Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, 29.01.2019

Handreichung
zur datenschutzgerechten Nutzung von De-Mail

Einführung

Diese Handreichung möchte einen Überblick geben, wie De-Mail funktioniert, was De-Mail bezogen auf Datenschutz und Datensicherheit ausmacht, welche Vorteile die Nutzung von De-Mail bringen kann und welche datenschutzrechtlichen Anforderungen beim Versand personenbezogener Daten mittels De-Mail zu beachten sind. Sie soll damit zu einer rechtssicheren Anwendung von De-Mail-Diensten beitragen.

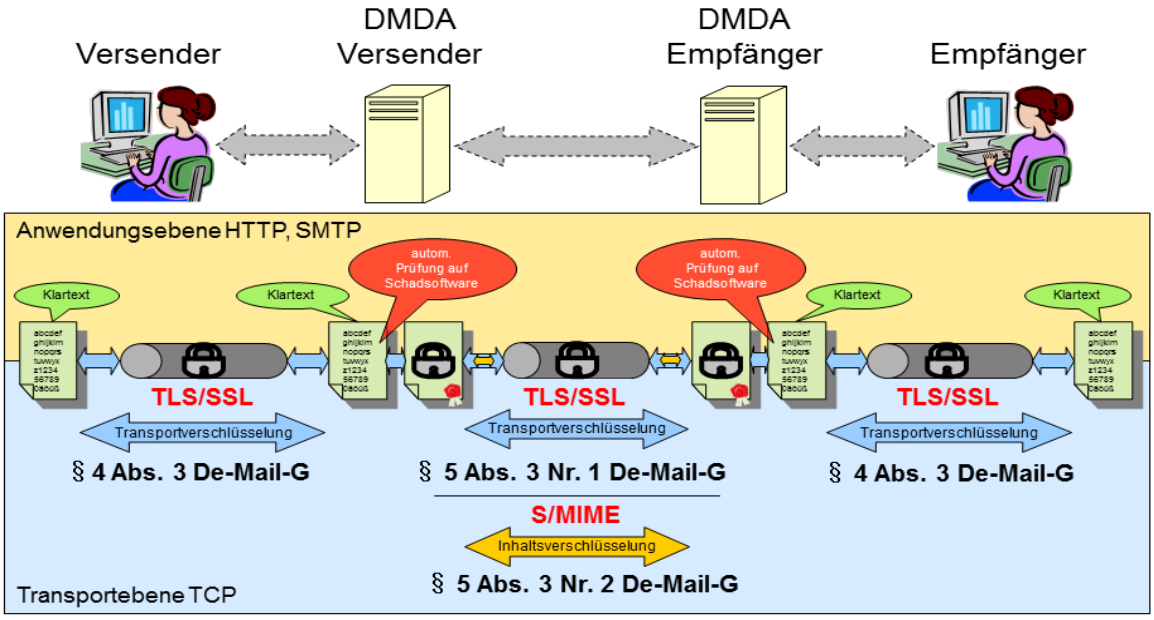
Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten, das den rechtlichen Rahmen für den De-Mail-Dienst vorgibt. De-Mail-Dienste sind nach § 1 Abs. 1 De-Mail-Gesetz Telekommunikationsdienste auf einer elektronischen Plattform, die eine sichere, vertrauliche und nachweisbare Kommunikation für jedermann im Internet gewährleisten sollen. Die De-Mail stellt letztlich eine besondere Form der E-Mail dar. Sie soll ohne zusätzliche Hard- und Software genauso einfach bedienbar sein wie die E-Mail, aber deren Nachteile ausgleichen. Im Gegensatz zur einfachen E-Mail ist die De-Mail auf dem Transport zwischen dem Postfach des Versenders und dem des Empfängers verschlüsselt und kann daher nicht von Dritten abgefangen und/oder verändert werden. Die Kommunikationspartner sind darüber hinaus authentifiziert. Zudem können Nachweise über den Versand und den Zugang von Nachrichten erstellt werden.

