Orientierungshilfe zum E – Mail - Versand

Orientierungshilfe der Konferenz der unabhängigen Datenschutz-aufsichtsbehörden des Bundes und der Länder Stand 16.06.2021[1]

Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind … ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail. Risiken, denen ruhende Daten, wie bereits empfangene E-Mails ... oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet. 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. (Auszüge)[1]

1. Auswahl des Dienstanbieters

Für die Verantwortlichen gilt eine Sorgfaltspflicht bei der Auswahl des E – Mail – Dienstanbieters. Dieser sollte hinreichend die Einhaltung der DS-GVO (u.a. kryptografische Algorithmen, Authentifizierung und Autorisierung der Gegenstelle) einschließlich technischer Richtlinien bestätigen bzw. garantieren. Orientierungsprofil ist die technische Richtlinie TR-03108 des BSI.[2]

2. Anforderungen bei normalen Risiken für die Betroffenen

(a) Eine obligatorische Transportverschlüsselung

(Protokolle: SMTPS, STARTTLS, TLS) nach dem Anforderungsprofil TR-02102 des BSI[3] gilt als Basisschutz bzw. Mindestanforderung. Einen unverschlüsselte Verbindung ist auszuschließen. Bei Entgegennahme von personenbezogenen Daten per E – Mail (z. B. über die Homepage) ist der Empfänger verpflichtet mit einem möglichst breiten Spektrum die Voraussetzungen für einen verschlüsselten Empfang zu gewährleisten bzw. zu schaffen. Die Verantwortung für die Übermittlung liegt beim Sender. E – Mail Signaturen sind zwingend zu prüfen und bei Fehlermeldungen an den Absender zurückzusenden.

(b) Voraussetzung einer qualifizierte Transportverschlüsselung

Kryptografische Algorithmen und Protokolle nach dem Stand der Technik (BSI TR-02102[3]), DNSSEC – Signatur (Sicherheitsmechanismus zur Authentizität und Integrität) und authentifizierten, zertifikatsbasierter Server

3. Anforderungen bei hohen Risiken für die Betroffenen

(a) Generell Transportverschlüsselung und Ende-zu-Ende Verschlüsselung.

Diese schützt nicht nur den Transport per E-Mail, sondern auch „ruhende Daten“ im Posteingang, bei Weiterleitung u. ä., wenn der Schlüssel dazu nur von Berechtigten vorgehalten wird. Aktuelle Standards lt. DSK: „S/MIME (RFC 5751) und OpenPGP (RFC 4880) i.d.R. in Verbindung mit PGP/MIME (RFC 3156)“1. In welchem Umfang auf einzelne Maßnahmen verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

(b) Prüfroutine

Hinreiche Sicherheits- und Echtheitsprüfung von Zertifikaten oder öffentlichen Schlüsseln. Bei automatischem Austausch (z. B. Perfect Forward Secrecy) ist eine Verifizierung über einen anderen Kanal zwingend vorzunehmen. Eigene Schlüssel sollten mit hinreichenden Sicherheitsparameter erzeugt werden.

1 *Quelle: DSK – Orientierungshilfe „Schutzmaßnahmen bei E-Mail Übermittlung (Verschlüsselung)"*
2 *LINK: BSI TR-03108 "Sicherer E - Mail - Transport"*
3 *LINK: BSI TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“*

Für den eiligen Leser kurz zusammengetragen (2/2)

4. Besondere Anforderungen bei Berufsgeheimnisträgern

Berufsgeheimnisse (z.B. Rechtsanwälte*innen, Ärzt*innen u.a.) stellen ein Indiz für eine hohes Risiko dar (Erwägungsgrund 75 DS-GVO) und sind deshalb in ihrer Höhe für die Betroffenen besonders zu prüfen, unabhängig von anderen gesetzlichen Vorschriften (z.B. §203 StGB)[4]. Grundsätzlich gilt die Anforderungen für hohe Risiken einzuhalten, sofern sich nicht aus den konkreten Umstände ein normales Risiko ergibt.

5. Können Betroffene auf Schutzmaßnahmen verzichten?

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im Fazit eines 11-seitigen „Vermerks“ Stand April 2021[5] es wie folgt festgehalten:

> *Der Verantwortliche und der Auftragsverarbeiter haben die nach Art. 32 DSGVO (Sicherheit in der Verarbeitung) erforderlichen Maßnahmen zwingend umzusetzen und vorzuhalten. Betroffene Personen können in die Herabsetzung des nach Art. 32 DSGVO vorgesehenen Schutzniveaus allerdings bezogen auf ihre eigenen Daten im Einzelfall einwilligen, wenn die Einwilligung freiwillig im Sinne des Art. 7 DSGVO erfolgt. Dies setzt jedoch voraus, dass der Verantwortliche die nach Art. 32 DSGVO erforderlichen Schutzvorkehrungen grundsätzlich vorhält und der betroffenen Person auf Verlangen zur Verfügung stellt, ohne dass der betroffenen Person Nachteile dadurch entstehen.*

(a) JA, Voraussetzungen sind:

1.) Der Verantwortlich muss die erforderlichen Schutzmaßnahmen in jedem Fall vorhalten!

2.) Die Bedingungen für eine Einwilligung nach Art 7 DSGVO sind zwingend einzuhalten!

(b) Zur Einwilligung

- Die Einwilligung ist in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so zu halten und von anderen Sachverhalten klar zu unterscheiden.
- Die Betroffenen sollten / müssen über die Möglichkeiten und vor allem den Risiken aufgeklärt sein.
- Die Freiwilligkeit ohne Zwang, also die Wahlmöglichkeiten muss dem gegebenen Umstand in größtmöglichen Umfang Rechnung tragen.
- Als Nachweis ist die Einwilligung eindeutig zu dokumentieren.

(c) Aber Vorsicht!

Den Ausführungen des HambBFDI ist zu entnehmen, dass es ausschließlich im Interesse der Betroffenen liegen darf, da der Verantwortlich die erforderlichen Schutzmaßnahmen in jedem Fall zur Verfügung halten muss. Beispiele sind hier:
Zu einer unsicheren Datenverarbeitung darf nicht gezwungen werden, wer eine Onlinedienst nutzt, einen Arzt oder Rechtsanwalt seiner Wahl aufsuchen möchte. Auch höhere Alternativkosten oder verlängerte Bearbeitungszeiten sprechen gegen die Freiwilligkeit.

Liebe(r) Leser(in)*

**Datenschutz praktisch, einfach, unkompliziert,
einfach einmal sprechen!**

Vielen Dank für Ihr Interesse

4 *LINK: §203 StGB „Verletzung von Privatgeheimnissen“*
5 *Quelle: Vermerk des HmbBfDI zur Abdingbarkeit von technisch-organisatorischen Maßnahmen (Art. 32 DSGVO)*