Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail[1]

Orientierungshilfe des Arbeitskreises
„Technische und organisatorische Datenschutzfragen"

Stand: 13. März 2020

1 Zielstellung

Die vorliegende Orientierungshilfe zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter[2] auf dem Transportweg zu erfüllen sind. Diese Anforderungen richten sich nach den Vorgaben des Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DS-GVO. Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen.

Verantwortliche und Auftragsverarbeiter[3] sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind. Sie setzt voraus, dass die Verantwortlichen bzw. ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können.

Die Orientierungshilfe geht von typischen Verarbeitungssituationen aus. Sie bestimmt hierbei ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung der Risiken zu treffen haben. Die Verantwortlichen und Auftragsverarbeiter sind verpflichtet, die Besonderheiten ihrer Verarbeitungen, darunter insbesondere den Umfang, die Umstände und die Zwecke der vorgesehenen Übermittlungsvorgänge zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können. Dabei müssen sie berücksichtigen, dass die vorliegende Orientierungshilfe ausschließlich Risiken betrachtet, die sich auf dem Transportweg ergeben. Risiken, denen ruhende Daten wie bereits empfangene E-Mails ausgesetzt sind oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet und können weitere Maßnahmen oder eine andere Gewichtung der im Folgenden aufgeführten Maßnahmen notwendig

[1] Die Orientierungshilfe wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Bayerns beschlossen.

[2] Diensteanbieter, die eigene oder fremde E-Mail Dienste zur öffentlichen Nutzung bereithalten

[3] Auftragsverarbeiter ausschließlich im Hinblick auf ihre Pflichten nach Art. 32 DS-GVO.

machen. Können die Anforderungen an eine sichere Übermittlung per E-Mail nicht erfüllt werden, so muss ein anderer Kommunikationskanal gewählt werden[4].

2 Anwendungsbereich und Grundsätze

Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen[5]. Dieser Schutz muss abseits des Blickwinkels dieser Orientierungshilfe ergänzt werden durch Maßnahmen zum Schutz der beteiligten Systeme und zur Minimierung, Speicherbegrenzung und Zweckbindung der auf diesen Servern verarbeiteten Verkehrsdaten.

Diese Orientierungshilfe thematisiert den Vertraulichkeitsschutz der personenbezogenen Inhalte der E-Mail-Nachrichten lediglich insoweit, wie diese nicht bereits vorab (z. B. anwendungsspezifisch) gemäß dem Stand der Technik so verschlüsselt wurden, dass nur der Empfänger sie entschlüsseln kann.

Sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten. Daher müssen Verantwortliche beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen.

Der durchgreifendste Schutz der Vertraulichkeit der Inhaltsdaten wird durch Ende-zu-Ende-Verschlüsselung erreicht, wofür derzeit die Internet-Standards S/MIME (RFC 5751) und OpenPGP (RFC 4880) i.d.R. in Verbindung mit PGP/MIME (RFC 3156) zur Verfügung stehen. Ende-zu-Ende-Verschlüsselung schützt nicht nur den Transportweg, sondern auch ruhende Daten. Bei Ende-zu-Ende-Verschlüsselung kann die Verarbeitung unverschlüsselter Inhaltsdaten auf besonders geschützte Netzsegmente bzw. auf solche Teile des Netzes beschränkt werden, die ausschließlich zur Nutzung durch Befugte (wie eine Personalabteilung oder einen Amtsarzt) vorgesehen sind.

Der Einsatz von Transportverschlüsselung bietet einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht.

Die Transportverschlüsselung reduziert die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Um auch gegen Dritte zu bestehen, die aktiv in den Netzverkehr eingreifen, muss sie in qualifizierter Weise durchgeführt und durch Maßnahmen zur kryptografischen Absicherung der Angaben der Empfänger über die zur Entgegennahme der Nachrichten berechtigten Geräte flankiert werden.

Eine Darstellung der Anforderungen an die einfache und an die qualifizierte obligatorische Transportverschlüsselung sowie an die Ende-zu-Ende-Verschlüsselung und die Signatur von E-Mail-Nachrichten ist in Abschnitt 5 niedergelegt.