Aufgrund der verschiedenen Sicherheitsanforderungen ist De-Mail ein Kommunikationsverfahren, das der normalen E-Mail in jedem Fall vorzuziehen ist. Schon allein durch das notwendige Akkreditierungsverfahren, das Voraussetzung für das Anbieten des Dienstes am Markt ist, bietet De-Mail die Gewähr für ein Verfahren mit hohen Datenschutz- und Datensicherheitsanforderungen. Das Akkreditierungsverfahren wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt,

nachdem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die datenschutzrechtliche Unbedenklichkeit des De-Mail-Dienstes überprüft hat. Dazu prüfen unabhängige Sachverständige die Unternehmen anhand von Regelwerken des BSI (Technische Richtlinie De-Mail) und der BfDI (De-Mail-Kriterienkatalog).

Sicherheitskonzeption von De-Mail

Das De-Mail-Gesetz stellt einerseits Anforderungen an Datenschutz und Datensicherheit beim De-Mail-Diensteanbieter (DMDA) und regelt andererseits, wie De-Mail für die rechtssichere elektronische Kommunikation eingesetzt werden kann. Dies bedingt einige Besonderheiten im Vergleich zur Nutzung von herkömmlichen E-Mail-Diensten, so z.B. eine eindeutige Identifizierung des De-Mail-Nutzers vor der erstmaligen Kommunikation mittels De-Mail. Daher bietet De-Mail die Gewähr dafür, dass der Absender einer De-Mail zweifelsfrei festgestellt werden kann. Absende- und Eingangsbestätigungen, die mit einer qualifizierten elektronischen Signatur des DMDA versehen werden, bieten den sicheren Nachweis, dass die De-Mail versendet wurde und eingegangen ist. Dabei wird die Nachricht durch den Anbieter transport- und inhaltsverschlüsselt (vgl. Abbildung).



Nach dem De-Mail-Gesetz hat der akkreditierte DMDA sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt. Die Kommunikation von einem DMDA zu jedem anderen DMDA muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen. Zudem muss der Inhalt einer De-Mail-Nachricht vom DMDA des Versenders zum DMDA des Empfängers verschlüsselt übertragen werden.

Die technischen Details lassen sich wie folgt zusammenfassen:

- Die Nachricht vom Versender an seinen DMDA sowie vom DMDA des Empfängers an den Empfänger ist auf der Transportebene jeweils einfach durch Transportverschlüsselung gesichert.
- Die Nachricht zwischen dem DMDA des Versenders und dem DMDA des Empfängers ist doppelt gesichert: auf Anwendungsebene durch Inhaltsverschlüsselung und Signierung der Nachricht sowie auf Transportebene durch Transportverschlüsselung.
- Die Transportverschlüsselung ist eine Punkt-zu-Punkt-Verschlüsselung, weshalb die Nachricht nach dem Versand wieder unverschlüsselt vorliegt. Die Inhaltsverschlüsselung wird von der Technischen Richtlinie des BSI zu De-Mail (TR De-Mail) nur zwischen den beiden am Mailverkehr beteiligten DMDA gefordert.

§ 3 Abs. 4 Nr. 4 De-Mail-Gesetz fordert, dass der DMDA die De-Mail auf Befall mit Schadsoftware überprüfen muss. Vor dem Versand der Nachricht an den DMDA des Empfängers erfolgt entsprechend beim DMDA des Versenders in einer sowohl gegen unbefugte Zugriffe als auch gegen unberechtigten Zutritt abgesicherten Umgebung eine Überprüfung der De-Mail auf Schadsoftwarebefall. Anschließend leitet er die Nachricht zusätzlich zur Transportverschlüsselung inhaltsverschlüsselt an den DMDA des Empfängers weiter. Ist die Nachricht beim DMDA des Empfängers eingegangen, wird die verschlüsselte Nachricht wiederum in einer sowohl gegen unbefugte Zugriffe als auch gegen unberechtigten Zutritt abgesicherten Umgebung entschlüsselt und auf Schadsoftwarebefall hin geprüft. Wenn kein Befund vorliegt, wird die Nachricht verschlüsselt im Postfach des Empfängers abgelegt. Ist ein Befund vom DMDA festgestellt worden, wird die Nachricht nicht zugestellt. Sender und Empfänger erhalten stattdessen vom DMDA einen entsprechenden Hinweis auf den Befund. Dieser Prüfprozess erfolgt automatisiert auf Servern in einem Rechenzentrum des DMDA, das den IT-Sicherheitsvorgaben des BSI entspricht. Die Maßnahmen, die der DMDA aufgrund der entsprechenden Vorgaben der TR De-Mail des BSI treffen muss, umfassen Maßnahmen an das Personal sowie hinsichtlich des Zutritts und Zugangs zu den Serverräumen bzw. des Zugriffs auf Nachrichteninhalte. So muss etwa über ein ent-

sprechendes Rollen- und Rechtekonzept sichergestellt sein, dass der Zugriff auf bestimmte Daten nur durch das Zusammenwirken verschiedener Mitarbeiter möglich ist. So darf z.B. der Administrator, der für die Verwaltung der kryptografischen Schlüssel zuständig ist, keinen alleinigen Zugriff auf Nachrichteninhalte haben.

