ALLABOUT COMPLIANCE

Datenschutzkonformität und Beweisfunktionalitäten der GINA-Technologie von

SEPPMAIL

Inhalt

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. 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 macht mit diesem Whitepaper keine Rechtsberatung. Diese erfolgt ausschließlich über PRW Rechtsanwälte.

RA Wilfried Reiners, MBA
RAin Janina Thieme

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 mehr als fünfzehnjährige 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 Administrationsaufwand.[1] Darüber hinaus hat SEPPmail als Spezialist der Branche die GINA-Technologie entwickelt. Diese patentierte Technologie kann ohne eine spezifische

[1] Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH

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 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 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. 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.

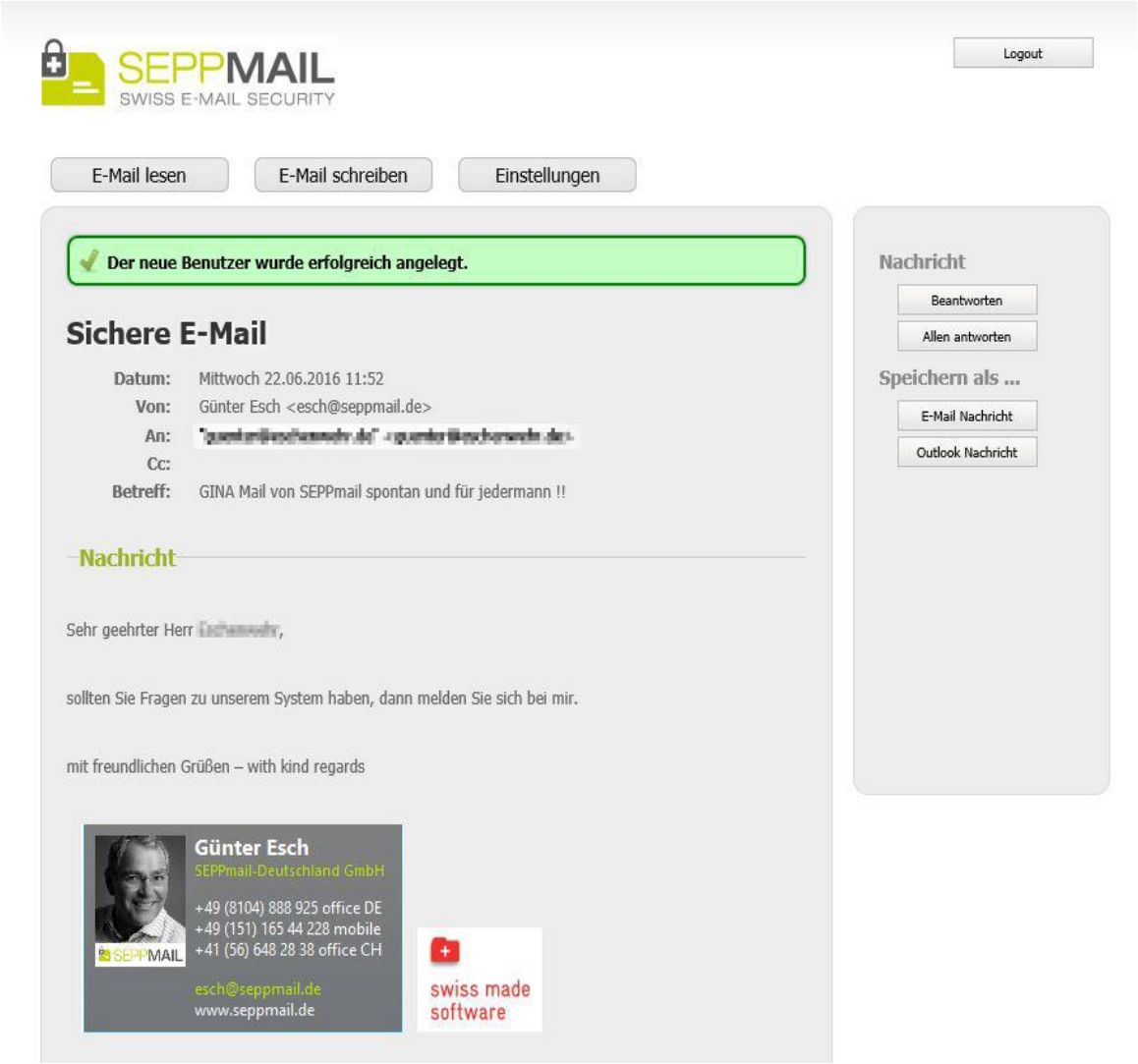
[2] Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH

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 GINAmails zum Verschlüsseln und Entschlüsseln für diese Empfangsadresse verwendet. Für jeden unbekannten externen Empfänger wird ein eigener symetrischer 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 symetrischen Schlüssel zur Entschlüsselung auf der Appliance zu erlangen. Anschließend erfolgt eine einmalige Registrierung im System. Ein eigenes Passwort wird vergeben. Beim nächsten Lesen der E-Mail oder bei einer neuen vertraulichen E-Mail, wird dann nur noch das eigene Passwort verwendet.