---

[4] Für die Kommunikation mit betroffenen natürlichen Personen (z. B. mit Kunden) kann ein Kommunikationsweg in der Bereitstellung eines Webportals bestehen.

[5] Informationen über die Umstände der Kommunikation lassen sich verschiedenen Verarbeitungsprozessen entnehmen, die mit Versand und Empfang von E-Mail-Nachrichten in Verbindung stehen (vom Abruf von Angaben aus dem DNS bis zur Protokollierung der Kommunikation auf verschiedenen Geräten). Diese Orientierungshilfe thematisiert lediglich den Schutz der in den Kopfzeilen einer E-Mail-Nachricht enthaltenen Angaben während des Transports der Nachricht.

3 Die Inanspruchnahme von E-Mail-Diensteanbietern

3.1 Grundlegende technische Anforderungen an die Erbringung von E-Mail-Diensten

Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der TR 03108-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten.

Dies bedeutet, dass sie verpflichtend die in dieser Technischen Richtlinie niedergelegten Voraussetzungen für einen geschützten Empfang von Nachrichten schaffen und bei dem Versand von Nachrichten in Bezug auf die Anwendung von kryptografischen Algorithmen und die Überprüfung der Authentizität und Autorisierung der Gegenstelle den unter den gegebenen Bedingungen auf Empfängerseite bestmöglichen mit verhältnismäßigen Mitteln erreichbaren Schutz erzielen müssen.

3.2 Sorgfaltspflicht bei der Inanspruchnahme von E-Mail-Diensteanbietern

Verantwortliche, die öffentliche E-Mail-Diensteanbieter in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DS-GVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung eigener Systeme und Endgeräte an die Diensteanbieter ein.

Darüber hinaus müssen die Verantwortlichen die Risiken sorgfältig einschätzen, die mit dem Bruch der Vertraulichkeit und Integrität von E-Mail-Nachrichten verbunden sind, die sie versenden oder gezielt empfangen. In Abhängigkeit von diesen Risiken können sich die im Folgenden dargestellten zusätzlichen Anforderungen ergeben, deren Erfüllung sie durch Weisung an den Diensteanbieter (z. B. durch Vornahme geeigneter Konfigurationseinstellungen, soweit solche von dem Diensteanbieter angeboten werden) durchsetzen müssen.

4 Fallgruppen

4.1 Gezielte Entgegennahme von personenbezogenen Daten in den Inhalten von E-Mail-Nachrichten

Verantwortliche, die gezielt personenbezogene Daten per E-Mail entgegennehmen, z. B. durch explizite Vereinbarung des Austauschs personenbezogener Daten per E-Mail oder die Aufforderung auf der Homepage, personenbezogene Daten per E-Mail zu übermitteln, haben die im Folgenden beschriebenen Verpflichtungen zu erfüllen.

4.1.1 Verpflichtungen bei normalen Risiken[6]

Der Schutz von Vertraulichkeit und Integrität von personenbezogenen Daten bei der Übermittlung von E-Mail-Nachrichten setzt voraus, dass Sender und Empfänger zusammenarbeiten. Die Verantwortung für den einzelnen Übermittlungsvorgang liegt bei dem Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen (direkt per SMTPS oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss und hierbei ausschließlich die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf. Um den Aufbau verschlüsselter Verbindungen zu erleichtern, sollte der Verantwortliche für Verschlüsselung und Authentifizierung ein möglichst breites Spektrum an qualifizierten Algorithmen anbieten.

Um die Authentizität und Integrität der empfangenen E-Mail-Nachrichten zu überprüfen, sollten Verantwortliche DKIM-Signaturen prüfen und signierte Nachrichten, bei denen die Prüfung fehlschlägt,

[6] Zur Einstufung von Risiken s. das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder „Risiko für die Rechte und Freiheiten natürlicher Personen", abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr_18_Risiko.pdf.

markieren oder, bei entsprechender Festlegung des Absenders über einen DMARC-Eintrag im DNS, zurückweisen.

4.1.2 Verpflichtungen bei hohen Risiken

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte Transportverschlüsselung (s. u. Nr. 5.2) als auch den Empfang von Ende zu Ende verschlüsselter Nachrichten ermöglichen.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei den der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen (s. u. Nr. 5.4).

