

WHITEPAPER



ALL ABOUT COMPLIANCE

**Edition 2018
inkl. DSGVO**

**Datenschutzkonformität und
Beweisfunktionalitäten der
GINA-Technologie von**

 **SEPPMAIL**

Inhalt

I. Hinweise	3
II. Produktinformationen zur GINA-Technologie	3
1. Alleinstellungsmerkmale	4
a) GINA ist unabhängig	4
b) GINA ist sicher	7
c) GINA ist vielseitig	7
2. Kundennutzen	8
a) Einfache Bedienbarkeit	8
b) Sicherer Datentransfer	8
c) Flexible Einsetzbarkeit	8
III. Datenschutzkonformität der GINA-Technologie	9
1. Der Anwendungsbereich des neuen europäischen Datenschutzes (DSGVO)	9
2. Datensicherheit gemäß Art. 32 DSGVO: E-Mail-Verschlüsselung	11
3. Die Verschlüsselungsmethoden der GINA-Technologie	13
IV. Beweisfunktionalitäten der GINA-Technologie	14
1. Rechtliche Grundsätze	14
a) Zugang von Erklärungen	14
b) Zugang von E-Mails	14
c) Darlegungs- und Beweisprinzipien beim Versand von E-Mails	14
2. Gestaltungsmöglichkeiten mit der GINA-Technologie	17
a) Beweiserleichterung mit GINA	17
b) Signaturen bei GINA	17
V. Fazit	18
VI. Fact Sheet	19

I. Hinweise

PRW Rechtsanwälte wurde von der SEPPmail Deutschland GmbH mit der Erstellung eines rechtlichen Whitepapers zur SEPPmail GINA-Technologie beauftragt. Die SEPPmail Deutschland GmbH stellt ihren Kunden dieses Whitepaper kostenlos und zu Informationszwecken zur Verfügung. Intention des Whitepapers ist es, einerseits einen guten Überblick über die wichtigsten Produktinformationen und Alleinstellungsmerkmale der GINA-Technologie zu geben, und andererseits eine fundierte Begutachtung hinsichtlich der Rechtsthemen Datenschutzkonformität und Beweisfunktionalitäten darzustellen. Dabei wurden in der Edition 2018 bereits die neuen gesetzlichen Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) berücksichtigt.

Die Alleinstellungsmerkmale und besonderen Kundennutzen der GINA-Technologie stehen außer Frage. GINA ist eine technische Innovation und ihre Anwender genießen viele Vorzüge. Darüber hinaus bietet das im Fokus stehende Produkt in seiner Anwendung auch nennenswerte rechtliche Vorteile. In Zusammenarbeit mit der Geschäftsleitung der SEPPmail Deutschland GmbH konnten die nachfolgenden Produktinformationen zusammengetragen und die anschließende rechtliche Begutachtung realisiert werden. Die SEPPmail Deutschland GmbH leistet mit diesem Whitepaper keine Rechtsberatung. Diese erfolgt ausschließlich über PRW Rechtsanwälte.

RA Wilfried Reiners, MBA
RAin Janina Thieme

Stand: Mai 2018

II. Produktinformationen zur GINA-Technologie

Das in der Schweiz ansässige und international tätige Unternehmen SEPPmail AG hat als Hersteller seinen Produktfokus auf die Sparte „Secure-Messaging“ gelegt. Das Unternehmen wurde 2001 gegründet und verfügt über eine siebzehnjährige Erfahrung im sicheren Versenden digitaler Nachrichten. Die Produktphilosophie von SEPPmail gründet sich auf zwei Hauptmerkmale: ein Höchstmaß an Sicherheit, in Kombination mit hohem Benutzerkomfort. Zu letzterem zählen insbesondere ein allseits verfügbarer Betrieb mit hoher Stabilität und geringem Administrationsaufwand¹. Bei der vertraulichen E-Mail-Kommunikation wird vorrangig auf die für den Nutzer transparente Verschlüsselungstechnologien von S/MIME, OpenPGP oder Domainverschlüsselung gesetzt. Für den Fall, dass der Kommunikationspartner unbekannt, oder keine sichere E-Mail Infrastruktur vorhält, hat SEPPmail als Spezialist der Branche die GINA-Technologie entwickelt. Diese patentierte Technologie kann ohne eine spezifische Secure-Mail-Infrastruktur genutzt und für den spontanen und sicheren E-Mail-Verkehr eingesetzt werden. GINA verschlüsselt elektronische Nachrichten und versieht diese auf Wunsch mit einer digitalen Signatur. Die Secure E-Mail-Lösungen von SEPPmail im Allgemeinen und die GINA-Technologie im Speziellen sind über die SEPPmail AG, die Tochtergesellschaft der SEPPmail Deutschland GmbH, sowie über zahlreiche Integrationspartner erhältlich und leisten einen nachhaltigen Beitrag zur sicheren Kommunikation mittels elektronischer Post. Das Unternehmen pflegt zudem Technologiepartnerschaften zur DATEV in Nürnberg, der Schweizerischen Post und dem Health Info Network (www.hin.ch). In diesem Netzwerk, das mit der Technologie von SEPPmail ausgestattet ist, tauschen ca. 180.000 Nutzer sensible Patientendaten aus.² Im Folgenden sollen die Alleinstellungsmerkmale und die besonderen Kundennutzen der GINA-Technologie im Einzelnen vorgestellt werden.

¹ Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH
² Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH

1. Alleinstellungsmerkmale

a) GINA ist unabhängig

GINA ist eine E-Mail-Technologie, die E-Mail-Kommunikation verschlüsselt. Verschlüsselungstechnologien sind in der Regel dann reibungslos anwendbar, wenn sowohl der Sender als auch der Empfänger über die notwendige Technologie zur Verschlüsselung und Entschlüsselung verfügen.

Was passiert aber, wenn der Empfänger nicht über die Einrichtung zur Entschlüsselung verfügt?

Genau für diese Fallkonstellation hat SEPPmail die GINA-Technologie entwickelt. Mittels GINA lassen sich verschlüsselte E-Mails auch zu Empfängern übertragen, die selbst über keine entsprechende Vorkehrung zur Entschlüsselung verfügen. Die Technologie benötigt lediglich einen Web-Browser und die Möglichkeit E-Mails zu empfangen, also einen beliebigen E-Mail-Client und Internetzugang. Weitergehende Anforderungen an die Infrastruktur des Benutzers stellt GINA nicht. Damit ist auch sichergestellt, dass die sogenannten GINA-Mails auf ausnahmslos allen Endgeräten empfangen, entschlüsselt dargestellt und verarbeitet werden können.

Ablauf des Verschlüsselungsvorgangs:

Der Sender verfasst in seinem Standard E-Mail-Client eine E-Mail und klassifiziert diese als „vertraulich“. Die als vertraulich markierte E-Mail wandert durch den Mailserver und passiert danach die SEPPmail. Die Appliance prüft bei jeder ausgehenden E-Mail, ob der oder die Empfänger schon mit eigenem Schlüsselmaterial (S/MIME, OpenPGP) erfasst sind, das heißt, ob der Empfänger schon bekannt bzw. registriert ist. Wenn die Nachricht als „vertraulich“ gekennzeichnet ist und der Empfänger noch unbekannt ist, wird die GINA Verschlüsselung angewendet.