Die beschriebenen und vom BSI geprüften technischen Maßnahmen minimieren im Hinblick auf die Versendung personenbezogener Daten beim DMDA das Innentäter-Risiko, da nur überprüftes Personal entsprechend eines festgelegten Rollen- und Rechte-Konzepts zugreifen kann. Das Restrisiko besteht darin, dass sich mehrere Administratoren des Anbieters dazu verabreden könnten, vom Nachrichteninhalt Kenntnis zu nehmen. Aufgrund der vorgesehenen Protokollierungsverpflichtungen würde ein solch unbefugter Zugriff aber mit hoher Wahrscheinlichkeit dokumentiert werden und wäre damit nachvollziehbar.

Verschlüsselung als weitere Sicherungsmaßnahme

De-Mail stellt mit ihren umfassenden Sicherheitsmaßnahmen ein für die meisten Nachrichteninhalte adäquates und sicheres Kommunikationsverfahren dar. Sie ist in jedem Fall der herkömmlichen E-Mail vorzuziehen. Dennoch besteht aufgrund des beschriebenen Restrisikos die Notwendigkeit in bestimmten Fällen weitere Sicherungsmaßnahmen zu ergreifen. Gefragt sind hier die Nutzer von De-Mail selbst. Insbesondere wenn personenbezogene Daten von Betroffenen übermittelt werden, die selbst keinen Einfluss auf die Wahl des Kommunikationsverfahrens haben oder wenn durch die massenhafte Versendung von personenbezogenen Daten der Nutzer von De-Mail selbst als Angriffsziel relevant wird.

Die Ende-zu-Ende-Verschlüsselung, d.h. eine durchgängige Inhaltsverschlüsselung zwischen Versender und Empfänger, stellt eine geeignete Maßnahme dar, das Restrisiko zu mindern und bietet sich daher insbesondere für die Versendung besonders schutzbedürftiger Daten an. Allerdings kann der DMDA im Fall einer Ende-zu-Ende-Verschlüsselung keine Prüfung auf Schadsoftware durchführen.

Die akkreditierten DMDA bieten für den Privatanwender eine Ende-zu-Ende-Verschlüsselung an, deren Einrichtung und Nutzung mit wenigen und einfachen Konfigurationen möglich ist. Die DMDA stellen dafür ein Browser-Plug-in zur Verfügung, welches kostenlos installiert werden kann. Dieses Plug-in nutzt den Verschlüsselungsstandard PGP (pretty good privacy). Beim Einsatz von PGP bleibt der Nutzer Herr des privaten Schlüssels, mit dem De-Mails und Anhänge verschlüsselt werden.

Eventuellen Befürchtungen, dass der DMDA über die Schlüsselherrschaft Einsicht in die personenbezogenen Daten des Nutzers erhalten könnte, wird somit vorgebeugt. Die Unterstützung privater Nutzer durch die DMDA bei der Verwendung von Verschlüsselungsverfahren zur Absicherung der De-Mail-Kommunikation ist aus Sicht des Datenschutzes zu begrüßen.

Die Anbindung von Wirtschaftsunternehmen und Behörden an De-Mail erfolgt in der Regel über ein Gateway, d.h. im Firmen- bzw. Behördennetzwerk können normale E-Mail-Clients wie Outlook oder Lotus Notes genutzt werden, die von Hause aus die zu PGP funktionsgleiche Verschlüsselung S/MIME (Secure Multipurpose Internet Mail Extensions) unterstützen, so dass diese weitestgehend automatisiert erfolgen kann. Darüber hinaus existieren Erweiterungen, die den PGP-Standard unterstützen. Behörden stellen entweder auf ihren Web-Sites oder über den Öffentlichen Verzeichnisdienst (ÖVD) von De-Mail die erforderlichen Schlüssel für eine verschlüsselte Kommunikation zur Verfügung. Der ÖVD steht auch für die Veröffentlichung der öffentlichen Schlüssel privater Nutzer zur Verfügung.