4.2 Versand von E-Mail-Nachrichten

4.2.1 Verpflichtungen bei normalen Risiken

Alle Verantwortliche, die E-Mail-Nachrichten mit personenbezogenen Daten versenden, bei denen ein Bruch der Vertraulichkeit (des Inhalts oder Umstände der Kommunikation, soweit sie sich auf natürliche Personen beziehen) ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen.

4.2.2 Versand von E-Mail-Nachrichten bei hohem Risiko

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese (s. Kap. Ende-zu-Ende-Verschlüsselung) oder an die qualifizierte Transportverschlüsselung (z. B. DANE oder DNSSEC) verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

4.2.3 Versand von E-Mail-Nachrichten mit geheim zu haltenden Inhalten bei hohen Risiken

Verantwortliche, die aufgrund von § 203 StGB zur Geheimhaltung von Kommunikationsinhalten verpflichtet sind, müssen über die unter 4.2.1 bzw. 4.2.2 aufgeführten Anforderungen hinaus durch Verschlüsselung sicherstellen, dass nur Stellen eine Entschlüsselung vornehmen können, an die die Inhalte der Nachrichten offenbart werden dürfen.

5 Anforderungen an die Verschlüsselungs- und Signaturverfahren

5.1 Obligatorische Transportverschlüsselung

Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Sie kann über das Protokoll SMTPS oder durch Aufruf des SMTP-Befehls STARTTLS und den nachfolgenden Aufbau eines mit dem Protokoll TLS verschlüsselten Kommunikationskanals realisiert werden, wobei die Anforderungen der TR 02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen sind.

Bei dem letztgenannten Verfahren (STARTTLS) kann die obligatorische Transportverschlüsselung durch entsprechende Konfiguration des sendenden MTA (Mail Transfer Agent) erreicht werden – die entsprechenden Konfigurationseinstellungen werden (En)Forced TLS, Mandatory TLS o. ä. genannt. Unterstützt die Gegenstelle kein TLS, dann wird der Verbindungsaufbau abgebrochen. Einige MTA ermöglichen eine domänenspezifische oder regelbasierte Spezifizierung dieses Verhaltens.

5.2 Qualifizierte Transportverschlüsselung

Transportverschlüsselung erreicht unter folgenden Voraussetzungen einen ausreichenden Schutz gegen aktive Angriffe von Dritten, die in der Lage sind, den Netzwerkverkehr auf der Übermittlungsstrecke zu manipulieren:

1. Die eingesetzten kryptografischen Algorithmen und Protokolle entsprechen dem Stand der Technik: Sie erfüllen die Anforderungen der Technischen Richtlinie BSI TR-02102-2 und garantieren Perfect Forward Secrecy.

2. Die Bezeichnung der zum Empfang autorisierten Mailserver und ihre IP-Adressen wurden auf Empfängerseite per DNSSEC signiert. Die Signaturen der DNS-Einträge werden auf Senderseite überprüft. Alternativ kann die Bezeichnung der zum Empfang autorisierten Mailserver auch durch Kommunikation mit dem Empfänger verifiziert werden.

3. Der empfangende Server wird im Zuge des Aufbaus der verschlüsselten Verbindung entweder zertifikatsbasiert authentifiziert oder anhand eines öffentlichen oder geheimen Schlüssels, der über einen anderen Kanal zwischen Sender und Empfänger abgestimmt wurde.

4. Erfolgt die Authentifizierung zertifikatsbasiert, so führt der Empfänger die Authentizität des Zertifikats auf ein vertrauenswürdiges Wurzelzertifikat bzw. einen via DANE publizierten Vertrauensanker zurück.

Die Einhaltung dieser Anforderungen muss nachgewiesen werden.

5.3 Ende-zu-Ende-Verschlüsselung

Durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP ist es möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

1. Der Verantwortliche muss die öffentlichen Schlüssel der Empfänger auf die Einhaltung hinreichender Sicherheitsparameter (insbesondere einer hinreichenden Schlüssellänge) überprüfen, sie durch Verifikation der Zertifikate bzw. Beglaubigungen authentisieren, vor jedem Versand bzw. Signaturprüfung auf Gültigkeit überprüfen und zuverlässig verwalten.

