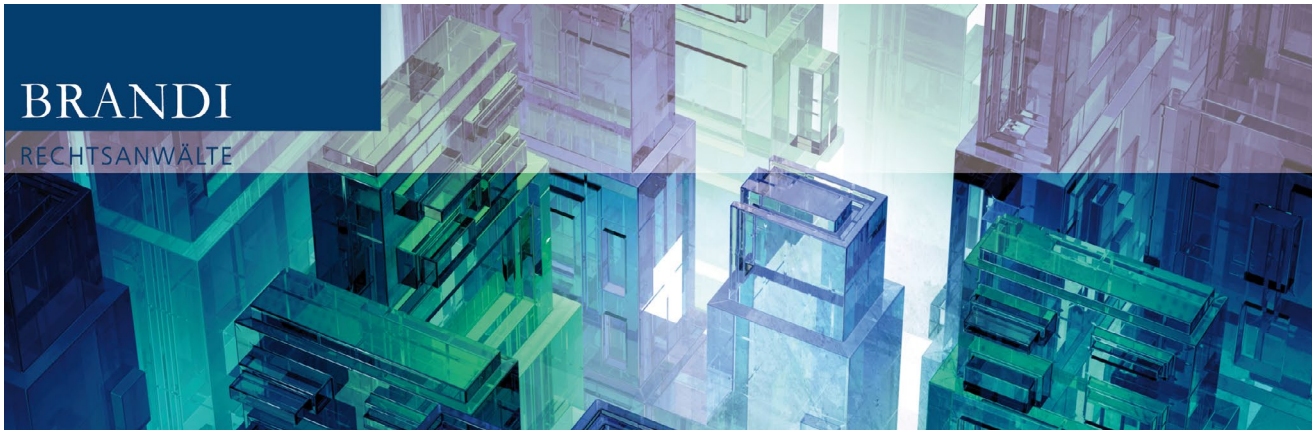

E-Mail-Verschlüsselung

Einleitung

Die Regelungen der Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 Anwendung finden, verlangen einen umfassenden Schutz von personenbezogenen Daten. Insbesondere die Anforderungen an die Datenweitergabe und Datenübermittlung werden häufig diskutiert. Abseits von etwaigen Vereinbarungen zur Auftragsverarbeitung werden insoweit auch verschiedene Schutzmaßnahmen diskutiert, die bei der Übermittlung von Daten eingehalten werden sollen. Eine von Unternehmen in diesem Zusammenhang häufig gestellte Frage ist, ob sich aus den neuen datenschutzrechtlichen Bestimmungen der DSGVO eine Pflicht zur Verschlüsselung von E-Mail-Korrespondenz ergibt.

War eine E-Mail-Verschlüsselung nach bisherigem Recht erforderlich?

Nach altem Recht war es erforderlich, bei der Verarbeitung personenbezogener Daten gemäß § 9 BDSG alte Fassung („BDSG a.F.") solche technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Sicherheit der Datenverarbeitung zu gewährleisten. Die Vorgabe gemäß § 9 BDSG a.F. wurde dahingehend ausgelegt, dass abhängig von den betroffenen Daten und deren Relevanz angemessene Maßnahmen zur, Einhaltung von Datenschutz und Datensicherheit ergriffen werden mussten. Konkrete Vorgaben, welche Schutzmaßnahmen zwingend implementiert werden müssen, gab die gesetzliche Bestimmung nicht vor. In der Aufzählung der Kategorien der technischen und organisatorischen Maßnahmen in der Anlage zu § 9 BDSG a.F. wurde die Verschlüsselung nicht erwähnt; dennoch war die Verschlüsselung von Inhalten natürlich in der Vergangenheit bereits eine übliche Schutzmaßnahme.

Was ändert sich durch die DSGVO?

Durch die DSGVO ergeben sich gegenüber der bisherigen Rechtslage grundsätzlich keine Veränderungen. In den neuen Bestimmungen heißt es weiterhin, dass geeignete technische und organisatorische Maßnahmen zu treffen sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die neue Regelung in Art. 32 DSGVO verweist dabei insbesondere auf den Stand der Technik, die Implementierungskosten sowie Art und Umfang der Datenverarbeitung. Es kommt also weiterhin darauf an, angemessene Schutzmaßnahmen zu implementieren, ohne dass diese konkret benannt werden.

