SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Schutz von Berufsgeheimnissen in E-Mails

Hinweise für Berufsgeheimnisträger (m/w/d) zu den Anforderungen an die datenschutzkonforme Verarbeitung personenbezogener Daten per E-Mail

Vorbemerkungen

Werden so genannte besondere Kategorien personenbezogener Daten und auch Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet, ist bei unbefugter Offenlegung in den meisten Fällen ein hoher Schaden zu erwarten. Daher muss ein erhöhtes Schutzniveau hergestellt werden (vgl. Art. 9, 10, 25 und 32 der Europäischen Datenschutz-Grundverordnung - DS-GVO, ggf. in Verbindung mit § 22 des Bundesdatenschutzgesetzes - BDSG). Bei den besonderen Kategorien personenbezogener Daten handelt es sich um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Diese Datenkategorien werden häufig in besonderem Umfang von Berufsgeheimnisträgern verarbeitet. Dies sind z. B. Ärzte, Psychotherapeuten, Apotheker, Physiotherapeuten, Rechtsanwälte, Notare, Steuerberater, Sozialarbeiter[1] sowie Beschäftigte von staatlich anerkannten Beratungsstellen und privaten Kranken-, Unfall- oder Lebensversicherungen. Auch deren Beschäftigte, mitwirkende Personen und Auftragsverarbeiter müssen die Daten in gleichem Maße schützen. Dass hier besondere Anforderungen gelten, ergibt sich auch strafrechtlich aus § 203 des Strafgesetzbuches (StGB) und teilweise auch aus berufsrechtlichen Regelungen.

Die Herstellung von Vertraulichkeit wird auch und gerade bei elektronischer Kommunikation durch die DS-GVO explizit gefordert. Nach Art. 5 Abs. 1 lit. f DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Grundsatz der Integrität und Vertraulichkeit). Art. 24 Abs. 1, Art. 25 Abs. 2, Art. 32 Abs. 1 lit. a DS-GVO regeln dies näher.

In einer unverschlüsselten E-Mail werden etwaige Daten vollkommen ungeschützt in einem von jedermann lesbaren Klartextformat (ASCII, TXT, PDF, DOCX, XLSX usw.) mit öffentlichen und umfänglich bekannten Protokollen (TCP/IP, SMTP) über eine nicht bekannte Route in einem weltweiten Netzwerk (Internet) transportiert. Mit technischen Mitteln kann eine solche E-Mail abgefangen, mitgelesen, kopiert oder verändert werden. *Das Versenden einer unverschlüsselten E-Mail mit personenbezogenen Daten ohne Umsetzung irgendeiner Sicherheitsmaßnahme ist daher als unzulässig einzustufen.*

Da gemäß Art. 32 Abs. 1 DS-GVO das Schutzniveau dem Risiko angemessen sein muss, gilt es abzuschätzen, wie sensibel die übertragenen Informationen sind. Dabei spielt hinsichtlich der Schädigung einer Person durch Offenlegung im Wesentlichen die Eintrittswahrscheinlichkeit und das Schadenausmaß eine Rolle. Werden z. B. Daten von vielen

[1] Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Betroffenen unbefugt offengelegt, steigt die Wahrscheinlichkeit, dass eine Person dabei ist, die dadurch eine Schädigung erleidet. Werden von wenigen Personen sehr detaillierte Daten in großem Umfang unbefugt offengelegt, steigt das Ausmaß des Schadens, den eine einzelne Person erleiden könnte. Beide Faktoren können für sich das Gesamtrisiko erhöhen und eine angemessene Reaktion durch erhöhte Sicherheitsmaßnahmen erfordern.