Wenn für den Empfänger keine Schlüssel hinterlegt sind, oder dieser gänzlich „unbekannt“ ist, greift automatisch die GINA-Technologie ein.

Es wird ein AES-256 Key erzeugt, die vertrauliche E-Mail damit symmetrisch verschlüsselt und als HTML-Anhang an eine Standard-E-Mail beigefügt. Diese wird an den Empfänger versendet und die E-Mail dabei immer vollständig ausgeliefert. Auf der Appliance werden außer den Empfängerdaten keine weiteren Daten zwischengespeichert. Der Key für den Empfänger bleibt dauerhaft auf der Appliance und wird für die erste, wie für alle anderen GINA-Mails zum Verschlüsseln und Entschlüsseln für diese Empfangsadresse verwendet. Für jeden unbekanntem externen Empfänger wird ein eigener symmetrischer Schlüssel im AES-256 Format errechnet und sicher auf der Appliance abgelegt. Damit wird die komplette E-Mail inklusive Anhang RFC-konform verschlüsselt und als HTML-Text-Anhang an eine Standardträgermail beigefügt. Der Empfänger öffnet den HTML-Anhang und wird zur Eingabe seines Initialpasswortes aufgefordert. Dieses hat er im Vorfeld, auf anderem Weg z. B. per SMS oder über ein persönliches Telefonat, bereits erhalten. Damit erreicht man eine 2-faktor Authentifizierung. Etwas was man hat (E-Mail mit HTML-Textanhang als sicherer Container) und etwas was man weiß (SMS Initialpasswort). Beides benötigt man, um Zugang zu dem symmetrischen Schlüssel zur Entschlüsselung auf der Appliance zu erlangen. Anschließend erfolgt eine einmalige Registrierung im System. Ein eigenes Passwort wird vergeben.

Neuen Benutzer registrieren

Bitte geben Sie Ihren Namen und E-Mail-Adresse ein und setzen ein Passwort sowie eine Sicherheitsfrage und -antwort.

*** E-Mail-Adresse:**

Voller Name:

Sprache:

Passwortkriterien Passwort-Mindestlänge: 8

*** Neues Passwort:**

*** Passwort bestätigen:**

Passwort-Rücksetzung Bitte wählen Sie eine Sicherheitsfrage, deren Antwort nur Ihnen bekannt ist. Sie wird im Passwort-Rücksetzungs-Prozess sowohl online als auch telefonisch von unserem Support-Team verwendet werden.

*** Sicherheitsfrage:**

*** Antwort:**

Handynummer:

Bitte geben Sie die Telefonnummer im internationalen Format (z.B. 0041123456789) ein.

Danach wird die entschlüsselte E-Mail im Webmailer angezeigt. Aus diesem kann verschlüsselt geantwortet und die E-Mail, wenn gewollt, als Klartext im System gespeichert werden. Deshalb spricht man im Rahmen der Anwendung von GINA von einer spontan möglichen, verschlüsselten Email-Kommunikation.

Sichere E-Mail

Der neue Benutzer wurde erfolgreich angelegt

Beantworten | Allen antworten | Speichern als ▾

Datum: Donnerstag 09.03.2017 10:14

Von: Günter Esch <esch@seppmail.de>

An: "guenter@eschenwehr.de" <guenter@eschenwehr.de>


Betreff: GINA - Mail die Neue

Anhänge: [Günter Esch.vcf \(29.4 KB\)](#)
[SEPPmail Lösungsbeschreibung - 010316.pdf \(509.1 KB\)](#)
[SEPPmail_Productcard_DE.pdf \(1.5 MB\)](#)

Nachricht:

Die wunderbare neue GINA 8.0

mit freundlichen Grüßen – with kind regards



Günter Esch
SEPPMAIL Geschäftsbereich Vertrieb
+49 (0)1041 8999031 - Phone
+49 (0)151 16544228 - Mobil
esch@seppmail.de
www.seppmail.de

swiss made software

Beim nächsten Lesen der E-Mail oder bei einer neuen vertraulichen E-Mail, wird dann nur noch das eigene Passwort verwendet:

SEPPMAIL | Anmelden | Registrierung | Suchen | Deutsch ▾

Passwort-Login

E-Mail:

Passwort:

Anmelden | [Passwort vergessen?](#)

b) GINA ist sicher

Darüber hinaus bietet die verschlüsselte E-Mail-Kommunikation via GINA viele Vorteile hinsichtlich des Themas Sicherheit. Zum einen wird durch die Verschlüsselung die Vertraulichkeit gewahrt und zum anderen kann der Absender über die Einstellung „automatische Lesebestätigung“ nachvollziehen, ob der Empfänger seine Nachricht erhalten hat. Unter Verschlüsselung versteht man die von einem Schlüssel abhängige Umwandlung von „Klartext“ in einen „Geheimtext“. Aus dem Geheimtext kann nur unter Verwendung des geheimen Schlüssels wieder ein Klartext gewonnen werden. Wenn nur der Empfänger Inhaber des geheimen Schlüssels ist, kann nur dieser den Geheimtext wieder entschlüsseln. Somit können durch Verschlüsselung Nachrichten vertraulich übermittelt werden. Wie Eingangs schon erwähnt, benötigt der GINA-Mail-Empfänger, außer einem Client zum Empfangen von E-Mails und somit Internetzugang sowie einem Browser, keine weiteren Komponenten. Beim Öffnen des HTML-Attachments und während der Eingabe des Zugangspasswortes, wird im Hintergrund über eine https-Strecke das Passwort geprüft und die E-Mail an die SEPPmail-Appliance zur Entschlüsselung temporär eingeliefert und danach sofort wieder zur Klartextdarstellung an den GINA-Webmailserver ausgeliefert. Des Weiteren kann der Sender eine automatische Lesebestätigung anfordern, um sicher zu gehen, ob der Empfänger seine Nachricht erhalten hat.

c) GINA ist vielseitig

Außerdem ist die GINA-Technologie vielseitig einsetzbar und bietet zahlreiche individuelle Einstellungsmöglichkeiten. Alle Texte in der GINA-Oberfläche können angepasst und das Aussehen per CSS-Stylesheet verändert werden. Im Auslieferungszustand sind die Sprachen Englisch, Deutsch, Französisch, Italienisch, Spanisch, Niederländisch, Ungarisch, Russisch und Polnisch integriert. Diese können beliebig erweitert oder deaktiviert werden. Darüber hinaus sind keine zusätzlichen Technologie-Layer, bzw. Konvertierungen z. B. in PDF-, zip- oder exe-Formate notwendig. Das Zugriffspasswort kann jederzeit vom Empfänger geändert werden. Zusätzlich sind zahlreiche Passwort-Reset Möglichkeiten konfigurierbar. Hinsichtlich des Registrierungsprozesses für externe Kommunikationspartner ist noch einmal der Vorteil verschiedener Optionen des Kommunikationsbeginns herauszustellen:

Spontaner Kommunikationsbeginn

Wie oben bereits dargestellt, ist eine Möglichkeit die Kommunikation via GINA aufzunehmen, als Sender eine E-Mail zu verfassen, diese als „vertraulich“ einzustufen und sie an den Empfänger zu versenden. Hat der Absender die Mobilnummer des Empfängers, könnte er diese im Betreff schon als „Tag“ mitangeben. Die Appliance würde dann mit dem Versenden der GINA-Mail das „Tag“ aus dem Betreff löschen und gleichzeitig die SMS auslösen. Der Sender bekommt zur Kenntnisnahme das Initialpasswort und die Mitteilung der erfolgreichen Auslieferung als Informations-E-Mail übermittelt. Ansonsten wird der Sender aufgefordert, dem neuen Empfänger sein Initialpasswort auf parallelem Wege (SMS, Telefon, Fax) zu übermitteln.