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.



b) GINA ist sicher

Darüber hinaus bietet die verschlüsselte E-Mail-Kommunikation via GINA viele Vorteile hinsichtlich dem Thema 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-Webmailer 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 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 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 ergebenen Kundennutzen im Wesentlichen in drei Headlines zusammengefasst werden:

a) Einfache Bedienbarkeit

Zum einen ist die GINAmail sehr einfach bedienbar. 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.

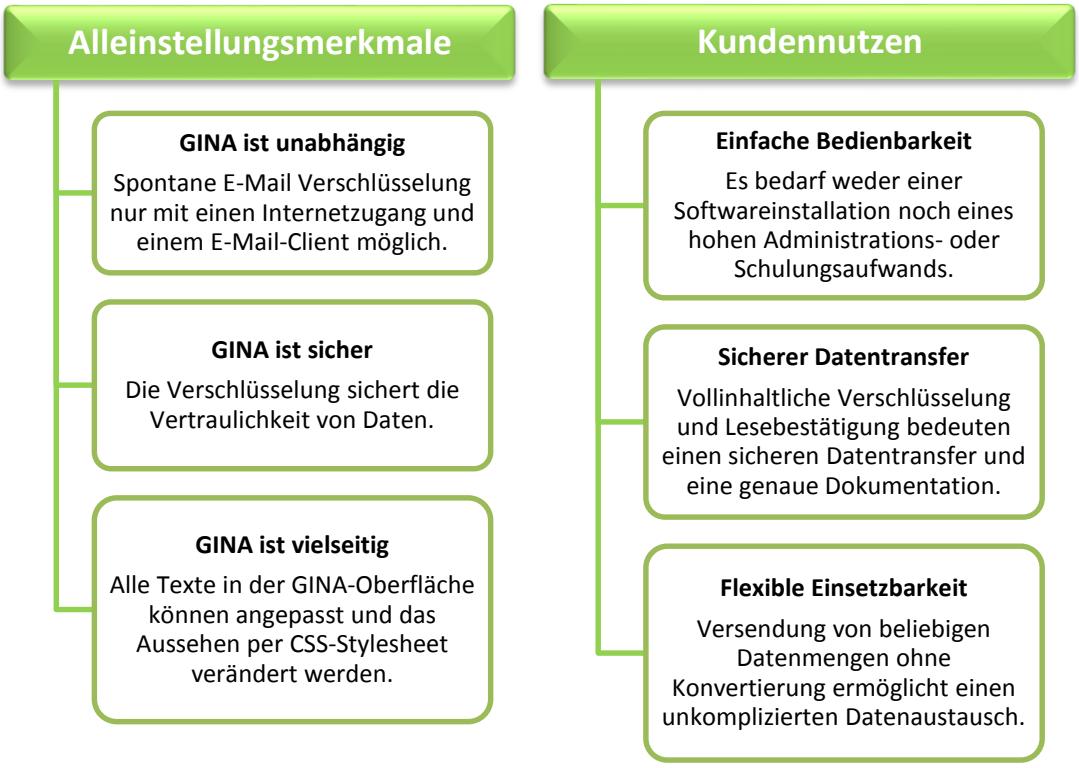
b) Sicherer Datentransfer

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

1. Datenschutzrechtliche Grundlagen

Unter Datenschutz versteht man den Schutz des Einzelnen vor unbefugter Verwendung und Weitergabe seiner personenbezogenen Daten.[3] Das bedeutet, dass z.B. bei Datentransfers via E-Mail ein sorgfältiger Umgang mit angemessenem Schutzniveau erfolgen muss. In Deutschland regelt das Bundesdatenschutzgesetz (BDSG) den Umgang mit personenbezogenen Daten durch öffentliche Stellen des Bundes sowie für alle nicht-öffentlichen, also den privatwirtschaftlichen Sektor, soweit diese personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder erheben oder die Daten in oder aus automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Bei den Landesdatenschutzgesetzen handelt es sich um die in den 16 Bundesländern verabschiedeten landesrechtlichen Pendants zum Bundesdatenschutzgesetz. Sie regeln den Umgang mit personenbezogenen Daten durch die Behörden und sonstige öffentliche Stellen des Landes. Daneben gibt es noch bereichsspezifische Vorschriften in anderen Gesetzen wie z.B. dem Telekommunikationsgesetz und dem Telemediengesetz.

