## Sicherheit beim E-Mail-Versand: Wie viel Verschlüsselung muss sein?

*Erreicht meine E-Mail den Empfänger auf dem Sicherheitsniveau einer Postkarte? Wie sicher sind die Daten, die ich per Mail verschicke? Wann ist eine angemessene Datensicherheit gewahrt und ein Verstoß gegen die DSGVO damit ausgeschlossen? Wir haben eine neue Orientierungshilfe der Datenschutzkonferenz zum Thema Verschlüsselung für Sie genauer betrachtet.*

Die Datenschutzkonferenz erläutert in einer neuen Orientierungshilfe, welche Schutzmaßnahmen Unternehmen bei der Kommunikation per E-Mail einhalten müssen.

In der Pflicht sind dabei Empfänger und Absender: Einige Verschlüsselungsmaßnahmen können nur durch beide Kommunikationspartner wirksam umgesetzt werden. Deshalb haben sowohl die Sender als auch die Empfänger von E-Mails die notwendigen technischen Maßnahmen zu ergreifen, um die Sicherheit und Vertraulichkeit der Kommunikation zu gewährleisten.

**Risiken unzureichender Verschlüsselung**

Eine unzureichende Verschlüsselung kann einen Datenschutzverstoß begründen. Dies kann zu einer Verwarnung führen (siehe hierzu das Verfahren vor dem VG Mainz, über das wir im Newsletter aus April 2021 berichteten). Möglich sind abhängig vom Einzelfall (Verschulden, Ausmaß, Schäden) auch Bußgelder und Schadensersatzansprüche von Betroffenen.

Neben dem Datenschutzrecht müssen Unternehmen auch eine andere Folge unzureichender Verschlüsselung beachten, die zu ganz erheblichen kommerziellen Schäden führen kann: Unternehmens-Know-How und andere sensible Informationen sind nach dem Geschäftsgeheimnisschutzgesetz nur dann Geschäftsgeheimnisse, wenn Unternehmen hinreichende Schutzmaßnahmen ergreifen. Die Verschlüsselung von E-Mails könnte eine solche erforderliche

Schutzmaßnahme sein … Mehr dazu können Sie hier im Geheimnis-blog lesen.

**Verschlüsselungsstandards in der E-Mail-Kommunikation**

Die Verschlüsselung von Daten ist eine geeignete technische Schutzmaßnahme, um die Datensicherheit zu gewährleisten. Art. 32 DSGVO sagt dies ausdrücklich. Bei der E-Mail-Kommunikation kommen grundsätzlich zwei Arten der Verschlüsselung in Betracht:

- Die **Transportverschlüsselung** als „äußere Hülle" in zwei Formen:
    - einfache Transportverschlüsselung
    - qualifizierte Transportverschlüsselung

    Die **einfache Transportverschlüsselung basiert** häufig auf den weit verbreiteten SSL oder TLS-Protokollen. Die **qualifizierte Transportverschlüsselung** wird durch weitere kryptografische Authentifizierungselemente ergänzt. So kann durch die Nutzung einer Kombination aus öffentlichen und privaten Schlüsseln etwa sichergestellt werden, dass die Geräte und Server, mit denen auf die Emails zugegriffen wird, auch tatsächlich die berechtigten Geräte des Empfängers sind (über die dahinterstehende Verschlüsselungstechnik informiert das BSI).

    Sobald die E-Mail auf dem Server des Empfängers angekommen ist, wird sie entschlüsselt. Dies geschieht auf der Grundlage symmetrischer Schlüssel, das heißt sowohl der Versender wie auch der Empfänger nutzen denselben Schlüssel. Die Transportverschlüsselung stellt einen Schutz der Kommunikation gegen passives Abfangen während des Übermittlungsvorgangs dar (daher **Transport**verschlüsselung). Ihr Nachteil ist, dass entschlüsselte Emails von den Servern abgegriffen werden können.

- **Ende-zu-Ende-Verschlüsselung der Inhalte**

    Bei der **Ende-zu-Ende-Verschlüsselung** wird die E-Mail nicht nur auf dem Transportweg, sondern auch bei der Zwischen- und Weiterverarbeitung auf dem Server des Empfängers verschlüsselt. Durch die Nutzung spezifischer Verfahren wie

S/MIME oder OpenPGP werden asymmetrische öffentliche und private Schlüssel kombiniert: Die Nachricht wird mit einem öffentlichen Schlüssel verschlüsselt, kann aber nur mittels des privaten Schlüssels, den nur die berechtigten Empfänger haben, entschlüsselt werden.

Der Vorteil dieses Verfahrens ist, dass der Zugriff unbefugter Dritter weitestgehend ausgeschlossen ist. Einen Überblick über gängige Verfahren und Tools bietet das BSI. Wird die E-Mail abgefangen, können die Inhalte nicht gelesen werden: Sie werden erst beim Empfänger mit einem bei diesem vorhandenen Schlüssel entschlüsselt. *(mehr dazu beim Bundesamt für Sicherheit in der Informationstechnik und der Datenschutzkonferenz)*

**Welche Verschlüsselung ist wann zu wählen?**

Für die Auswahl des Verschlüsselungsgrades gilt der risikobasierte Ansatz des Art. 32 DSGVO. Dies bedeutet: Je höher das Risiko für die Betroffenen, desto sicherer muss die E-Mail verschlüsselt werden. Dabei ist sowohl der Inhalt der Daten zu berücksichtigen, als auch das Risiko, dass auf diese im Laufe der Kommunikation (Transport und/oder Speicherung) zugegriffen wird.