Vorbereitete Kommunikation

Eine andere Möglichkeit ist, der Sender verschickt eine Einladungsmail ohne Initialpasswort an den zukünftigen Kommunikationspartner. Diese sollte OHNE vertraulichen Inhalt sein. Der Empfänger öffnet das HTML-Attachment und der beschriebene Registrierungsprozess startet. Danach kann gesichert kommuniziert werden. Der externe Kommunikationspartner hat sein eigenes Passwort dann schon im Vorfeld festgelegt. Alternativ kann sich der potentielle Empfänger natürlich auch auf Eigeninitiative - z. B. über einen auf einer Unternehmenswebsite hinterlegten Link - anmelden. Ein Link bringt den externen Kommunikationspartner auf das Registrierungsportal der SEPPmail-Appliance. Dort hinterlegt er sein Passwort (oder Schlüsselmaterial). Ein „E-Mail-Ping“ bestätigt seine Registrierung.

2. Kundennutzen

Auf Grundlage der dargestellten Alleinstellungsmerkmale können die sich daraus ergebenden Kundennutzen im Wesentlichen in drei Headlines zusammengefasst werden:

a) Einfache Bedienbarkeit

Zum einen ist die GINAMail sehr einfach bedienbar und zudem barrierefrei gestaltet. Es bedarf weder einer Softwareinstallation noch eines hohen Administrationsaufwands. Im Rahmen der Anwendung bietet GINA ein flexibles Registrierungs-, Passwort- und Schlüsselmanagement. Die E-Mail wird sofort und vollständig in das Mailsystem des Empfängers ausgeliefert. Die Appliance des Senders wird nicht mit „fremden“ Material belastet.

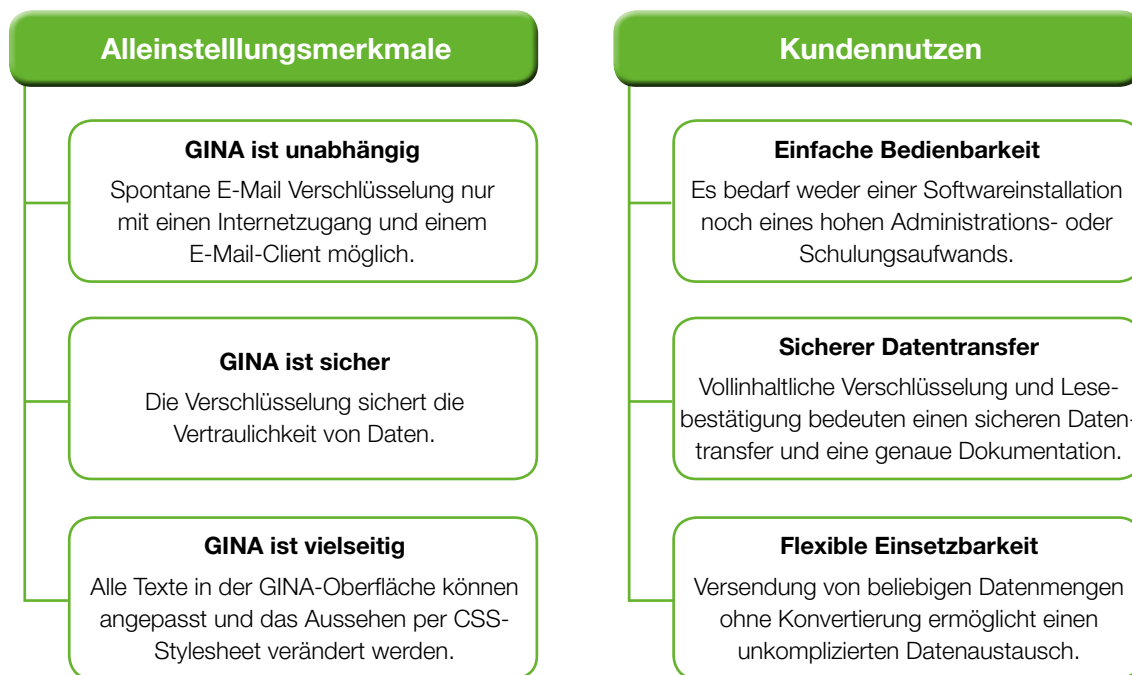
b) Sicherer Datentransfer

Die spontane und vollinhaltliche Verschlüsselung an Jedermann und die Option der Lesebestätigung bedeuten einerseits, dass Daten durch die Verschlüsselung vertraulich und sicher transferiert werden können und der Sender andererseits nachverfolgen kann, ob und wann seine Nachricht beim Empfänger eingegangen ist.

c) Flexible Einsetzbarkeit

Da mit Hilfe der GINA-Technologie beliebige Datenmengen ohne Konvertierung in andere Dateiformate verschickt werden können, ist das Email-Programm maximal flexibel einsetzbar und ermöglicht einen spontanen und unkomplizierten Datenaustausch auch mit größeren Datenmengen.

Visualisierung der GINA-Technologie



III. Datenschutzkonformität der GINA-Technologie

Hinsichtlich des Themas Datenschutzkonformität im Rahmen elektronischer Kommunikation stellen sich die Fragen, **welche datenschutzrechtlichen Vorschriften gibt es? Für wen gelten diese? Wann finden diese Anwendung? Und welche konkreten Maßnahmen können eine datenschutzkonforme E-Mail-Kommunikation gewährleisten?** Im Folgenden sollen diesen Fragen mit Bezugnahme auf die GINA-Technologie beantwortet werden.

1. Der Anwendungsbereich des neuen europäischen Datenschutzes (DSGVO)

Unter Datenschutz versteht man den Schutz des Einzelnen (des sog. Betroffenen) vor unbefugter Verwendung und Weitergabe seiner personenbezogenen Daten. Die geltenden deutschen Vorschriften zum Datenschutz sind im Bundesdatenschutzgesetz (BDSG), in den Landesdatenschutzgesetzen sowie in Spezialgesetzgebungen (beispielsweise für öffentlich-rechtliche Religionsgemeinschaften) und in bereichsspezifischen Vorschriften in anderen Gesetzen (wie dem Telemediengesetz und dem Telekommunikationsgesetz) geregelt. Für den privatwirtschaftlichen Sektor sind mit einigen wenigen Ausnahmen bisher die Vorschriften des BDSG sowie eventuell zusätzlich bereichsspezifische Vorschriften einschlägig gewesen. Die deutschen Vorschriften zum Datenschutz sind im Zuge der Umsetzung der europäischen Richtlinie zum Datenschutz 95/46/EG seit 1995 vom deutschen Gesetzgeber nach und nach entwickelt worden. Da jede europäische Nation den Datenschutz in eigener nationaler Gesetzgebung umgesetzt hat, gab es gerade bei datenschutzrechtlichen Sachverhalten mit nationsübergreifenden Bezügen in Europa, immer wieder Unsicherheiten in der praktischen Umsetzung.