Datenschutzrechtlich ist also zum einen immer zu prüfen, wer Daten erhebt oder verarbeitet und zum anderen immer festzulegen, ob es sich bei diesen erhobenen oder verarbeiteten Daten um sogenannte personenbezogene Daten handelt. Personenbezogene Daten sind laut Legaldefinition[4] Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Für die geschäftliche E-Mail-Kommunikation im privatwirtschaftlichen Sektor, z.B. mit Personaldaten, Lohndaten oder Daten der Finanzbuchhaltung, aber auch nur mit persönlichen Kontaktdaten gelten somit die Vorschriften des BDSG. Gemäß § 9 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im

[3] § 1 Abs. 1 BDSG, Simitis in Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 23 f.
[4] § 3 Abs. 1 BDSG, Dammann in Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 4ff.

Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.[5] Erforderlich sind Maßnahmen dabei nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Als Maßnahme wird in der Anlage u.a. die Verwendung von Verschlüsselungsverfahren nach dem Stand der Technik aufgeführt. 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 über einen angemessenen Aufwand hinaussgeht. 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.[6]

Neben der Frage, ob eine Verschlüsselungspflicht besteht, gilt der datenschutzrechtliche Grundsatz, dass durch die Maßnahme einer angemessenen Verschlüsselung ein drohender Datenschutzverstoß in jedem Fall verhindert werden kann. Wenn personenbezogene Daten angemessen verschlüsselt werden, fehlt es nach gängiger Rechtsprechung bereits an der Übermittlung personenbezogender Daten.[7]

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-Kriminalität, dem steigenden Wert der Daten im Zeitalter der Digitalisierung und den gemäß dem BDSG und der in zwei Jahren geltenden europäischen Datenschutzgrundverordnung (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-*

[5] Ernestus in Simitis, BDSG, 8. Aufl., § 9 Rn. 8
[6] Ernestus in Simitis, BDSG, 8. Aufl., § 9 Rn. 20f.
[7] Spies, MMR-Aktuell 2011, 313727, Kroschwald, ZD 2014, 75, 78, Körffer in Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 10a

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.

2. 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. 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: Februar 2016) sollten für neue Anwendungen nur noch Blockchiffren eingesetzt werden, deren Blockgröße

mindestens 128 Bit beträgt.[8] Die Blockchiffren AES-128, AES-192 und AES-256 werden zur Verwendung in neuen kryptographischen Systemen empfohlen.[9] 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.

IV. Beweisfunktionalitäten der GINA-Technologie

Wer Erklärungen im Geschäfts- und Rechtsverkehr gegenüber Dritten abgibt und sich auf einen bestimmten Erklärungsinhalt und Erklärungszeitpunkt beruft, hat früher oder später mit Fragen der Beweisbarkeit zu tun. Dem Grundsatz nach gilt gemäß dem deutschen Zivlilprozessrecht (ZPO) und dem Bürgerlichen Gesetzbuch (BGB) das Prinzip, dass die Partei die sich auf Erklärungen im Geschäfts- und Rechtsverkehr berufen möchte, diese auch nachweisen muss, sprich beweisbelastet ist. Der deutsche Gestzgeber kennt keine grundsätzlichen, rechtlichen Schranken für die Kommunikation und die Beweisführung an Hand elektronischer Dokumente. Die E-Mail ist als elektronische Post und Beweismittel im Geschäfts- und Rechtsverkehr anerkannt. Es ist aber festzuhalten, dass trotz der eindeutigen Entwicklung und Umstellung in der Geschäftspraxis auf merhheitlich elektronische Kommunikation und elektronisches Dokumentenmanagement, die korrespondierende Gesetzeslage und aktuelle Rechtsprechung insofern hinterherhinkt, als dass im Rahmen von elektronischer Kommunikation bisher nur unter erschwerten und eher unpraktikablen Bedingungen ein sogenannter Vollbeweis erbracht werden kann. 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

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1), Feb. 2016, S. 22
[9] Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1), Feb. 2016, S. 22

