Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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 Str. 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 4
II. Kriterienkatalog 4
III. Gestaltung des Gutachtens 5
IV. Fachliche Eignung für die Gutachtenerstellung 5
V. Veröffentlichung 6
VI. Webadressen 6
VII. Technische Richtlinien 6
VIII. Abkürzungsverzeichnis 7

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

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

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.

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.

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

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
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