Die neue europäische Datenschutz-Grundverordnung (DSGVO)³ ist Teil der EU-Datenschutzreform und ist am 25.05.2016 in Kraft getreten. Die Verordnung wird die aus dem Jahr 1995 stammende europäische Datenschutzrichtlinie 95/46/EG ersetzen und einerseits die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlichen und andererseits die Betroffenenrechte stärken. Bis 25.05.2018 läuft die zweijährige Umsetzungsfrist. Dann gilt die Verordnung unmittelbar. Bis dahin müssen die bereits in Kraft getretenen neuen gesetzlichen Anforderungen der europäischen Verordnung in die Praxis umgesetzt worden sein⁴. Darüber hinaus enthält die DSGVO einige sogenannte Konkretisierungsklauseln. Diese erlauben es den nationalen Gesetzgebern ergänzend zur unmittelbar geltenden DSGVO flankierende Regelungen als nationale Sondervorschriften zu treffen. Am 05.07.2017 wurde das am 25.05.2018 in Kraft tretende Bundesdatenschutzgesetz (BDSG-neu) als Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) (DSAnpUG-EU) 2016/679 und zur Umsetzung der Richtlinie(EU) 2016/680 im Bundesgesetzblatt (BGBl.) Teil I Nr. 44 veröffentlicht⁵. Das derzeitige Bundesdatenschutzgesetz (BDSG-alt) tritt gemäß Art. 8 des DSAnpUG-EU am 25.05.2018 außer Kraft.

Die DSGVO bedeutet die Einführung von neuen datenschutzrechtlichen Anforderungen, die die Überprüfung der vorhandenen unternehmerischen Vertrags- und Regelwerke zum Datenschutz und darüber hinaus die Entwicklung neuer gesetzeskonformer Datenschutzkonzepte erfordern. Die unternehmerische Verantwortung für eine rechtzeitige Umstellung obliegt der Geschäftsleitung. Aus den neuen Sanktionsvorschriften der DSGVO spricht der deutliche gesetzgeberische Wille, Datenschutzverstöße konsequent und empfindlich zu ahnden. „(...) Unternehmen müssen den Datenschutz daher zwangsläufig mehr als bisher in den Fokus ihrer eigenen Aufmerksamkeit nehmen.“⁶ Die Bußgeldrahmen für den Fall eines Datenschutzverstößes sind empfindlich erhöht worden. Gelten heute gemäß § 43 Abs. 3 S.1 BDSG Bußgeldobergrenzen von 300.000,00 Euro, so drohen den Unternehmen ab Mai 2018 bei Datenschutzverstößen Geldbußen von 10 bis 20 Millionen Euro oder bis zu 2 bis 4 Prozent des unternehmerischen Jahresumsatzes. Maßgeblich ist dabei der Jahresumsatz der gesamten Unternehmensgruppe, nicht der einzelnen verantwortlichen Gesellschaft.

3 <https://dejure.org/gesetze/DSGVO>

4 Art. 99 Abs. 2 DSGVO

5 Bundesgesetzblatt Jahrgang 2017 Teil 1 Nr. 44, ausgegeben zu Bonn am 5. Juli 2017, 2097

6 Website des Bayerischen Landesamtes für Datenschutzaufsicht, https://www.lida.bayern.de/media/baylda_DSGVO_7_sanctions.pdf

Ein weiterer zentraler Aspekt des Datenschutzes ist und bleibt dabei auch die Aufgabe, für die notwendige Datensicherheit zu sorgen. Die Unternehmenskonzepte und Maßnahmen zur Datensicherheit müssen nicht nur hinsichtlich technischem Fortschritt und dynamischer Bedrohungslage, sondern auch unter dem Aspekt der Rechtsfortbildung laufend überprüft und verbessert werden. Unternehmen sollten deshalb im Rahmen der Überarbeitung ihrer Datenschutzkonzepte auch ihre Datensicherheitsmaßnahmen auf den Prüfstand stellen.

Für die datenschutzrechtliche Umsetzung bedeutet dies, dass im Rahmen einer unternehmerischen Datenverarbeitung zunächst immer zu prüfen ist, ob personenbezogene Daten verarbeitet werden und ob somit die angeführten datenschutzrechtlichen Vorschriften einschlägig sind. Es ist also immer zu prüfen, ob und wer Daten erhebt oder verarbeitet und zum anderen immer festzulegen, ob es sich bei diesen erhobenen oder verarbeiteten Daten um sogenannte personenbezogene Daten handelt. Die „Verarbeitung“ gemäß Art. 4 Nr. 2 DSGVO umfasst jeden - mit oder ohne Hilfe automatisierter Verfahren - ausgeführten Vorgang, oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Gemäß Art. 4 Nr. 1 DSGVO bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Kundendaten gehören ebenso zu den personenbezogenen Daten wie die Personaldaten von Beschäftigten. Personenbezogene Kundendaten sind beispielsweise Namen von Ansprechpartnern, oder Email-Kontaktdaten. Der räumliche Anwendungsbereich umfasst gem. Art. 3 Abs. 1 DSGVO alle Verarbeitungen personenbezogener Daten, die – unabhängig vom Ort der Verarbeitung - von einem Verantwortlichen oder einem Auftragsverarbeiter mit Niederlassung in der EU durchgeführt werden.

Soweit man bei der Prüfung des Sachverhalts zu dem Ergebnis kommt, dass die geltenden Datenschutzgesetze Anwendung finden, ist desweiteren die Rechtsgrundlage der Datenverarbeitung und das angemessene Datenschutzniveau im Rahmen der Verarbeitung zu prüfen. Für die Verarbeitung von personenbezogenen Daten gilt der Grundsatz des Verbotsprinzips mit Erlaubnisvorbehalt. Datenverarbeitungen dürfen somit nur stattfinden, wenn eine Rechtsgrundlage, das heißt wenn eine Einwilligung oder ein sonstiger legitimer Rechtfertigungsgrund für die Verarbeitung, vorliegt. Diese ist einzelfallbezogen zu prüfen und wird regelmäßig unter einen Fall des Art. 6 Abs. 1 lit a) bis f) DSGVO zu subsumieren sein. Das angemessene Schutzniveau ist allgemein an Art. 32 DSGVO zu messen. Vor dem Hintergrund der geltenden Definitionen lässt sich für die unternehmerische E-Mail-Kommunikation subsumieren, dass bei Email-Kommunikation, bzw. Datentransfers via E-Mail in der Regel immer eine Verarbeitung von personenbezogenen Daten stattfindet. Da somit der datenschutzrechtliche Anwendungsbereich eröffnet ist, muss im Rahmen der unternehmerischen Email-Kommunikation desweiteren sichergestellt werden, dass die Verarbeitung personenbezogener Daten mit einem angemessenen Schutzniveau erfolgt.