Zugangs und 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.[10] 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 der des Providers abrufbar gespeichert wird.[11] Hat der Empfänger nicht zu erkennen gegeben, dass ihm Erklärungen auf elektronischem Wege erreichen können (ausdrückliche Mitteilung der E-Mailadresse), 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.[12]

---

[10] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 75. Aufl. 2016, § 130 BGB Rn. 5
[11] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 75. Aufl. 2016, § 130 BGB Rn. 7a
[12] 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.[13] 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.[14] Erhält der Absender eine Lese- und Empfangsbestätigung, belegt diese rein materiell-rechtlich, ob eine E-Mail zugegangen ist und darüber hinaus den spätmöglichsten Zeitpunkt, also das „Wann“ des Zugangs, nämlich die tatsächliche Kenntnisnahme.[15] Diese Empfangsbestätigung kann damit prozessual einen Anscheinsbeweis für das „Ob“ und das „Wann“ des Zugangs der Erklärung sein.[16] 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. Sind sie bewiesen, so scheitert der Anscheinsbeweis erst, wenn der Gegner Tatsachen behauptet und beweisen kann, aus denen sich die ernsthafte Möglichkeit eines abweichenden (atypischen) Ablaufs ergibt.[17] Hat man also eine Lesebestätigung erhalten, liefert diese den Anscheinsbeweis, dass die E-Mail auch zugegangen ist und wann. Der

[13] LAG Berlin-Brandenburg, Beschluss vom 27.11.2012 – Az. 15 Ta 2066/12
[14] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 75. Aufl. 2016, § 130 BGB Rn. 21
[15] Spindler in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 130 BGB Rn. 25.
[16] Spindler in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 130 BGB Rn. 25.
[17] Foerste in Musielak/Voit, ZPO, 13. Aufl. 2016, § 286 Rn. 23; Spindler in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 130 BGB Rn. 25.

Anscheinsbeweis statuiert dabei eben nur einen typischen Geschensablauf. Mithin ist ein Restrisiko hinzunehmen, sofern ausnahmsweise eine atypische Situation vorliegt.

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. Das Signaturgesetz (SigG) sowie die ab Juli 2016 geltende neue EU-Verordnung „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" (eIDAS-VO) unterscheidet folgende Signaturarten:

- einfache elektronische Signatur
  (d.h. diese Signatur verknüpft elektronische Daten logisch miteinander, ohne dabei besondere Sicherheitsanforderungen zu erfüllen.)

- fortgeschrittene elektronische Signatur (AES, advanced electronic signature)
  (d.h. diese Signatur ist ausschließlich dem Signaturschlüsselinhaber zugeordnet, wodurch die Authentifizierung des Zertifikatsinhabers gewährleistet ist und die Integrität der Daten überprüft werden kann.)

- qualifizierte elektronische Signatur (QES)
  (d.h. diese Signatur funktioniert wie die fortgeschrittene, allerdings wird sie mit einer sicheren Signaturerstellungseinheit (SSEE) erzeugt. Zudem wird den elektronischen Daten zum Zeitpunkt ihrer Erzeugung ein qualifiziertes Zertifikat von einem Zertifizierungsdiensteanbieter (Trust Center) ausgestellt.)

In Deutschland kann die qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG gem. §§ 371a Abs. 1, 416 ZPO als „urkundsgleiches“ Beweismittel, d.h. als Vollbeweis im Prozess geführt werden. Darüber hinaus erlaubt das BGB in Fällen der gesetzlich vorgeschriebenen Schriftform den Ersatz durch die elektronische Form, soweit nichts anderes bestimmt ist, vgl. § 126 BGB. Die Form ist dann gewahrt, wenn dem elektronischen Dokument der Name des Unterzeichners hinzugefügt und dieses mit einer qualifizierten elektronischen Signatur versehen wird, vgl. § 126a BGB. Die für qualifizierte elektronische Signaturen zugelassenen Kryptoalgorithmen werden von der Bundesnetzagentur genehmigt und veröffentlicht. Dort sind auch die für eine

qualifizierte elektronische Signatur zugelassenen Produkte aufgelistet. Das in Deutschland bekannteste qualifiziert elektronische Zertifikat ist der sog. neue elektronische Personalausweis (nPA). Das Signaturzertifikat wird von einem Partner der Bundesdruckerei ausgegeben und ist nur in Kombination mit einem Kartenleser und einer Face-to-Face Kontrolle (z.B. sog. Postident) 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. Eine Auflistung der durch die Bundesnetzagentur akkreditierten Anbieter in Deutschland finden Sie auf der Website der Bundesnetzagentur.[18] Der hohe beschriebene Aufwand sorgt aber dafür, dass diese Form der elektronischen Signatur zwar maximal sicher, jedoch nur sehr gering verbreitet im Einsatz ist.