Neu ist lediglich, dass die Verschlüsselung in Art. 32 Abs. 1 lit. a) DSGVO als eine von verschiedenen möglichen technischen und organisatorischen Maßnahmen explizit genannt ist. Hieraus wird teilweise abgeleitet, dass die Verschlüsselung unter der DSGVO einen höheren Stellenwert erlangt als dies noch unter den bisherigen Datenschutzbestimmungen der Fall war. Letztlich lässt sich aus der sprachlichen Änderung aber wohl lediglich ableiten, dass die Verschlüsselung jetzt aufgrund der Modernisierung der Bestimmungen als eine gängige Maßnahme explizit genannt wird, dies aber nur einen beispielhaften Charakter hat.

Letztlich würde eine grundsätzliche Vorgabe, zwingend Verschlüsselungstechnologien zu verwenden, auch gegen die Systematik der DSGVO verstoßen, wonach immer abhängig von den eigenen Möglichkeiten der Gefährdungslage angemessene Maßnahmen ergriffen werden müssen.

Wie lässt sich eine E-Mail-Verschlüsselung technisch umsetzen?

Eine E-Mail-Verschlüsselung lässt sich technisch vor allem auf zwei Arten umsetzen: Zum einen kann der gesamte Inhalt einer E-Mail verschlüsselt werden, beispielsweise durch den Einsatz von OpenPGP oder durch eine Transportverschlüsselung, z. B. den TLS-Standard. Diese Gestaltung hat den Vorteil, dass sowohl Nachrichtentext als auch E-Mail-Anhänge verschlüsselt übermittelt werden. Zur Einrichtung einer entsprechenden Verschlüsselung müssen allerdings zuvor die hierfür notwendigen technischen Maßnahmen ergriffen werden. Insbesondere muss ein Austausch der jeweiligen öffentlichen Schlüssel erfolgen, was bei einem stätig wechselnden Empfängerkreis oftmals mit erheblichem Aufwand verbunden ist.

Eine andere Möglichkeit kann insoweit die Verschlüsselung von personenbezogenen Daten in E-Mail-Anhängen sein. Hierbei wird der Anhang einer E-Mail mit allen darin enthaltenen personenbezogenen Daten verschlüsselt und das Passwort zur Entschlüsselung wird auf einem separaten Übertragungsweg, beispielsweise am Telefon, übertragen. Bei dieser Gestaltung

besteht zwar das Risiko, dass die unverschlüsselte E-Mail-Nachricht abgefangen wird. Die im Anhang verschlüsselten Daten können aber – eine ausreichende Verschlüsselung vorausgesetzt – lediglich von dem vorgesehenen Empfänger geöffnet werden.

Fazit

Es sollte regelmäßig überprüft werden, ob eine Verschlüsselung mit angemessenem Aufwand umgesetzt werden kann und zu einer spürbaren Verbesserung des Datenschutzniveaus führt. Wenn dies der Fall ist, empfiehlt sich tatsächlich, zumindest die Möglichkeit der E-Mail-Verschlüsselung anzubieten. Die Verschlüsselung von E-Mails ist dabei nicht isoliert zu betrachten, sondern immer nur im Zusammenhang mit weiteren denkbaren Schutzmaßnahmen zu sehen.

Letztlich kann immer nur die Summe aller Maßnahmen im Hinblick auf die Angemessenheit geprüft werden, nicht eine isolierte Maßnahme. Eine Aussage, dass eine E-Mail-Verschlüsselung zwingend erforderlich ist oder umgekehrt durch die E-Mail-Verschlüsselung alle rechtlichen Anforderungen erfüllt werden, ist irreführend. Im Falle einer datenschutzrechtlichen Prüfung dürfte diese vielmehr in der Form erfolgen, dass insgesamt die getroffenen Schutzmaßnahmen geschildert werden müssen, einschließlich einer etwaig implementierten Verschlüsselung. Es ist dann zu bewerten, ob die Summe der Maßnahmen zu einem angemessenen Schutzniveau führt.

Robert Bommel, LL.M. / Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 115
M sebastian.meyer@brandi.net

www.brandi.net