2. Datensicherheit gemäß Art. 32 DSGVO: E-Mail-Verschlüsselung

Gemäß Art. 32 DSGVO muss ein angemessenes Datenschutzniveau bei der Verarbeitung von personenbezogenen Daten gewährleistet sein. Die zutreffenden Maßnahmen müssen unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein angemessenes Schutzniveau gewährleisten. Sinn und Zweck dieser Vorschrift ist es, dass auch auf technischer und organisatorischer Ebene durch Maßnahmen sichergestellt wird, dass ein dem Risiko angemessenes Schutzniveau für die im Verantwortungsbereich des Verantwortlichen bzw. Auftragsverarbeiters liegenden personenbezogenen Daten besteht.⁷ In Art. 32 DSGVO werden vier Beispiele für angemessene technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung aufgeführt. Eine Maßnahme, die ausdrücklich in Artikel 32 Abs. 1a) DSGVO zur Sicherheit der Verarbeitung personenbezogener Daten genannt wird, ist die Verschlüsselung:

Art. 32 DSGVO-Sicherheit der Verarbeitung (Original Gesetzestext)

- (1) *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
- a) *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
 - b) *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
 - c) *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
 - d) *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung*
- (2) *Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.*
- (3) *Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*
- (4) *Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.*

⁷ vgl. Tim Wybitul (Hrsg.), Handbuch EU-Datenschutzgrundverordnung, 1. Auflage 2017, Schreibaue/ Spittka, Art. 32 DSGVO, Rn. 2

Ob diese Auflistung eine generelle, gesetzliche Verschlüsselungspflicht für die geschäftliche E-Mail-Kommunikation bedeutet, ist umstritten. Dabei wird vor allem die Frage diskutiert, ob die Maßnahme der Verschlüsselung im Einzelfall über einen angemessenen Aufwand hinausgeht. Dieser Argumentation ist die aktuelle technische Entwicklung entgegenzuhalten. Verschlüsselungs- und Signaturlösungen sind auch nach Ansicht der Datenschutzaufsichtsbehörden inzwischen Stand der Technik und können mit geringem und vertretbarem Aufwand eingesetzt werden.⁸ Die Formulierung des Art. 32 DSGVO lässt Spielraum für Interpretation und einzelfallbezogene Abwägungen. Die Implementierung einzelner Maßnahmen, wie der Verschlüsselung, ist dann nicht zwingend, wenn diese durch eine Risikoanalyse nicht geboten ist⁹. Welche konkrete Sicherheitsmaßnahme im Einzelfall als angemessen einzustufen ist, ist im Rahmen einer Abwägung zu ermitteln. Hierbei sind insbesondere die möglichen Risiken bei Vernichtung, Verlust oder Veränderung, der Daten zu berücksichtigen¹⁰. Im Umkehrschluss bedeutet dies aber auch, dass soweit keine Verschlüsselung eingesetzt wird, eine solche Risikoanalyse und entsprechende Abwägung zwingend zu erfolgen hat. Anderenfalls liegt ein bußgeldbewährter Verstoß vor, da gemäß DSGVO nun auch der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen eine hart sanktionierte Ordnungswidrigkeit darstellt. Insoweit muss jede Geschäftsleitung individuell entscheiden, ob die vom Gesetzgeber angeführte technische Maßnahme umgesetzt wird, oder unter Vornahme einer Risikoanalyse und Abwägung solange darauf verzichtet wird, bis seitens der zuständigen Behörden und der Rechtsprechung eindeutige Vorgaben vorliegen. Die Geschäftsleitung der SEPPmail Deutschland GmbH bezieht dazu sowohl als Unternehmen, das selbst der Umsetzungspflicht gemäß DSGVO unterliegt, als auch als Anbieter von IT-Lösungen eindeutig folgende Stellung: „Die DSGVO fordert in Art. 32 ganz konkret die Pseudonymisierung und Verschlüsselung personenbezogener Daten. Aus unserer Sicht sollte an dieser Stelle durch Interpretation kein Risiko eingegangen werden.“¹¹

Neben der Frage, ob eine Verschlüsselungspflicht besteht, gilt zudem der datenschutzrechtliche Grundsatz, dass durch die Maßnahme einer angemessenen Verschlüsselung ein drohender Datenschutzverstoß verhindert werden kann. Wenn personenbezogene Daten angemessen verschlüsselt werden, fehlt es nach gängiger Rechtsprechung bereits an der Übermittlung personenbezogener Daten.¹² Darüber hinaus sollten Unternehmen nicht nur aufgrund einer datenschutzrechtlichen Pflicht wichtige Informationen konsequent verschlüsseln. Mit Blick auf die immer raffinierteren Methoden und dem signifikanten Anstieg der Cyber-Kriminalität¹³, dem steigenden Wert der Daten im Zeitalter der Digitalisierung und den gemäß DSGVO drohenden Bußgeldern bei Verstößen, ist es zu raten, in eine umfassende Verschlüsselungslösung zu investieren.

Auch seitens der eigenen Geschäftspartner kann eine Verschlüsselung vertraglich eingefordert werden. Zudem kann sich eine Verschlüsselungspflicht auch mittelbar aus anderen vertraglichen Pflichten ergeben. Durch Geheimhaltungsvereinbarungen, zumeist sogenannten „Non-Disclosure-Agreements“, werden Vertragsparteien zur Geheimhaltung verpflichtet.

Damit wird zwar nicht unmittelbar festgelegt, ob und wie eine Kommunikation zwischen den Vertragsparteien verschlüsselt werden muss. Vor dem Hintergrund der Geheimhaltungspflicht sind aber alle Informationen mit Vertragsbezug vor dem Zugriff Dritter zu schützen.

8 Ernestus in Simitis, BDSG, 8. Auflage, § 9 Rn. 20f.

9 vgl. Tim Wybitul (Hrsg.), Handbuch EU-Datenschutzgrundverordnung, 1. Auflage 2017, Schreibauer/Spittka, Art. 32 DSGVO, Rn. 15f.

10 vgl. Tim Wybitul (Hrsg.), Handbuch EU-Datenschutzgrundverordnung, 1. Auflage 2017, Schreibauer/Spittka, Art. 32 DSGVO, Rn. 15f.+

11 Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH, vgl. <https://www.seppmail.de/eu-dsgvo-e-mail-verschluesselung-ist-pflicht/>

12 Spies, MMR-Aktuell 2011, 313727, Kroschwald, ZD 2014, 75, 78; Körfner in Gola/Schomerus, BDSG, 12. Auflage 2015, § 3 Rn. 10a

13 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf?__blob=publicationFile&v=5