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-Mailprogramme 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.

[18] http://www.bundesnetzagentur.de/cln_1412/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/ZertifizierungsDiensteAnbietr_node.html

b) Signaturen bei GINA

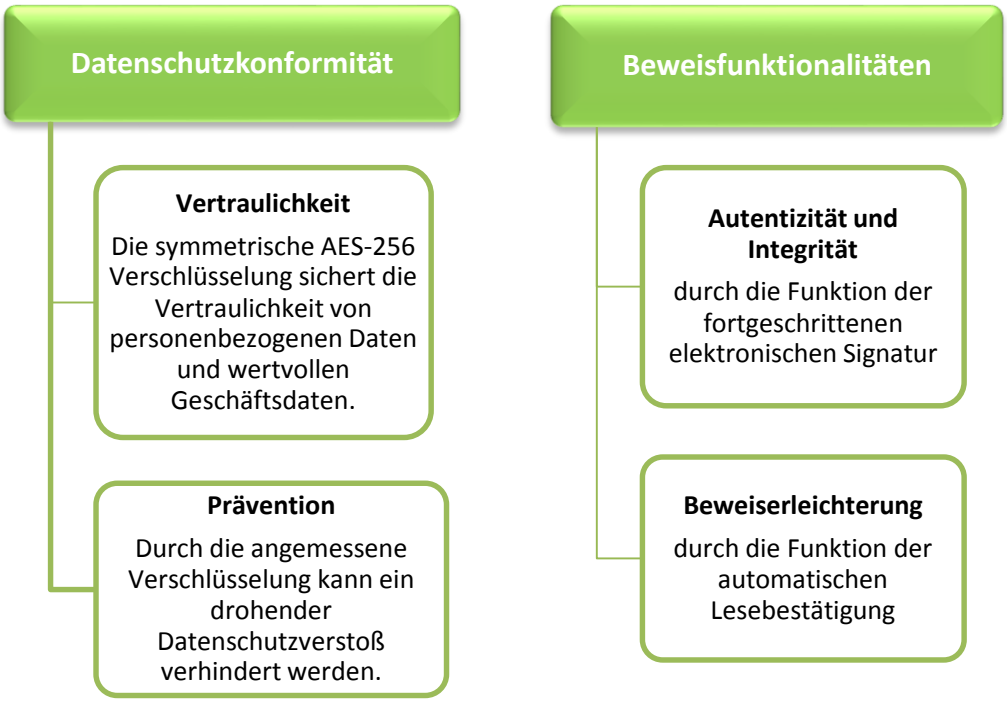
Darüber hinaus kann jede GINAmail mit einer fortgeschrittenen elektronischen Signatur versehen werden. Die Secure E-Mail-Gateways von SEPPmail ermöglichen die digitale Signatur von E-Mails unkompliziert und schnell. Der Nutzer benötigt ein sogenannte S/MIME-Zertifikat (Schlüssel), wobei bereits vorhandene 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 und SwissSign, anerkannte schweizerische Zertifizierungsstellen. Eine versendete GINAmail wird beim Versenden automatisch im Namen des Absenders signiert und kann sodann von keinem Außenstehenden mehr verändert werden. Außerdem können in allen Fällen, in denen kein Schriftformerfordernis besteht, Dokumente, die mit einer fortgeschrittenen elektronischen Signatur gemäß § 2 Nr. 2 SigG versehen wurden, als Augenscheinsbeweis vor Gericht verwendet werden.

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 unverhältnismäßig ist. Vor allem da für alle formfreien Vereinbarungen die Vertragspartner eine andere Signaturform als die qualifizierte, also entweder eine „einfache“ oder eine fortgeschrittene elektronische Signatur wählen können, § 127 BGB. Für die Fälle, in denen von vornherein feststeht, dass die gesetzliche Schriftform erforderlich ist oder rechtserhebliche Erklärungen beweissicher abgegeben werden

möchten, sollte 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 / Kontaktdaten

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 27 Jahren auf die Beratung im IT-Umfeld spezialisiert und hat zahlreiche Veröffentlichungen zum IT-Recht publiziert. Seit 1998 ist er Lehrbeauftragter an der Europäischen Privathochschule MUNICH BUSINESS SCHOOL für die Fächer IT Law and Management Liability.

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.

PRWRECHTSANWÄLTE

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