte zu begutachten (Artikel 6 Absatz 4 DSGVO, § 24 BDSG): – Ermächtigungsgrundlage für die Verarbeitung zu dem anderen Zweck (Rechtsvorschrift oder Einwilligung der nutzenden Person) oder – Vorliegen der Voraussetzungen nach Artikel 6 Absatz 4 DSGVO bzw. § 24 BDSG.			
5.6	Erfolgt im Rahmen des Vertragszwecks eine Datenübermittlung, ist zu begutachten, ob die Daten, die nicht von der Zweckbindung erfasst werden, nicht übermittelt werden und ob der Empfänger auf die Zweckbindung der empfangenen Daten hingewiesen bzw. hierauf verpflichtet wird.			
5.7	Es ist zu begutachten, ob eine Kennzeichnung von Datensätzen bezüglich der entsprechenden Zwecke bzw. eine Trennung der Daten nach den verfolgten Zwecken und betroffenen Personen (Trennungsgebot) erfolgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit			
5.8	Nach Erreichen des Zwecks entfällt in der Regel die Erforderlichkeit und die personenbezogenen Daten müssen unverzüglich nach dem Stand der Technik sicher gelöscht werden. Die Aufbewahrungsfristen für die in Nummer 5.1 genannten personenbezogenen Daten (vgl. unter anderem § 13 Absatz 2 des De-Mail-Gesetzes, §§ 9 und 10 TTDSG) sind zu nennen und zu begutachten. Es ist zu beschreiben, durch welche Maßnahmen die Einschränkung der Verarbeitung der personenbezogenen Daten zwischen Wegfall der Erforderlichkeit und der Löschfrist gewährleistet wird. Es ist zudem darzulegen, durch welche Prozesse bzw. Verfahren sichergestellt wird, dass die Daten nach Wegfall der Erforderlichkeit und Ablauf der Aufbewahrungsfristen tatsächlich nach dem Stand der Technik sicher gelöscht werden. In die Begutachtung sind auch Sicherheitskopien und Backups einzubeziehen.			
	Verarbeitung im Auftrag			
5.9	Für alle in Nummer 5.1 genannten personenbezogenen Daten ist zu begutachten, ob diese durch einen Auftragsverarbeiter verarbeitet werden. Der jeweilige Auftragnehmer sowie die von diesem zu verarbeitenden Daten sind zu benennen. Sofern Auftragsverarbeitung erfolgt, ist die Rechtmäßigkeit jeder einzelnen Auftragsverarbeitung in Nummer 5.10 zu begutachten.			
5.10	Für die Rechtmäßigkeit einer Verarbeitung im Auftrag sind folgende Punkte zu begutachten: – Ist eine Verarbeitung der Daten durch einen Auftragsverarbeiter zulässig? Dies ist nicht der Fall, wenn bei Daten von Berufsgeheimnisträgern durch die Auftragsverarbeitung vom Geheimnisträger ein fremdes Geheimnis im Sinne des § 203 StGB offenbart wird. Zudem darf der Auftragnehmer kein Eigeninteresse an der Datenverarbeitung besitzen. Er darf die personenbezogenen Daten der nutzenden Person nicht für eigene Zwecke verarbeiten. – Werden die Vorgaben des Artikels 28 DSGVO eingehalten? Jede einzelne Vorgabe ist zu prüfen (z. B. Auswahl des Auftragsverarbeiters, Vertrag mit dem Auftragsverarbeiter, Einsatz von Subunternehmern, Dokumentation der Maßnahmen nach Artikel 32 DSGVO, Durchführung von Kontrollen durch den Diensteanbieter, …). – Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf Weisung des Diensteanbieters (Artikel 29 DSGVO)? – Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 2 DSGVO? – Welche Meldeprozesse bestehen mit dem Auftragsverarbeiter für den Fall von Datenschutzverstößen nach Artikel 33 Absatz 2 DSGVO? – Erfüllt der Auftragsverarbeiter die Anforderungen nach dem De-Mail-Gesetz? Wie wird dies sichergestellt? – Hat der Auftragsverarbeiter seinen Sitz außerhalb des EU-/EWR-Raums? Wenn ja, werden die zusätzlichen Anforderungen nach Artikel 44 ff. DSGVO (siehe auch Schrems-II-Urteil) erfüllt? Sofern der Auftragsverarbeiter Unterauftragnehmer beauftragt, ist die Anforderung auch bezogen auf die Unterauftragnehmer zu begutachten. – Werden besondere Kategorien von personenbezogenen Daten vom Auftragsverarbeiter verarbeitet? Wenn ja, werden insoweit die einschlägigen rechtlichen Vorgaben beachtet (vgl. Artikel 9 DSGVO, § 22 BDSG)?			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Informationspflichten			
5.11	Werden im Rahmen der Dokumentenablage personenbezogene Daten bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 13 DSGVO Informationspflichten (vgl. Nummer 1.13). Es ist zu begutachten, wie die oben genannten Informationspflichten umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. Zusätzlich ist zu betrachten, ob die Information in korrekter Form und unentgeltlich erfolgt (Artikel 12 Absatz 1 und 5 DSGVO). § 29 Absatz 2 und § 32 BDSG sind bei der Begutachtung zu berücksichtigen.			