3. Die Verschlüsselungsmethoden der GINA-Technologie

Wie bereits festgestellt, dient eine angemessene Verschlüsselung als wirksame Maßnahme, um drohende Datenschutzverstöße auszuschließen. **Was aber bedeutet angemessene Verschlüsselung?** Dafür gibt es keine gesetzlich festgeschriebenen Standards. Die DSGVO gibt in Art. 32 DSGVO nichts Konkretes vor, wie eine Verschlüsselung technologisch ausgestaltet sein sollte. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt aber technische Richtlinien an die Hand, die eine Bewertung der Sicherheit vornehmen und insoweit Orientierungshilfe für die Auswahl angemessener, kryptographischer Verfahren sind. Wie bereits im Rahmen der Produktinformationen ausgeführt, arbeitet die GINA-Technologie mit einer symmetrischen Verschlüsselung mit 2-faktor-Authentifizierung. Bei symmetrischer Verschlüsselung handelt es sich um Verfahren, in denen der Verschlüsselungs- und Entschlüsselungsschlüssel gleich sind (Schlüssel-Schloss-Prinzip). Mit Einsatz von GINA verfasst der Absender eine E-Mail. Diese wird im Klartext bis zur SEPPmail-Appliance übertragen. Dann wird ein AES-256 Key erzeugt, die vertrauliche E-Mail damit symmetrisch verschlüsselt und als HTML-Anhang an eine Standard-E-Mail beigefügt. Diese wird an den Empfänger versendet und die E-Mail dabei immer vollständig ausgeliefert. Bei AES-256 (Advanced Encryption Standard) handelt es sich um einen symmetrischen Algorithmus, um eine Blockchiffre. Dieser verschlüsselt einen Klartext mit fester Bitlänge mittels eines Schlüssels zu einem Chiffretext gleicher Bitlänge, bzw. gleicher Blockgröße. Seine Funktionsweise beruht auf einer Reihe von Byteersetzungen (Substitutionen), Verwürfelung (Permutationen) und linearen Transformationen, die auf Datenblöcken von 16 Byte ausgeführt werden – daher die Bezeichnung Blockverschlüsselung. Diese Operationen werden mehrmals wiederholt, wobei in jeder dieser Runden ein individueller, aus dem Schlüssel berechneter Rundenschlüssel in die Berechnungen einfließt. Laut BSI (Stand: Januar 2018) sollten für neue Anwendungen nur noch Blockchiffren eingesetzt werden, deren Blockgröße mindestens 128 Bit beträgt.¹⁴ Die Blockchiffren AES-128, AES-192 und AES-256 werden zur Verwendung in neuen kryptographischen Systemen empfohlen.¹⁵ Die GINA-Technologie setzt hinsichtlich der symmetrischen AES-Verschlüsselung, die Blockchiffre mit der größtmöglichen Blockgröße 256 ein. Mit der von GINA im Einsatz befindlichen symmetrischen Verschlüsselung ist somit die Vertraulichkeit von Daten in datenschutzrechtlicher Hinsicht in angemessener Weise geschützt. Durch konsequenten Einsatz der GINA-Verschlüsselungstechnologie kann die Datenschutzkonformität der geschäftlichen, elektronischen Kommunikation gewährleistet werden.

¹⁴ Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, (BSI TR-02102-1), Januar 2018, S. 16

¹⁵ Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, (BSI TR-02102-1), Januar 2018, S. 16

IV. Beweisfunktionalitäten der GINA-Technologie

Die E-Mail ist seit Jahren im Geschäftsverkehr die gängigste Art der Kommunikation. Die meisten Vorgänge werden ausschließlich via E-Mail korrespondiert. Gemäß dem deutschen Zivilprozessrecht (ZPO) und dem Bürgerlichen Gesetzbuch (BGB) gilt das Prinzip, dass die Partei die sich auf Erklärungen im Geschäfts- und Rechtsverkehr berufen möchte, diese auch nachweisen muss, sprich beweibelastet ist. Kurz: „Was mir nützen soll, muss ich auch beweisen.“ Der deutsche Gesetzgeber kennt keine grundsätzlichen, rechtlichen Schranken für die Kommunikation und die Beweisführung an Hand elektronischer Dokumente. Die E-Mail ist als elektronisches Post- und Beweismittel im Geschäfts- und Rechtsverkehr anerkannt. Die aktuelle Gesetzeslage und Rechtsprechung zur Beweismittelwürdigkeit elektronischer Dokumente entwickelt sich aber deutlich langsamer, als die sich bereits im Einsatz befindlichen elektronischen Kommunikationstools. Deshalb kann bisher im Zuge dessen nur unter erschwerten und eher unpraktikablen Bedingungen elektronische Kommunikation als ein sogenannter Vollbeweis in einen Gerichtsprozess eingebracht werden. Im Vergleich dazu genießt das klassische Schriftstück in Papierform bisher noch eine größere und leichtere rechtliche Anerkennung. Auf Grundlage der gesetzlichen Anerkennung elektronischer Dokumente ist aber die Möglichkeit eröffnet, die Fragen des Zugangs, der Echtheit und Vertrauenswürdigkeit eines elektronischen Dokumentes und die Sicherheit vertraulicher Daten mit Technologien wie der GINA zu gestalten.

1. Rechtliche Grundsätze

a) Zugang von Erklärungen

Nach § 130 Abs. 1 Satz 1 BGB wird eine Erklärung, die in Abwesenheit des Empfängers abgegeben wird (also nicht von Angesicht zu Angesicht) in dem Zeitpunkt wirksam, in welchem sie dem Empfänger „zugeht“. Zugegangen ist dabei nach rechtlicher Ansicht eine Erklärung, wenn sie derart in den Machtbereich des Empfängers gelangt ist, dass er unter normalen Umständen die Möglichkeit hat, von der Erklärung Kenntnis zu nehmen.¹⁶ Auf die tatsächliche Kenntnisnahme kommt es dabei nicht an.

b) Zugang von E-Mails

Die rechtliche Bewertung „Ob“ eine E-Mail zugegangen ist, erfolgt nach den gleichen Grundsätzen. Lediglich beim Zeitpunkt, also dem „Wann“ des Zugangs ist auf Besonderheiten der elektronischen Kommunikation zu achten. Hat der Empfänger die Kommunikation mittels E-Mail eröffnet oder gestattet, geht eine E-Mail in dem Zeitpunkt zu, wenn sie in die Mailbox des Empfängers oder des Providers abrufbar gespeichert wird.¹⁷ Hat der Empfänger nicht zu erkennen gegeben, dass ihm Erklärungen auf elektronischem Wege erreichen können (ausdrückliche Mitteilung der E-Mail-Adresse), erfolgt der Zugang erst mit tatsächlicher Kenntnisnahme.

c) Darlegungs- und Beweisprinzipien beim Versand von E-Mails

Wer sich auf den Erhalt oder Nichterhalt einer E-Mail beruft, trägt grundsätzlich die Beweislast hierfür und wenn es darüber hinaus noch auf den Zeitpunkt des Zugangs ankommt, muss er auch den Zeitpunkt des Zugangs beweisen.

¹⁶ Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 130 BGB Rn. 5
¹⁷ Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 130 BGB Rn. 7a
¹⁸ BGH 70, 232

Einfache E-Mails ohne Lesebestätigung

Für den Beweis „Ob“ eine einfache E-Mail - ohne Lesebestätigung - zugegangen ist, reicht es nicht aus, darzulegen und zu beweisen, dass die E-Mail abgesandt worden ist.¹⁹ Denn unabhängig von der Frage, ob eine E-Mail abgesandt wurde, kann kein Nachweis erbracht werden, dass die Nachricht auch beim Empfänger zugegangen ist, i. S. d. § 130 BGB. Da mittels einer einfachen E-Mail nicht bewiesen werden kann, ob eine E-Mail überhaupt zugegangen ist, kann auch der Zeitpunkt, wann eine einfache E-Mail zugegangen ist nicht beweisfest dokumentiert werden. Es kann also festgehalten werden, dass die Versendung einer einfachen E-Mail ohne zusätzliche Mechanismen auf das alleinige beweisrechtliche Risiko des Absenders erfolgt. Der Absender kann nicht wissen, ob die E-Mail den Empfänger erreicht hat, bzw. wann der Empfänger die E-Mail erhalten hat. Der Empfänger hingegen kann die Integrität der E-Mail als auch die Authentizität des Absenders nicht nachvollziehen.

