DSGVO-konformer E-Mail-Versand

Kann ich E-Mails mit SSL/TLS datenschutzkonform gemäß EU DSGVO verschlüsseln?

➡ **JEIN**, ohne Ende-zu-Ende-Verschlüsselung liegen die Inhalte auf den beteiligten Servern im Klartext vor.

Datenschutzrelevante E-Mail-Inhalte

Technisch besteht eine E-Mail aus ihrem eigentlichen Inhalt (Text, Bilder und evtl. angehängte Dateien) sowie Meta-Informationen (Absender, Empfänger, Datum und Betreff der Nachricht).

Sowohl Inhalt als auch die Metainformationen können personenbezogene Daten enthalten, deswegen müssen beide Ebenen in die datenschutzrechtliche Beurteilung einbezogen werden.

Ob der Versender eine E-Mail verschlüsseln muss, hängt vom Schutzbedarf der übertragenen Daten ab. Daten, die nach Art. 9 Abs. 1 DSGVO einen sehr hohen Schutzbedarf haben, müssen mit einer Ende-zu-Ende-Verschlüsselung gesichert werden.

Diese chiffriert den Inhalt der E-Mail. Allerdings erfasst sie nicht die Metainformationen.
Deswegen müssen die Nutzer dafür sensibilisiert werden, für den Betreff einer Nachricht einen neutralen Text zu wählen, der nicht zu viel über den Inhalt verrät.

E-Mail per TLS zu verschlüsseln

funktioniert nur bedingt. Die Gefahr, dass Sie gar nicht verschlüsseln, obwohl Sie glauben per TLS zu verschlüsseln, ist hoch. In der Regel erkennen weder Sender noch Empfänger einer E-Mail, ob mittels TLS verschlüsselt wurde oder nicht. Dies kann abhängig von den Inhalten der E-Mail zu unbequemen Rückfragen führen, da die Verschlüsselung von personenbezogenen Daten nach der Europäischen Datenschutz-Grundverordnung (EU DSGVO) nachweisbar sein muss (vgl. Kapitel 2, Artikel 5, Absatz 1 und 2):

> **Grundsätze für die Verarbeitung personenbezogener Daten (**aus Kapitel 2, Artikel 5, Absatz 1 und 2**)**
>
> 1) **Personenbezogene Daten müssen …**
>   **f)** 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 („Integrität und Vertraulichkeit“);
>
> 2) **Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).**

Der Nachweis der Verschlüsselung per TLS ist allerdings aufwändig. Zudem wird eine alternative Lösung für Fälle, in denen TLS nicht oder nur in einer veralteten, unsicheren Version verfügbar ist, benötigt. Der Sender weiß nicht ob der Empfänger TLS unterstützt / aktiviert hat, besonders bei nicht gewerblichen Empfängern! Theoretisch ist also eine Verschlüsselung per TLS EU-DSGVO konform, diese zuverlässig anzuwenden, ist jedoch schwierig und vom Sender in der Regel auch nicht zu steuern.

Möglichkeiten der Verschlüsselung

Für die Verschlüsselung der Inhalte bieten sich die beiden Verfahren S/MIME und OpenPGP an.
Beide Standards unterstützen digitale Signaturen. Sie können Manipulationen auf dem Transportweg entdecken. Beide Verfahren benötigen entsprechende Software auf beiden Seiten (Sender und Empfänger).
Außerdem müssen zuvor Schlüssel erstellt und ausgetauscht werden. Auch das kann kompliziert sein, besonders beim Kontakt zu Privatpersonen oder Erstkontakt per E-Mail!

SicherSenden von ProMaSoft,
verschlüsselt Inhalt und Anhänge in einem PDF, welches Sie mit einer normalen E-Mail versenden können.
Teilen Sie dem Empfänger das Passwort in einer getrennten Nachricht oder in umschriebener Form (Ihre KdNr + Geburtstag) mit, und er kann das PDF öffnen.
Da das PDF vor dem Senden verschlüsselt wird, sind die Daten zu jedem Zeitpunkt, auch auf den Mailservern, geschützt!
Erst der Empfänger kann sie mit dem Passwort wieder entschlüsseln!