5.12	Werden im Rahmen der Dokumentenablage personenbezogene Daten nicht direkt bei der nutzenden Person erhoben? Wenn ja, bestehen nach Artikel 14 DSGVO Informationspflichten. Es ist zu begutachten, wie diese Informationspflichen unter Berücksichtigung von Artikel 12 Absatz 1 und 5 DSGVO umgesetzt werden. Es ist dabei auf jede einzelne Informationspflicht einzugehen. § 29 Absatz 1 Satz 1 und § 33 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Weitere Anforderungen (§ 8 des De-Mail-Gesetzes)			
5.13	Der Diensteanbieter kann dem Nutzer eine Dokumentenablage anbieten. Er hat dafür Sorge zu tragen, dass die Dokumente sicher abgelegt werden; Vertraulichkeit, Integrität und ständige Verfügbarkeit der abgelegten Dokumente sind zu gewährleisten (§ 8 Satz 1 und 2 des De-Mail-Gesetzes). Nur die nutzende Person darf Zugriff auf die in seiner Dokumentenablage niedergelegten Dokumente haben. Es ist zu begutachten, wie diese Anforderungen umgesetzt werden. Dabei sollte auch dargelegt werden, wie ausgeschlossen wird, dass durch Dritte ein Zugriff auf Inhalte der Dokumentenablage (Schutz der Dokumentenablage durch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme) erfolgt.			
5.14	Die Dokumente sind durch den Diensteanbieter verschlüsselt abzulegen (§ 8 Satz 3 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird. Es ist darüber hinaus darzulegen, ob die nutzende Person bei Bedarf auch ihrerseits zusätzlich verschlüsselte Dokumente ablegen kann und welche Programme der Diensteanbieter hierfür bereitstellt oder empfiehlt.			
5.15	Der Nutzer muss die Möglichkeit haben, für jede einzelne Datei eine für den Zugriff erforderliche sichere Anmeldung im Sinne des § 4 des De-Mail-Gesetzes festzulegen (§ 8 Satz 4 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderung umgesetzt wird.			
5.16	Der Diensteanbieter hat ein Protokoll über die Einstellung und Herausnahme von Dokumenten bereitzustellen, wenn die nutzende Person dieses wünscht. Das Protokoll ist mit einer qualifizierten elektronischen Signatur zu versehen (§ 8 Satz 5 des De-Mail-Gesetzes). Es ist zu begutachten, wie diese Anforderungen umgesetzt werden. Es ist dabei darzulegen, welche Daten ein solches Protokoll (Aufzählung von Dokumentennamen, Prüfsummen von Dokumenten, Daten der letzten Lese- oder Schreibzugriffe) enthält.			
5.17	Es ist zu begutachten, wie ausgeschlossen wird, dass der Diensteanbieter Zugriff auf Dokumente nehmen kann (während des Uploads, Downloads, Malware-Scannings und der Bereitstellung per Webserver liegen die Daten unverschlüsselt im Arbeitsspeicher vor; der Diensteanbieter hat weiterhin Zugriff auf die Schlüssel, die für die verschlüsselte Speicherung verwendet werden). Entsprechendes gilt auch für den Zugriff auf Protokolldaten.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
5.18	Es ist zu begutachten, wie Metadaten, die Aktivitäten bezüglich einzelner Ordner/Dateien betreffen, nach dem Stand der Technik sicher gelöscht werden, ob die Metadaten ordner- oder dateibasiert gespeichert werden oder Protokolle aus einer chronologischen Aufzeichnung aller Änderungen erzeugt und gespeichert werden.			
	Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung			
5.19	Der Diensteanbieter hat nach Artikel 32 Absatz 2 DSGVO durch technische und organisatorische Maßnahmen die Sicherheit der Verarbeitung der in Nummer 5.1 genannten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen betreffen unter anderem Folgendes: – die Pseudonymisierung und Verschlüsselung personenbezogener Daten, – die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, – die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, – ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Es ist zu begutachten, ob die Sicherheit der Verarbeitung gewährleistet ist. Dabei sind auch zu betrachten: – Zutritts- und Zugangskontrolle zu allen IT-Einrichtungen – Kopplung mit weiteren technischen Systemen, z. B. Strom- und Netzversorgung – Art und Qualität der Verschlüsselung – Trennung von Daten über die Nutzung von De-Mail-Diensten von Daten über andere Nutzungen beim Diensteanbieter – Zugriffskontrolle (Zugriffe der nutzenden Person, Zugriffe der Diensteanbieter) Es ist davon auszugehen, dass die Sicherheit der Verarbeitung gewährleistet ist, wenn ein Testat die Konformität zu den Prüfgrundlagen BSI TR-01201, Teil 1 – Modul IT-Basisinfrastruktur, BSI TR-01201, Teil 5 – Modul Dokumentenablage bestätigt und ein Zertifikat zur BSI TR-01201 Teil 6 – Modul Informationssicherheit vorgelegt wird. Diese Nachweise dürfen zum Zeitpunkt des Gutachtens nicht älter als drei Monate sein.			
	Löschung und Datensparsamkeit (bezogen auf die Dokumente im Sinne des § 8 des De-Mail-Gesetzes)			
5.20	Es ist zu begutachten, ob es eine „Papierkorb-Funktion“ oder eine explizite Nachfrage gegen unbeabsichtigtes Löschen gibt.			
5.21	Es ist zu begutachten, wie lange Dateien bzw. Dokumente auf Backup-Medien gespeichert sind.			
5.22	Es ist zu begutachten, ob es einen Wiederherstellungsprozess, mit dem die nutzende Person eine irrtümliche Löschung durch Recovery-Prozesse aus dem Backup anstoßen kann, gibt.			
5.23	Es ist zu begutachten, ob mit der Löschung von Dateien bzw. Dokumenten auch die dazugehörigen Metadaten nach dem Stand der Technik sicher gelöscht werden.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
6	**Rechte der betroffenen Personen**			
	Auskunftsanspruch (Artikel 15 DSGVO)			
6.1	Die betroffene Person hat das Recht, von dem Diensteanbieter eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogene Daten und auf folgende Informationen (Artikel 15 Absatz 1 DSGVO): – Verarbeitungszwecke, – Kategorien der verarbeiteten personenbezogenen Daten, – Empfänger, denen die personenbezogenen Daten offengelegt werden, – geplante Speicherdauer, – Bestehen eines Rechts auf Berichtigung, Löschung, auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung, – Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde, – Recht auf Informationen über die Herkunft der Daten, sofern die Daten nicht bei der betroffenen Person erhoben wurden und – Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 unterrichtet zu werden (Artikel 15 Absatz 2 DSGVO). Auf Verlangen stellt der Diensteanbieter eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind zur Verfügung (Artikel 15 Absatz 3 DSGVO). Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (§ 15 Absatz 4 DSGVO). Es müssen definierte Prozesse zur Gewährleistung des Auskunftsrechts eingerichtet sein (z. B. ein einfaches Online-Auskunftsverfahren). Die Identität der Auskunft verlangenden Person muss überprüft werden. Die Auskunft muss vollständig sein. Die fristgerechte Umsetzung der Auskunft in korrekter Form und unentgeltlich muss gewährleistet sein. Der Schutz Dritter bei der Auskunft muss gewahrt werden. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers das Auskunftsrecht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. § 27 Absatz 2, § 28 Absatz 2, § 29 Absatz 1 Satz 2 und § 34 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Recht auf Berichtigung (Artikel 16 DSGVO)			
6.2	Nach Artikel 16 DSGVO hat die betroffene Person das Recht, vom Diensteanbieter unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. Es müssen definierte Prozesse zur Gewährleistung der Berichtigung eingerichtet sein. Die Identität der verlangenden Person muss geprüft werden. Die fristgerechte und unentgeltliche Umsetzung der Berichtigung muss gewährleistet sein. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Recht auf Löschung, „Recht auf Vergessenwerden“ (Artikel 17 DSGVO)			