Beweiserleichterung durch Lesebestätigung

Der Einsatz zusätzlicher Mechanismen, wie dem Versand von E-Mails mit Eingangs- oder Lesebestätigung, kann die praktischen Beweislücken unter Umständen schließen.²⁰ Erhält der Absender eine Lese- und Empfangsbestätigung, belegt diese rein materiell-rechtlich, ob eine E-Mail zugegangen ist und darüber hinaus den spätmöglichen Zeitpunkt, also das „Wann“ des Zugangs, nämlich die tatsächliche Kenntnisnahme.²¹ Die Empfangsbestätigung kann damit prozessual einen Anscheinsbeweis für das „Ob“ und das „Wann“ des Zugangs der Erklärung sein.²² Die Praxis zieht den Anscheinsbeweis heran, wenn ein „typischer“ Geschehensablauf vorliegt, der nach der Lebenserfahrung auf eine bestimmte Ursache oder Folge hinweist und derart gewöhnlich und üblich erscheint, dass die besonderen individuellen Umstände an Bedeutung verlieren. Der Anscheinsbeweis statuiert dabei aber nur einen typischen Geschehensablauf und liefert insoweit keinen unerschütterlichen Vollbeweis.

E-Mails mit elektronischer Signatur

Möchte man eine höhere Rechtssicherheit hinsichtlich Authentizität und Integrität erreichen, steht das Sicherheitstool der elektronischen Signatur zur Verfügung. Die elektronische Signatur soll gewährleisten, dass eine Datei nicht unbemerkt von dritter Seite verändert werden kann. Um Sicherungsmittel für elektronische Transaktionen zusammenhängend und unionsweit einheitlich zu gestalten, hat die Europäische Union am 23.07.2014 die VO (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO) erlassen. Als Unionsverordnung gilt die eIDAS-VO nach Art. 288 Abs. 2 Satz 1 AEUV in allen Mitgliedstaaten unmittelbar. Im Juli 2017 ist in Deutschland das Gesetz zur Durchführung der europäischen eIDAS-Durchführungsgesetz in Kraft getreten und mit ihm das neue Vertrauensdienstegesetz (VDG). Gleichzeitig traten das Signaturgesetz (SigG) und die Signaturverordnung (SigV) außer Kraft. Die wesentlichen Regelungen zu Vertrauensdiensten enthält die eIDAS-VO. Das VDG kann wegen des Anwendungsvorrangs der Verordnung nur konkretisierende und ergänzende Regelungen enthalten. An den Begrifflichkeiten des ehemaligen SigG wird auch in der neuen eIDAS-VO festgehalten:

- einfache elektronische Signatur (Art. 3 Nr. 10 eIDAS-VO) (d. h. diese Signatur verknüpft elektronische Daten logisch miteinander, ohne dabei besondere Sicherheitsanforderungen zu erfüllen).
- fortgeschrittene elektronische Signatur (AES, advanced electronic signature) (Art. 11 und 26 eIDAS-VO) (d. h. diese Signatur ist eindeutig dem Unterzeichner zugeordnet, die ermöglicht, die Identifizierung des Unterzeichners, sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt würde).
- qualifizierte elektronische Signatur (QES) (Art. 12 eIDAS-VO) (d. h. eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit (SSEE) erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht, das von einem Zertifizierungsdiensteanbieter (Trust Center) ausgestellt wurde).

¹⁹ LAG Berlin-Brandenburg, Beschluss vom 27.11.2012 – Az. 15 Ta 2066/12

²⁰ Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 130 BGB Rn. 21

²¹ Spindler in Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 130 BGB Rn. 25

²² Spindler in Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 130 BGB Rn. 25

Die Rechtswirkung der elektronischen Signatur regelt die eIDAS-Verordnung in Artikel 25 wie folgt:

- (1) Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.*
- (2) Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.*
- (3) Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.*

Eine elektronische Signatur ist folglich ein zulässiges Beweismittel. Lediglich die qualifizierte elektronische Signatur hat aber die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Dies entspricht auch den Vorgaben der geltenden, deutschen Zivilprozessordnung. Gemäß §§ 371a Abs. 1, 416 ZPO kann die qualifizierte elektronische Signatur als „urkundsgleiches“ Beweismittel, d. h. als Vollbeweis im Prozess, geführt werden.²³ Wohingegen bei einfachen oder fortgeschritten signierten elektronischen Dokumenten der Beweiswert erschüttert werden kann. Fortgeschritten signierte Dokumente bieten aber einen faktischen Integritätsschutz, der beweisrechtlich relevant ist, da die Sicherheit der eingesetzten mathematischen Verfahren durch einen Sachverständigenbeweis bestätigt werden kann. Die abschließende rechtliche Würdigung obliegt aber allein dem zuständigen Gericht. Die für qualifizierte elektronische Signaturen zugelassenen Kryptoalgorithmen für Deutschland werden von der Bundesnetzagentur genehmigt und veröffentlicht. Dort sind auch die für eine qualifizierte elektronische Signatur zugelassenen Produkte aufgelistet. Das in Deutschland bekannteste qualifizierte elektronische Zertifikat ist der sog. neue elektronische Personalausweis (nPA). Mit dem Gesetzesentwurf der Bundesregierung „zur Förderung des elektronischen Identitätsnachweises“ (18/11279) hat der Bundestag am 18.05.2017 beschlossen, dass jeder neue Personalausweis künftig mit einer einsatzbereiten Funktion zum elektronischen Identitätsnachweis ausgegeben wird. Das Signaturzertifikat des nPA wird von einem Partner der Bundesdruckerei ausgegeben und ist nur in Kombination mit einem Kartenleser oder ein kompatibles Smartphone mit NFC-Chip und AusweisApp sowie einer Face-to-Face Kontrolle (z. B. Videochat) gültig. Mit der Interaktion von Personalausweis, Kartenlesegerät einer zusätzlichen AusweisApp und dem Signaturportal kann man das Zertifikat auf den neuen Personalausweis laden und mit einer Signatur-PIN schützen. Auch können für eine qualifizierte elektronische Signatur die Zertifikate von öffentlich akkreditierten Zertifikatsanbietern (offizielle CA) verwendet werden. Der hohe beschriebene Aufwand sorgt aber dafür, dass diese Form der elektronischen Signatur zwar maximal sicher, jedoch bisher nur wenig verbreitet im Einsatz war.²⁴

²³ Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 126a BGB Rn. 11

²⁴ Deutscher Bundestag, „Gesetzesentwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises“ (Drucksache 18/11279), 22.02.2017, Seite 2

2. Gestaltungsmöglichkeiten mit der GINA-Technologie

a) Beweiserleichterung mit GINA

Wie bereits ausgeführt, bestehen im Rahmen einer einfachen E-Mail-Kommunikation im Zweifel Beweisschwierigkeiten. Eine Lesebestätigung, kann eine Beweiserleichterung bewirken. Dabei ist zu beachten, dass die Funktion einer Lesebestätigung im Rahmen gängiger E-Mail-Programme in der Regel vom Empfänger ausgestellt werden kann. Die GINAmail generiert im Gegensatz dazu eine automatische Lesebestätigung, wenn der verschlüsselte HTML-Container der GINAmail nach korrekter Eingabe des Passwortes eingeliefert, entschlüsselt und im Klartext wieder ausgeliefert wurde. Die Funktion der automatischen Lesebestätigung kann nicht vom Empfänger ausgestellt werden. Der Absender erhält demnach auf jeden Fall eine Rückmeldung, ob und wann seine E-Mail den Empfänger erreicht hat. Die automatische Lesebestätigung kann damit immer als Anscheinsbeweis eingesetzt werden.