Datenschutz/personenbezogene Daten

Es ist ein Grundsatz des Datenschutzes, dass bei der elektronischen Übertragung personenbezogener Daten die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein muss. Dies gilt erst recht bei einfachen E-Mails, aber auch bei De-Mails. Je schützenswerter Daten sind, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten, wie z.B. Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte sollen in keinem Fall Kenntnis von diesen Daten erhalten. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen. Dies gilt etwa für personenbezogene Daten an deren Verarbeitung und Nutzung besondere datenschutzrechtliche Anforderungen gestellt werden, wie z.B. die besonderen Kategorien personenbezogener Daten nach Artikel 9 Datenschutz-Grundverordnung und § 22 BDSG oder die dem Sozialdatenschutz unterfallenden personenbezogenen Daten. Bei der elektronischen Kommunikation kann die Vertraulichkeit dadurch gewährleistet werden, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt werden.
Welche Schutzmaßnahmen für personenbezogene Daten angemessen sind, ergibt sich allerdings nicht automatisch, sondern bedarf einer gesonderten Prüfung (Schutzbedarfsanalyse) durch die Versender von De-Mails, die für die Sicherstellung

datenschutzrechtlich angemessener Verfahren verantwortlich sind. Im Rahmen der Schutzbedarfsanalyse ist zu beachten, dass die durch die DMDA zu realisierenden IT-Sicherheitsmaßnahmen bereits auf die Schutzbedarfsklasse „hoch“ ausgerichtet sind. Die Vorgaben des De-Mail-Gesetzes, die TR De-Mail des BSI nach § 18 Abs. 2 De-Mail-Gesetz und der Kriterienkatalog der BfDI gemäß § 18 Abs. 3 Nr. 4 De-Mail-Gesetz machen deutlich, dass bei einer Nutzung von De-Mail das Datenschutz- und Datensicherheitsniveau im Vergleich zur herkömmlichen E-Mail-Kommunikation erheblich höher ist.

Schutzbedarf von personenbezogenen Daten

Ob eine Ende-zu-Ende-Verschlüsselung die datenschutzrechtlich angemessene Sicherungsmaßnahme darstellt, orientiert sich an dem konkreten Schutzbedarf der zu übermittelnden Daten. Dieser ist anhand der Grundschutzmethodik des BSI von der datenverarbeitenden Stelle - hier dem Versender - festzustellen:

- Bei einer Schutzbedarfsanalyse ist grundsätzlich danach zu fragen, welcher Schaden entstehen kann, wenn die Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Es muss also gefragt werden, welcher Schaden eintritt, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit), die Korrektheit der Informationen und die Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität) oder autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der Verfügbarkeit). Dabei wird zwischen den Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ unterschieden. Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene Schadensszenarien beziehen:
    - Verstöße gegen Gesetze, Vorschriften oder Verträge,
    - Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
    - Beeinträchtigungen der persönlichen Unversehrtheit,
    - Beeinträchtigungen der Aufgabenerfüllung,
    - negative Außenwirkung oder
    - finanzielle Auswirkungen.

- Bei der Schutzbedarfsanalyse ist auch der Kontext zu beachten, in dem ein Datum verwendet wird. Die Einstufung des jeweiligen personenbezogenen Datums kann je nach Kontext, in dem das Datum verwendet wird, unterschiedlich ausfallen. So ist beispielsweise der Schutzbedarf einer Adresse im Regel-

fall normal oder hoch. Befindet sich die betroffene Person aber in einem Zeugenschutzprogramm, ist der Schutzbedarf sehr hoch und die Daten dürften nur mit Ende-zu-Ende-Verschlüsselung übertragen werden.