Einwilligung ist keine Lösung

Eine Einwilligung der betroffenen Personen als Rechtsgrundlage der Datenverarbeitung ist kein taugliches Mittel, die Vorgaben der Art. 25 und 32 DS-GVO zu unterschreiten. Die Einwilligung nach Art. 7 DS-GVO dient der Frage, „ob" eine Verarbeitung zulässig ist. Die technischen und organisatorischen Vorgaben des Art. 32 DS-GVO geben dem Verantwortlichen grundsätzlich verbindlich vor, „wie" eine Datenverarbeitung durchzuführen ist. *Ein standardmäßiges Einholen von Einwilligungen zur Unterschreitung der technischen und organisatorischen Maßgaben ist damit nicht zu vereinbaren.*

Allerdings könnte die betroffene Person im Einzelfall gegenüber dem Verantwortlichen erklären, dass kein nennenswerter Schaden droht, auch wenn eine unbefugte Offenlegung wahrscheinlich eintreten könnte. Diese Erklärung kann der Verantwortliche berücksichtigen, um zu bewerten, ob eine Datenverarbeitung auf einem geringeren Schutzniveau zulässig sein kann. So kann es ausnahmsweise zulässig sein, auf ein ausdrückliches und dokumentiertes Verlangen der betroffenen Person, welches auf ihrer freien Entscheidung beruht, ein ansonsten nach Art. 32 DS-GVO erforderliches Schutzniveau zu unterschreiten (Beispiel: Patient verlangt wegen Eilbedürftigkeit den unverschlüsselten Versand einer Impfbescheinigung per E-Mail).

Nichts geht ohne Transportverschlüsselung

Das Mindestmaß ist nach aktuellem Stand der Technik die *Transportverschlüsselung ab dem Protokoll TLS 1.2* (vgl. Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik TR 02102-2). Dabei muss jedoch sichergestellt sein, dass die E-Mail nur übermittelt wird, wenn *auch die Gegenstelle*, der Empfänger, die Transportverschlüsselung unterstützt. Dies kann *auf organisatorische Weise (Überprüfung) oder durch die Konfiguration einer obligatorischen (qualifizierten) Transportverschlüsselung* (Forced TLS, Mandatory TLS o. ä.) geschehen. Ist die obligatorische Transportverschlüsselung aktiviert (z. B. durch den Standard DNSSEC bzw. das Protokoll DANE), wird eine E-Mail nur übermittelt, wenn auch die Server der Domain der jeweiligen Empfänger-E-Mail-Adresse (der Teil hinter dem @) die Transportverschlüsselung TLS unterstützen. Falls die obligatorische Transportverschlüsselung nicht technisch erzwungen wird, kann der Verantwortliche die Fähigkeit der Empfängerserver zur Transportverschlüsselung auf Webseiten wie https://www.checktls.com/TestReceiver überprüfen.

Diese technischen und organisatorischen Mindestanforderungen müssen umgesetzt und dabei sichergestellt sein, dass der eigene E-Mail-Provider und der Provider des Kommunikationspartners diese Protokolle unterstützen und *bei allen eigenen E-Mail-Clients* die entsprechenden Einstellungen vorgenommen wurden.

Mit diesen Einstellungen können Verantwortliche beispielsweise einfache Terminbestätigungen versenden, aus denen keinerlei Daten nach Art. 9 oder 10 DS-GVO hervorgehen, oder um Rückruf bitten.

Besonders schützenswerte Daten nur mit weiteren Maßnahmen

Lassen sich allein aus der Terminbestätigung oder Rückrufbitte allerdings besondere Kategorien personenbezogener Daten ableiten (z. B. bei einer Nachricht einer psycho- oder strahlentherapeutischen Praxis oder eines Fachanwalts für Strafrecht) oder wird die Nachricht mit weiteren Informationen angereichert (z. B. um was für einen Termin oder um welches Thema es sich handelt, was zu besprechen sein wird oder was die Person zum Termin mitbringen soll), müssen weitere Schutzmaßnahmen hinzutreten. Erst recht gilt dies, wenn detaillierte Daten(-sammlungen) nach Art. 9 bzw. 10 DS-GVO per E-Mail übermittelt werden sollen (z. B. Aufklärungsbögen mit Angabe der Diagnose oder geplanten Behandlung, Anamnesedaten, Verordnungen, Befundberichte, vollständige Schriftsätze, Vertragsangebote/-entwürfe, Leistungsabrechnungen, Schadensmeldungen).

Notwendig ist dann eine *Ende-zu-Ende-Verschlüsselung*. Diese kann z. B. mit den schlüsselbasierten Verfahren S/MIME (RFC 5751) oder OpenPGP (RFC 4880) i. d. R. in Verbindung mit PGP/MIME (RFC 3156) erreicht werden.