6.3	Nach Artikel 17 DSGVO hat die betroffene Person das Recht vom Diensteanbieter zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe vorliegt: – Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig. – Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO oder Artikel 9 Absatz 2 Buchstabe a DSGVO stützte und es fehlt an einer anderweitigen Rechtsgrundlage. – Die betroffene Person legt gemäß Artikel 21 Absatz 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangig berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß § 21 Absatz 2 DSGVO Widerspruch gegen die Verarbeitung ein. – Die personenbezogenen Daten wurden unrechtmäßig verarbeitet. – Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder Recht der Mitgliedstaaten erforderlich, dem der Diensteanbieter unterliegt. – Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 DSGVO erhoben. Hat der Diensteanbieter die zu löschenden personenbezogenen Daten öffentlich gemacht, hat er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen zu treffen, um andere Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat (Artikel 17 Absatz 2 DSGVO). Eine weitere Speicherung der personenbezogenen Daten ist trotz entgegenstehendem Willen der betroffenen Person zulässig, soweit die Verarbeitung erforderlich ist (Artikel 17 Absatz 3 DSGVO): – zur Ausübung des Rechts auf freie Meinungsäußerung und Information, – zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten erfordert, oder zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Diensteanbieter übertragen wurde, – aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, – für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 DSGVO, soweit das Recht auf Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, – zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Es müssen definierte Prozesse zur Gewährleistung des Rechts auf Löschung eingerichtet sein. Die Identität der verlangenden Person muss geprüft werden. Die fristgerechte und unentgeltliche Umsetzung der Löschung muss gewährleistet sein. Die Löschung muss vollständig und irreversibel sein. Dies betrifft auch Backups etc. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. § 35 Absatz 1 und 3 BDSG ist bei der Begutachtung zu berücksichtigen.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)			
6.4	Nach Artikel 18 Absatz 1 DSGVO hat die betroffene Person das Recht, vom Diensteanbieter die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist: – Die Richtigkeit der personenbezogenen Daten von der betroffenen Person wird bestritten, und zwar für eine Dauer, die es dem Diensteanbieter ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen. – Die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten. – Der Diensteanbieter benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, der Betroffene benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. – Die betroffene Person hat Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 DSGVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Diensteanbieters gegenüber denen der betroffenen Person überwiegen. Wurde die Verarbeitung auf Antrag der betroffenen Person eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden (Artikel 18 Absatz 2 DSGVO). Die betroffene Person ist von dem Diensteanbieter zu unterrichten, bevor die Einschränkung der Verarbeitung aufgehoben wird (Artikel 18 Absatz 3 DSGVO). Es müssen definierte Prozesse zur Gewährleistung des Rechts auf Einschränkung der Verarbeitung eingerichtet sein. Die Einschränkung der Verarbeitung muss so erfolgen, dass eingeschränkte Daten eindeutig markiert bzw. ausgesondert sind und nur noch von einem eingeschränkten Personenkreis im Rahmen der Zweckbindung eingesehen werden können. Die Identität der verlangenden Person muss geprüft werden. Die fristgerechte und unentgeltliche Umsetzung der Einschränkung der Verarbeitung muss gewährleistet sein. Es muss gewährleistet sein, dass nach Ablauf der Aufbewahrungsfrist eine nach dem Stand der Technik sichere Löschung der eingeschränkten Daten erfolgt. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. § 35 Absatz 2 BDSG ist bei der Begutachtung zu berücksichtigen.			
	Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)			
6.5	Nach Artikel 20 Absatz 1 DSGVO hat die betroffene Person die sie betreffenden personenbezogenen Daten, die sie einem Diensteanbieter bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Diensteanbieter, die die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern – die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO oder Artikel 9 Absatz 2 Buchstabe b DSGVO oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und – die Verarbeitung mithilfe automatisierter Verfahren erfolgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Bei der Ausübung dieses Rechts hat die betroffene Person das Recht zu erwirken, dass die personenbezogenen Daten direkt von einem Diensteanbieter einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist (Artikel 20 Absatz 2 DSGVO). Das Recht auf Datenübertragung wird mit Blick auf solche Verarbeitungen, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Diensteanbieter übertragen wurde, begrenzt (Artikel 20 Absatz 3 DSGVO). Das Recht auf Datenübertragung darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (Artikel 20 Absatz 4 DSGVO). Es müssen definierte Prozesse zur Gewährleistung des Rechts auf Datenübertragbarkeit eingerichtet sein. Interoperable Formate müssen genutzt werden, die die Datenübertragbarkeit ermöglichen. Die Identität der verlangenden Person muss geprüft werden. Die fristgerechte und unentgeltliche Umsetzung der Datenübertragung muss gewährleistet sein. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden.			