1. *Unternehmen müssen **zertifizierte E-Mail-Provider** wählen*

   Der E-Mail-Provider sollte die Zertifizierung über die Einhaltung der technischen Anforderungen der Technischen Richtlinie 03108-1 des BSI erhalten haben (Erläuterungen im Überblick des BSI). Dies stellt sicher, dass die wesentlichen technischen Voraussetzungen für eine angemessene Verschlüsselung über den E-Mail-Provider, etwa durch entsprechende Anweisungen oder Konfigurationen, mit diesem auch umgesetzt werden können.

2. *Immer* **einfache Transportverschlüsselung** *bei personenbezogenen Daten*

   Wenn E-Mails mit personenbezogenen Daten (also praktisch immer) verschickt werden, müssen diese immer (einfach) transportverschlüsselt sein (so die Aufsichtsbehörden). Die Transportverschlüsselung stellt das Mindestmaß dar, um eine angemessene Datensicherheit zu erreichen. Die Verschlüsselung sollte die Anforderungen der Technischen Richtlinie

02102-2 des BSI erfüllen und über die SMTPS und TLS-Protokolle aufgebaut sein; umfassende Hinweise zur Verwendung von TLS nach der Technischen Richtlinie 02102-2 veröffentlichte das BSI (siehe auch die Leitlinie des BSI).

3. ***Qualifizierte Transportverschlüsselung*** *bei höherem Risiko,* ***Ende-zu-Ende-Verschlüsselung*** *bei hohem Risiko, z.B. bei Gehaltsdaten, Gesundheitsdaten, Gewerkschaftsinformationen u.v.m.*

   Für die E-Mail-Kommunikation mit hohen Risiken ist für eine angemessene Datensicherheit regelmäßig die Ende-zu-Ende-Verschlüsselung oder zumindest die qualifizierte Transportverschlüsselung zu wählen. Ob die Ende-zu-Ende-Verschlüsselung oder die qualifizierte Transportverschlüsselung erforderlich ist, hängt aber auch nach der Auffassung der Datenschutzkonferenz von den für die Betroffenen bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und etwaiger Kompensationsmaßnahmen ab.

   Entsprechend müssen Versender und Empfänger die technische Infrastruktur schaffen, um diesen Verschlüsselungsgrad zu ermöglichen. Dies bedeutet zumindest die Einhaltung der Technischen Richtlinie 02102-2 des BSI. Für die Ausgestaltung einer zuverlässigen Ende-zu-Ende-Verschlüsselung und den Einsatz der S/MIME und OpenPGP-Protokolle können die Hinweise des BSI beachtet werden.

**Verzicht auf eine hinreichende Verschlüsselung?**

Höchst umstritten ist, ob Betroffene selbst auch auf eine angemessene Datensicherheit beim Versand ihrer Daten per E-Mail verzichten können. Diese Frage stellt sich in der Praxis insbesondere beim Versand von Gesundheitsdaten per E-Mail.

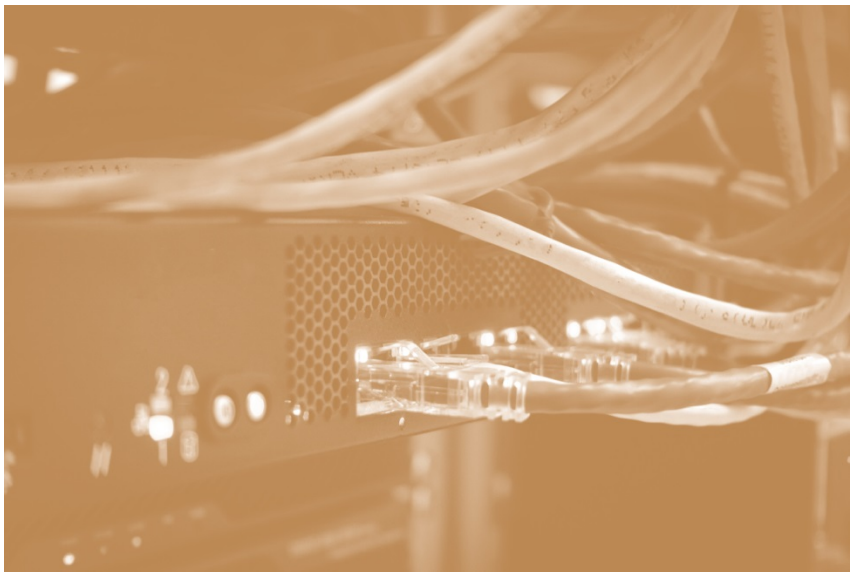
Eine Einwilligung in eine „unangemessene" niedrige Datensicherheit ist nach überzeugender Ansicht möglich, jedenfalls dann, wenn alternativ auch eine angemessene Datensicherheit angeboten wird. Dazu haben wir hier ausführlich berichtet.

Zu berücksichtigen ist aber, dass es für einen wirksamen Verzicht bzw. eine Einwilligung auf den Betroffenen ankommt. Dieser muss nicht identisch mit dem Empfänger oder dem Sender sein, sodass es hier maßgeblich auf den Inhalt der E-Mail ankommt. Daran kann

man erkennen, dass sich ein solcher Ansatz für eine unternehmensweite Handhabe grundsätzlich nicht anbietet, da sie im Alltag vom Inhalt der Mail abhängt und ggf. einer Einzelfallprüfung bedarf, was nicht praktikabel ist.

**Dokumentation der ergriffenen Maßnahmen**

Unabhängig davon, welche konkreten Verschlüsselungsmaßnahmen ergriffen wurden, sollten diese, wie die verwendeten Protokolle und Standards, umfassend dokumentiert werden. Die Datenschutzkonferenz fordert, dass die Einhaltung der im Rahmen der Orientierungshilfe aufgestellten Anforderungen an die Verschlüsselungs- und Signaturverfahren nachgewiesen werden müssen. Dies entspricht der allgemeinen Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.



## Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

## Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de