Alternativ ist es auch möglich, *Daten in einem verschlüsselten Anhang in einer obligatorisch transportverschlüsselten E-Mail* zu übermitteln. Bei diesem E-Mail-Anhang können einzelne Dokumente oder Dokumentenpakete mit einer hinreichend sicheren Verschlüsselung nach dem aktuellen Stand der Technik belegt werden. Bei den Dateiformaten DOCX, XLSX, PDF und ZIP ist dies mit gängiger Software in der Regel problemlos möglich.

Passwort-/Schlüsselmanagement

Der in der täglichen Praxis gut handhabbaren Vergabe und Verwaltung der Schlüssel kommt eine zentrale Bedeutung zu.

Bei der Ende-zu-Ende-Verschlüsselung kommen asymmetrische Verschlüsselungsverfahren zum Einsatz. Dabei wird zum Verschlüsseln einer Nachricht ein öffentlicher (nicht geheimer, aber dem Empfänger zugehöriger) Schlüssel genutzt, jedoch kann nur der Besitzer des dazu passenden privaten (geheimen) Schlüssels die Nachricht entschlüsseln. Es muss also kein Geheimnis (Passwort) ausgetauscht werden. Der Absender der E-Mail benötigt einmalig vor der ersten Übermittlung einer E-Mail den öffentlichen Schlüssel der E-Mail-Adresse des Empfängers. Dieser Schlüssel kann zusammen mit den Stammdaten der betroffenen Person elektronisch gespeichert bzw. im E-Mail-Programm hinterlegt werden.

Im Fall eines symmetrisch verschlüsselten E-Mail-Anhangs wird ein Passwort (auch „Schlüssel“ genannt) vergeben, das sowohl zur Ver- als auch zur Entschlüsselung verwendet wird. Dieses muss dem Empfänger *getrennt von der verschlüsselten Information, möglichst auf einem anderen Kommunikationsweg* als dem, der für die Daten selbst gewählt wurde, übermittelt werden. Möglich ist beispielsweise die persönliche oder telefonische Mitteilung, niemals eine vorangeschickte unverschlüsselte E-Mail.

Das Schutzniveau der Verschlüsselung hängt zudem von der *Sicherheit des gewählten Passwortes* ab. Passwörter sollten so lang wie möglich gewählt werden. Mit steigender Rechenleistung können zukünftig auch Passwörter, die aktuell als sicher gelten, gebrochen werden.

Es ist zulässig, zu Beginn des Vertragsverhältnisses mit der betroffenen Person oder bei erstmaliger Übermittlung einer E-Mail ein Passwort zu vereinbaren, das für alle künftigen Dateianhänge gilt. Dabei ist zu beachten, dass das Passwort selbst *keine personenbezogenen Daten der betroffenen Person* enthält und *keinem Muster* folgt, das für Dritte (z. B. andere Kunden/Patienten/Klienten des Verantwortlichen) nachvollziehbar und reproduzierbar ist.

Um Kompromittierung vorzubeugen, sollten diese Passwörter und auch der private Schlüssel des Verantwortlichen bei der Ende-zu-Ende-Verschlüsselung *nicht ungeschützt in der elektronischen Dateiablage* des Verantwortlichen gespeichert werden. Es empfiehlt sich einen Passwortmanager zu nutzen oder eine Papiernotiz, die verschlossen abgelegt wird.

Prüfen Sie auch die Empfängeradresse

Beim Verfassen einer E-Mail ist besondere Sorgfalt zu verwenden, um *Schreibfehler in der Adresse des Empfängers* zu *vermeiden*. Die Empfängeradresse sollte gut leserlich in Druckbuchstaben vorliegen. Der Verantwortliche sollte sie idealerweise im Vier-Augen-Prinzip im Adressbuch seines E-Mail-Programms abspeichern und in die Adressleiste einer E-Mail stets nur die gespeicherte Adresse aus dem Adressbuch aufnehmen.

Falls die obligatorische Transportverschlüsselung nicht technisch erzwungen wird, ist die *Fähigkeit der Empfängerserver zur Transportverschlüsselung* zu überprüfen (siehe Seite 2 oben).