	Recht auf Widerspruch (Artikel 21 DSGVO)			
6.6	Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht (§ 21 Absatz 2 DSGVO). Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet (§ 21 Absatz 3 DSGVO). Die betroffene Person kann ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden (Artikel 21 Absatz 5 DSGVO). Es müssen definierte Prozesse zur Gewährleistung des Widerspruchsrechts sein. Es muss gewährleistet sein, dass der Berechtigte sein Widerspruchsrecht mittels automatisierter Verfahren ausüben kann. Die Identität der Widerspruch einlegenden Person muss geprüft werden. Die fristgerechte und unentgeltliche Umsetzung des Widerspruchs muss gewährleistet sein. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. § 36 BDSG ist bei der Begutachtung zu berücksichtigen.			
	Recht auf nicht-automatisierte Entscheidung im Einzelfall einschließlich Profiling (Artikel 22 DSGVO)			
6.7	Nach Artikel 22 hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies gilt nicht, sofern die Entscheidung a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Diensteanbieter erforderlich ist, b) aufgrund von Rechtvorschriften der Union oder der Mitgliedstaaten, denen der Diensteanbieter unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
	Es ist zu begutachten, ob Entscheidungen des Diensteanbieters ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – erfolgt. Wenn ja, ist zu betrachten, ob die Ausnahmeregelungen des Artikels 22 Absatz 2 DSGVO vorliegen, angemessene Maßnahmen getroffen wurden, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffen Person zu wahren (Artikel 22 Absatz 3 DSGVO) sowie die Entscheidungen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 DSGVO beruhen (Artikel 22 Absatz 4 DSGVO). § 31 und § 37 BDSG sind bei der Begutachtung zu berücksichtigen.			
	Recht auf Benachrichtigung bei einer Datenschutzverletzung (Artikel 34 DSGVO)			
6.8	Nach Artikel 34 Absatz 1 DSGVO und § 169 Absatz 1 Satz 2 TKG hat die betroffene Person das Recht auf unverzügliche Benachrichtigung durch den Diensteanbieter bei einer Verletzung des Schutzes sie betreffender personenbezogener Daten mit voraussichtlich hohem Risiko für ihre persönlichen Rechte und Freiheiten. Die Benachrichtigung hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in Artikel 33 Absatz 3 Buchstaben b, c, und d DSGVO genannten Informationen und Maßnahmen zu enthalten (Artikel 34 Absatz 2 DSGVO). Eine Benachrichtigung der betroffenen Person entfällt, wenn eine in Artikel 34 Absatz 3 DSGVO genannten Bedingungen zutrifft. Es müssen definierte Prozesse zur Gewährleistung des Rechts auf Benachrichtigung eingerichtet sein. Die zeitnahe Umsetzung der Benachrichtigung muss gewährleistet sein. Es muss gewährleistet sein, dass auch bei Einschaltung eines Auftragnehmers dieses Recht umgesetzt werden kann. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. Dabei sind auch die Sprache und der Inhalt der Benachrichtigung zu betrachten. § 29 Absatz 1 Satz 3 und 4 BDSG ist bei der Begutachtung zu berücksichtigen.			
7	**Datenschutzmanagement**			
7.1	Der Diensteanbieter muss nach Artikel 5 Absatz 2 DSGVO die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 Absatz 1 DSGVO nachweisen (Rechenschaftspflicht). Es ist zu begutachten, in welcher Art und Weise diese Anforderung umgesetzt wird. Dabei ist zu betrachten, ob der Diensteanbieter interne Strategien festgelegt und Maßnahmen ergreift, die den Grundsätzen des Datenschutzes durch Technik (data protection by design) und dem Erfordernis datenschutzfreundlicher Voreinstellungen (data protection by default) Genüge tun und ob eine Dokumentation entsprechend Artikel 24 Absatz 1 DSGVO erfolgt.			
7.2	Es ist zu begutachten, ob ein Datenschutzkonzept vorliegt, ob es regelmäßig aktualisiert wird, ob alle Mitarbeiter hinreichend über das Datenschutzkonzept informiert sind und ob ausreichende Betriebsmittel für die Umsetzung des Datenschutzkonzepts vorhanden sind.			