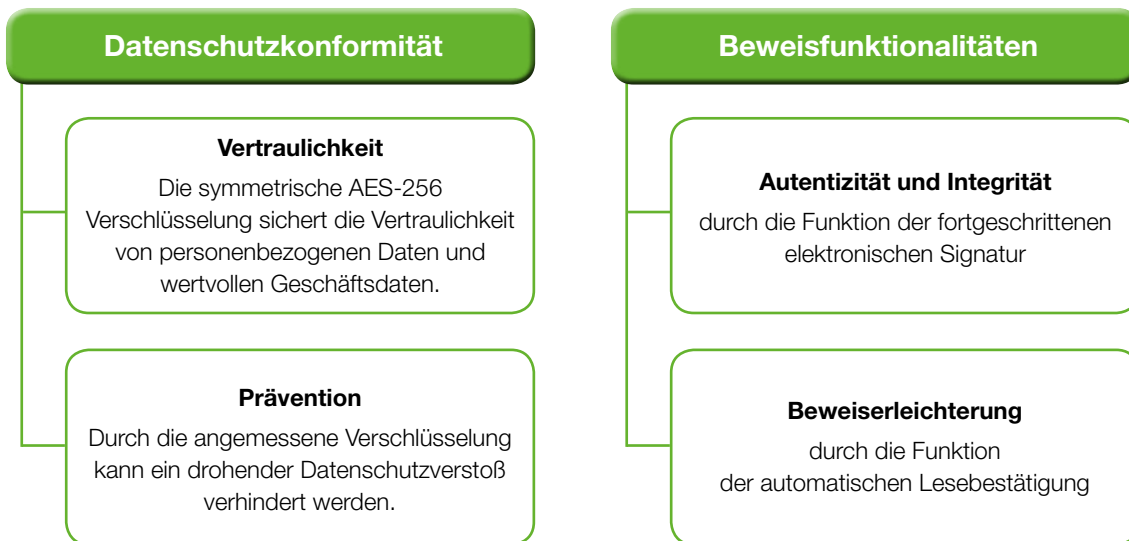
b) Signaturen bei GINA

Darüber hinaus kann jede GINAmail mit einer fortgeschrittenen elektronischen Signatur versehen werden. Die Secure E-Mail-Gateways von SEPPmail ermöglichen die digitale Signatur von E-Mails unkompliziert und schnell. Der Nutzer benötigt ein sogenannte S/MIME-Zertifikat (Schlüssel), wobei bereits vorhandene Schlüssel (S/MIME-Zertifikate und OpenPGP-Keys) sich nahtlos in SEPPmail integrieren lassen. Der Secure E-Mail-Server von SEPPmail beantragt dann bei der ersten ausgehenden Nachricht des Nutzers automatisch ein Zertifikat bei einer Zertifizierungsstelle. SEPPmail vertraut dabei auf seine Partner QuoVadis, Digicert, GlobalSign, DFN und SwissSign, anerkannte schweizerische Zertifizierungsstellen. Eine versendete GINAmail wird beim Versenden automatisch im Namen des Absenders signiert und kann sodann von keinem Außenstehenden mehr unerkannt verändert werden. Wie bereits ausgeführt, sind elektronische Dokumente mit fortgeschritten elektronischer Signatur ein zulässiges Beweismittel. Die beweisrechtliche Würdigung obliegt aber dem Spruchkörper.

V. Fazit

Die Technologie von GINA bietet den Unternehmen zum einen die Möglichkeit die eigene elektronische Kommunikation angemessen zu verschlüsseln. Durch die Verschlüsselung wird sowohl ein datenschutzkonformer Umgang mit personenbezogenen Daten als auch ein hoher Schutz der vertraulichen Unternehmensdaten erreicht. Zum anderen bietet die GINA die Möglichkeit die Authentizität und Integrität der elektronischen Geschäftspost durch Signaturen zu schützen und durch die automatische Lesebestätigung weitergehende Informationen und Beweiserleichterungen hinsichtlich des Zugangs von elektronischen Dokumenten zu erreichen. Es ist zwar festzustellen, dass vor deutschen Gerichten bisher nur unter Einsatz qualifizierter elektronischer Signaturen ein sogenannter Vollbeweis erlangt werden kann. Allerdings ist diese Funktion in der Praxis bisher zu umständlich einsetzbar, so dass der Aufwand für den alltäglichen, geschäftlichen E-Mail-Verkehr in der Regel unverhältnismäßig ist. Für die Fälle, in denen feststeht, dass die gesetzliche Schriftform erforderlich ist oder rechtserhebliche Erklärungen beweissicher abgegeben werden möchten, muss bis dato noch auf die klassische Schriftform gesetzt werden. Darüber hinaus ist der elektronische Geschäftsverkehr unter Einsatz der GINA-Technologie und den GINA-Funktionen, symmetrische Verschlüsselung und elektronische Signaturen, datenschutzkonform und sicher ausgestaltet.

Visualisierung der der GINA-Technologie



VI. Fact Sheet

PRW Rechtsanwälte

PRW RECHTSANWÄLTE hat sich auf ausgewählte Gebiete des nationalen und internationalen IT-Rechts spezialisiert, das in erheblichem Umfang auch den Bereich der IT-Compliance-relevanten Vorschriften umfasst. Der Branchenfokus der Kanzlei liegt auf der Informationstechnologie. In diesem Umfeld wurde die Kanzlei vielfach ausgezeichnet.

Autoren

Rechtsanwalt Wilfried Reiners, MBA

Studium der Rechts- und Wirtschaftswissenschaften in München und San Diego (MBA).

Nach einer mehrjährigen Tätigkeit für eine internationale Unternehmensberatung ist er seit 1989 zur Anwaltschaft zugelassen. Wilfried Reiners ist heute Managing Partner von PRW Rechtsanwälte in München und Geschäftsführer der PRW Consulting GmbH. RA Reiners ist seit 29 Jahren auf die Beratung im IT-Umfeld spezialisiert und hat zahlreiche Veröffentlichungen zum IT-Recht publiziert.

Rechtsanwältin Janina Thieme

Studium der Rechtswissenschaften und Referendariat in München mit Stationen in Hamburg und Washington DC. Nach einer mehrjährigen Tätigkeit als juristische Mitarbeiterin während der Ausbildung in den Bereichen Wirtschaftsprivatrecht und IT-Recht, ist sie seit 2016 zur Anwaltschaft zugelassen und angestellte Rechtsanwältin bei PRW Rechtsanwälte.

 **PRW**RECHTSANWÄLTE

Reiners Wilser Schloßmacher Herrmann PartG mbB

Leonrodstr. 54

D-80636 München

Telefon: +49 - (0) 89 - 21 09 77-0

Telefax: +49 - (0) 89 - 21 09 77-77

E-Mail: reiners@prw.de • office@prw.de

Web: www.prw.de