Und auch der E-Mail-Provider selbst kann datenschutzrechtliche Risiken mit sich bringen. Für bestimmte Dienste von Anbietern aus Drittstaaten ist allgemein bekannt, dass die Einhaltung des von der DS-GVO geforderten Datenschutzniveaus fraglich ist. Wenn mit der Übermittlung einer E-Mail verbunden ist, dass personenbezogene Daten an Empfänger in einem so genannten Drittland außerhalb der EU und des europäischen Wirtschaftsraumes offenbart werden, sind die Vorgaben von Art. 44 ff DS-GVO zu beachten. Für Datenübermittlungen in die USA und andere Drittstaaten muss z. B. besonders genau geprüft werden (vgl. Urteil des Europäischen Gerichtshofs vom 16. Juli 2020, Az. C-311/18, „Schrems II“). Ein Verantwortlicher sollte somit *keinesfalls einen E-Mail-Provider nutzen, der sich nicht nach europäischen Datenschutzstandards richtet*. Aber auch wenn ein Verantwortlicher Nachrichten an Empfänger übermittelt, die offensichtlich derartige Dienste nutzen, wäre dies grundsätzlich dem Verantwortlichen zuzurechnen.

Bereits den E-Mail-Eingang schützen

Schon bevor ein Verantwortlicher seinen Patienten, Klienten, Kunden den Kommunikationsweg E-Mail eröffnet, müssen die technischen Voraussetzungen geschaffen sein, um nicht nur beim Versand, sondern auch *bereits beim Empfang von E-Mails die erforderliche Datensicherheit* herzustellen. Daraus folgt, dass schon in dem Moment, in dem den betroffenen Personen die E-Mail-Adresse des Verantwortlichen bekanntgegeben wird (z. B. auf Briefbögen oder auf der Homepage des/der Verantwortlichen), eine sichere Kommunikation zu ermöglichen ist.

Die *eigene IT-Infrastruktur* bzw. die des eigenen Providers oder Dienstleisters muss demnach zumindest transportverschlüsselte E-Mails empfangen können. Zudem sollte den Betroffenen - sofern vorhanden - der für die Ende-zu-Ende-Verschlüsselung *notwendige öffentliche Schlüssel des Verantwortlichen zugänglich* sein. Falls der Verantwortliche keine Ende-zu-Ende-Verschlüsselung unterstützt, sollten die Betroffenen darauf hingewiesen werden, dass die nötige Datensicherheit bei der Übermittlung von sensiblen Daten ohne anderweitige Schutzmaßnahmen nicht gewährleistet ist.

Außerdem sollte der Verantwortliche darauf achten, dass er einen *Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO* mit seinem E-Mail-Anbieter abgeschlossen hat, sofern auf dessen Servern E-Mails (zwischen-)gespeichert werden.

Alternativen zur E-Mail-Kommunikation

Anstatt der Übermittlung per E-Mail kann der Verantwortliche den betroffenen Personen Nachrichten, die besondere Kategorien personenbezogener Daten enthalten, auch auf einer mit technischen Mitteln hinreichend geschützten Internetseite bereitstellen (z. B. in einem Postfach im passwortgeschützten Kundenbereich).

Ggf. können Messengerlösungen mit Ende-zu-Ende-Verschlüsselung eine Alternative zur Datenübermittlung per E-Mail darstellen. Dann muss allerdings besonderes Augenmerk auf die Auswahl eines sicheren Messengers, der die Datenschutzgrundsätze der DS-GVO umsetzt, gelegt werden. Insbesondere von marktgängigen Messengerdiensten U.S.-amerikanischer Anbieter ist dann jedoch abzusehen, da diese die Vorgaben der DS-GVO regelmäßig nicht einzuhalten vermögen.

Weitere Informationen

Weitere detaillierte, insbesondere technische Hinweise haben die Datenschutzaufsichtsbehörden in ihrem gemeinsamen Kurzpapier Nr. 17 zum Thema „Besondere Kategorien personenbezogener Daten“ (abrufbar unter https://lsaurl.de/Kurzpapiere) sowie im Detail in der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ zusammengestellt. Sie ist abrufbar unter https://lsaurl.de/OHEMail.

Impressum
Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Otto-von-Guericke-Str. 34a
39104 Magdeburg
Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de
Stand: Mai 2021
Bildnachweis: fotolia