7.3	Es ist zu begutachten, wie der Datenschutz im laufenden Betrieb aufrechterhalten wird, vor allem bei Änderungen im Datenschutzrecht oder in den IT-Verfahren. Dabei ist auch darzulegen, ob die Einhaltung der datenschutzrechtlichen Anforderungen regelmäßig überprüft wird.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
7.4	Nach Artikel 30 Absatz 1 und 3 DSGVO hat jeder Diensteanbieter ein Verzeichnis aller Verarbeitungstätigkeiten schriftlich (auch in elektronischer Form) zu führen. Es ist zu begutachten, wie diese Anforderungen umgesetzt sind. Dabei ist auch zu betrachten, ob im Verzeichnis die erforderlichen Angaben nach Artikel 30 Absatz 1 DSGVO enthalten sind.			
7.5	Es ist zu begutachten, ob neue bzw. aktualisierte Software und IT-Verfahren nach einem Testplan überprüft werden. Dabei ist auch zu betrachten, ob der Datenschutzbeauftragte vor den Software-Tests mit Daten, die Personenbezug haben könnten, informiert wird und ob vor der Freigabe von IT-Verfahren, die personenbezogene Daten verarbeiten, eine datenschutzrechtliche Prüfung durchgeführt wird.			
7.6	Im Falle einer Verletzung des Schutzes personenbezogener Bestandsdaten meldet der Diensteanbieter nach Artikel 33 Absatz 1 DSGVO unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen datenschutzrechtlichen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Es müssen definierte Prozesse für die Meldung der Datenschutzverletzungen und Verantwortlichkeiten für diese Tätigkeit eingerichtet sein. Es muss gewährleistet sein, dass, wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, der Auftragsverarbeiter diese dem Diensteanbieter unverzüglich meldet. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. Dabei ist zu betrachten, ob in der Vergangenheit die Vorschriften beachtet wurden und gegebenenfalls Meldungen erfolgt sind.			
7.7	Wenn personenbezogene Verkehrsdaten unrechtmäßig Dritten zur Kenntnis gelangen und schwerwiegende Beeinträchtigungen der nutzenden Person drohen, ist eine Meldung nach § 169 TKG an die Bundesnetzagentur sowie an die oder den BfDI erforderlich. Es müssen definierte Prozesse für diese Meldung und Verantwortlichkeiten für diese Tätigkeit eingerichtet sein. Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. Dabei ist auch zu betrachten, ob in der Vergangenheit die Vorschriften beachtet wurden und gegebenenfalls Meldungen erfolgt sind.			
7.8	Wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so führt nach Artikel 35 DSGVO der Diensteanbieter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Es ist zu begutachten, in welcher Art und Weise diese Anforderung umgesetzt wird und ob Datenschutzfolgeabschätzungen durchgeführt wurden. Dabei ist auch zu betrachten, ob für alle Verarbeitungsvorgänge die Erforderlichkeit einer Datenschutzfolgenabschätzung geprüft wurde.			

Nr.	Kriterium	Prüfung/ Erläuterung Umsetzung	Empfehlung	Ergebnis
7.9	Nach Artikel 37 Absatz 1 DSGVO hat der Diensteanbieter unter bestimmten Bedingungen einen Datenschutzbeauftragten zu benennen. Als Datenschutzbeauftragte dürfen nur Personen mit entsprechender Fachkunde auf dem Gebiet des Datenschutzrechts und mit der Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben (Artikel 37 Absatz 5 DSGVO) bestellt werden. Der Diensteanbieter muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen (Artikel 37 Absatz 7 DSGVO). Der Diensteanbieter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird (Artikel 38 Absatz 1 DSGVO). Der Datenschutzbeauftragte darf bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhalten (Artikel 38 Absatz 3 Satz 1 DSGVO). Der Diensteanbieter stellt dem Datenschutzbeauftragen die für seine Aufgabenerfüllung notwendigen Ressourcen zur Verfügung (§ 38 Absatz 3 Satz 1 DSGVO). Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Diensteanbieters (§ 38 Absatz 3 Satz 3 DSGVO). Es ist zu begutachten, wie diese Anforderungen im Einzelnen umgesetzt werden. Dabei ist auch zu betrachten, wie der Datenschutzbeauftragte in die Prozesse der Beauskunftung von betroffenen Personen eingebunden ist.			