2. Die Überprüfung der Authentizität eines Schlüssels kann regelmäßig durch Verifikation eines Zertifikats eines vertrauenswürdigen Zertifikatsdienstanbieters (S/MIME) oder Beglaubigung anderer vertrauenswürdiger und nachweislich zuverlässiger Dritter (OpenPGP) erfolgen. Es sei ausdrücklich darauf hingewiesen, dass die Veröffentlichung eines Schlüssels auf einem OpenPGP-Schlüsselserver kein Indiz für die Authentizität dieses Schlüssels ist. Die Überprüfung des Fingerprints eines OpenPGP-Keys ist für die Überprüfung der Authentizität eines Schlüssels ausreichend, sofern der Fingerprint mit einer sicheren kryptografischen Hashfunktion (s. BSI TR-02102) ermittelt und die Authentizität des Vergleichswerts z. B. durch direkte Kommunikation mit dem Empfänger über einen anderen Kanal überprüft wurde.

3. Die Authentizität eines über Web Key Directory (WKD) bereitgestellten öffentlichen Schlüssels ist äquivalent zu der Authentizität des bereitstellenden Webservers. Für die Überprüfung gelten die Anforderungen an die Überprüfung der Authentizität des empfangenden Mailservers entsprechend.

4. Diese Anforderung kann auch nachträglich in Bezug auf Schlüssel erfüllt werden, die zunächst opportunistisch ausgetauscht wurden (z. B. per Autocrypt). Hierzu ist eine Verifikation der Authentizität über einen anderen Kanal erforderlich.

5. Die Überprüfung der Gültigkeit eines S/MIME-Schlüssels vor seinem Einsatz soll durch Abruf von Gültigkeitsinformationen bei dem Zertifikatsdiensteanbieter (Abruf von CRL via http, OCSP) erfolgen. Die Überprüfung der Gültigkeit eines OpenPGP-Schlüssels ist nur möglich, wenn der Eigner bekannt gegeben hat, wo er ggf. Revokationszertifikate zu veröffentlichen beabsichtigt. Dies kann z. B. ein OpenPGP-Schlüsselserver oder die Webseite des Schlüsseleigners sein. Sofern es an einer solchen Abrufmöglichkeit fehlt, müssen Garantien dafür bestehen, dass alle Nutzer eines Schlüssels unverzüglich informiert werden, wenn dieser seine Gültigkeit – insbesondere aufgrund einer Kompromittierung des zugehörigen privaten Schlüssels – verliert.

Wer Nachrichten Ende zu Ende verschlüsselt, sollte beachten, dass Perfect Forward Secrecy durch Ende-zu-Ende-Verschlüsselung allein nicht gegeben ist, so dass eine Kompromittierung des privaten Schlüssels eines Empfängers alle Nachrichten gefährdet, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden. E-Mail-Nachrichten, die von Dritten abgefangen werden, können von diesen aufbewahrt und bei Offenlegung des privaten Schlüssels eines der Empfänger zu einem späteren Zeitpunkt entschlüsselt werden.

5.4 Signatur

Durch eine Signatur mit den Verfahren S/MIME und OpenPGP ist es möglich, die Integrität der Inhalte einer E-Mail-Nachricht nachhaltig gegen unbefugte Beeinträchtigung zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

Sender müssen die eigenen Signaturschlüssel mit hinreichenden Sicherheitsparametern erzeugen, die privaten Schlüssel sicher speichern und nutzen; soweit kein direkter Abgleich der Schlüssel zwischen Sender und Empfänger stattfindet, die korrespondierenden öffentlichen Schlüssel von zuverlässigen und vertrauenswürdigen Dritten zertifizieren lassen und sie ihren Kommunikationspartnern zur Verfügung stellen. Empfänger sollen in Abhängigkeit von den Authentizitäts- und Integritätsrisiken die in Kap. Ende-zu-Ende-Verschlüsselung aufgeführten Maßnahmen auf die Überprüfung und das Management der Schlüssel der Sender in entsprechender Weise anwenden.