- Im Rahmen der Schutzbedarfsanalyse muss für eine Einschätzung der notwendigen Sicherheitsmaßnahmen beim Versand personenbezogener Daten auch berücksichtigt werden, wer Versender und Empfänger der De-Mail ist. Versenden Behörden oder andere Institutionen personenbezogene Daten unmittelbar an den Betroffenen, richtet sich die Verpflichtung zur Ende-zu-Ende-Verschlüsselung grundsätzlich nach dem im Wege der Schutzbedarfsanalyse ermittelten Schutzbedarf der Daten. Daneben muss der Versender vor dem Versand das Einverständnis des potentiellen Empfängers einholen. Dies sollte mindestens einmalig für alle diesen Transportweg betreffenden Kommunikationsvorgänge erfolgen.
  Versenden Behörden oder andere Institutionen, die mit personenbezogenen Daten Dritter umgehen, solche Daten massenhaft untereinander, muss die Nachricht im Ergebnis auch ohne ein Schutzbedarfsanalyse Ende-zu-Ende verschlüsselt werden. Betrachtet man den Versand einzelner Nachrichten, würde eine Schutzbedarfsanalyse möglicherweise zu dem Ergebnis kommen, dass in bestimmten Fällen (z.B. beim Schutzbedarf „normal“) eine Ende-zu-Ende-Verschlüsselung nicht erforderlich ist. Hier muss aber berücksichtigt werden, dass im Falle eines unberechtigten Zugriffs durch die Vielzahl der versandten bzw. empfangenen Daten ein erhöhtes Angriffsrisiko und Schadenspotential vorliegt. Außerdem hat der Betroffene keine Möglichkeit zu entscheiden, auf welche Weise seine Daten versandt werden. Schließlich kann man davon ausgehen, dass Behörden oder andere Institutionen den De-Mail-Dienst über ein Gateway nutzen können und daher eine Ende-zu-Ende-Verschlüsselung in diesen Fällen mit vertretbarem technischen Aufwand möglich ist. Letztlich führt die einheitliche Behandlung aller vergleichbaren Nachrichteninhalte in diesem Kommunikationsverhältnis auch zu einer handhabbaren Anwendung für Versender und Empfänger.

Auswirkung des festgestellten Schutzbedarfs auf den Versand personenbezogener Daten

- Beim Schutzbedarf **„normal“** sind die Schadensauswirkungen begrenzt und überschaubar. Beim Versand von Daten mit dem Schutzbedarf „normal“ ist eine Ende-zu-Ende-Verschlüsselung daher nicht notwendig.

- Beim Schutzbedarf **„hoch“** können die Schadensauswirkungen beträchtlich sein. Beim Versand von Daten mit dem Schutzbedarf „hoch“ ist eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Auf sie kann nur dann verzichtet werden, wenn die datenverarbeitende Stelle anhand einer Risikoanalyse zu dem Ergebnis kommt, dass sie aufgrund der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen das Restrisiko in ihrem Verantwortungsbereich als vertretbar bewertet. Eine solche Risikoanalyse muss jedoch nicht in jedem Einzelfall vor Versendung einer einzelnen De-Mail durchgeführt werden. Vielmehr sollte sie bei regelmäßig wiederkehrenden Verfahren vorab erfolgen und die dabei anfallenden personenbezogenen Daten als Ganzes betrachten. Das Erstellen einer Risikoanalyse ist im Übrigen eine gängige Praxis vor der Einführung neuer IT-Verfahren.
  In jedem Fall sind die nach Artikel 32 Datenschutz-Grundverordnung vorgegebenen technischen und organisatorischen Maßnahmen zur IT-Sicherheit durchzuführen, damit personenbezogene Daten ihrem Schutzbedarf entsprechend verarbeitet werden können. Zusätzlich ist beim Versand von Daten mit hohem Schutzbedarf zwingende Voraussetzung, dass sich Versender und Empfänger an ihrem Konto im Sinne des § 4 Abs. 1 Satz 2 De-Mail-Gesetz mit dem Authentifizierungsniveau „hoch“ anmelden.
  Um ein angemessenes Schutzniveau bei der Versendung **besonderer Arten personenbezogener Daten** (z.B. Gesundheitsdaten) mittels De-Mail zu gewährleisten, ist aus datenschutzrechtlicher Sicht in diesen Fällen eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich, um auch das Restrisiko auf Seiten der datenverarbeitenden Stellen, d.h. der De-Mail-Nutzer, zu minimieren

- Beim Schutzbedarf **„sehr hoch“** können die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen. Beim Versand von Daten mit dem Schutzbedarf „sehr hoch“ sind eine Ende-zu-Ende-Verschlüsselung sowie weitere Maßnahmen zwingend notwendig.

Fortentwicklung

Der Entwicklungsstand der Technik und die tatsächliche Verfahrensweise im Umgang mit De-Mail sollten weiter beobachtet werden. Daraus können sich in Zukunft neue oder andere Anforderungen an die datenschutzgerechte Nutzung von De-Mail ergeben.