Edition 2019
inkl. DSGVO

# ALLABOUT COMPLIANCE

## Datenschutzkonformität und Beweisfunktionalitäten der GINA-Technologie von

SEPPMAIL

# Inhalt

# I. Hinweise

KOMDAT Datenschutz GmbH wurde von der SEPPmail Deutschland GmbH mit der Überarbeitung eines rechtlichen Whitepapers zur SEPPmail GINA-Technologie beauftragt. SEPPmail Deutschland GmbH stellt seinen 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 Begutachtung hinsichtlich der Rechtsthemen Datenschutzkonformität und Beweisfunktionalitäten darzustellen. Dabei wurden in der Edition 2018 bereits die neuen gesetzlichen Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) sowie zugehöriger nationaler Gesetze berücksichtigt.

Die Alleinstellungsmerkmale und der besondere 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 KOMDAT Datenschutz GmbH.

**Ronald Kopecky - Geschäftsführung**
*TÜV Austria zert. ISO/IEC27001, 27005, 27018 und ISO/IE31010 – zert. Auditor*
*Informations-Sicherheits-, Risiko- und Security-Manager, Datenschutzbeauftragter*
*TÜV Austria zert. Cloud-Security-Specialist*

Stand: März 2019

# 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 befasst sich seitdem mit dem 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]. 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 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 TU-Dresden, der Schweizerischen Post und dem Health Info Network (www.hin.ch). In diesem Netzwerk, das mit der Technologie von SEPPmail ausgestattet ist, tauschen täglich ca. 180.000 Nutzer sensible Patientendaten aus[2]. Im Folgenden sollen die Alleinstellungsmerkmale und die besonderen Kundennutzen der GINA-Technologie im Einzelnen vorgestellt werden. In Österreich ist das Produkt vor allem bei Behörden, öffentlichen Organisationen und führenden Industriebetrieben im Einsatz.

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

# 1. Alleinstellungsmerkmale

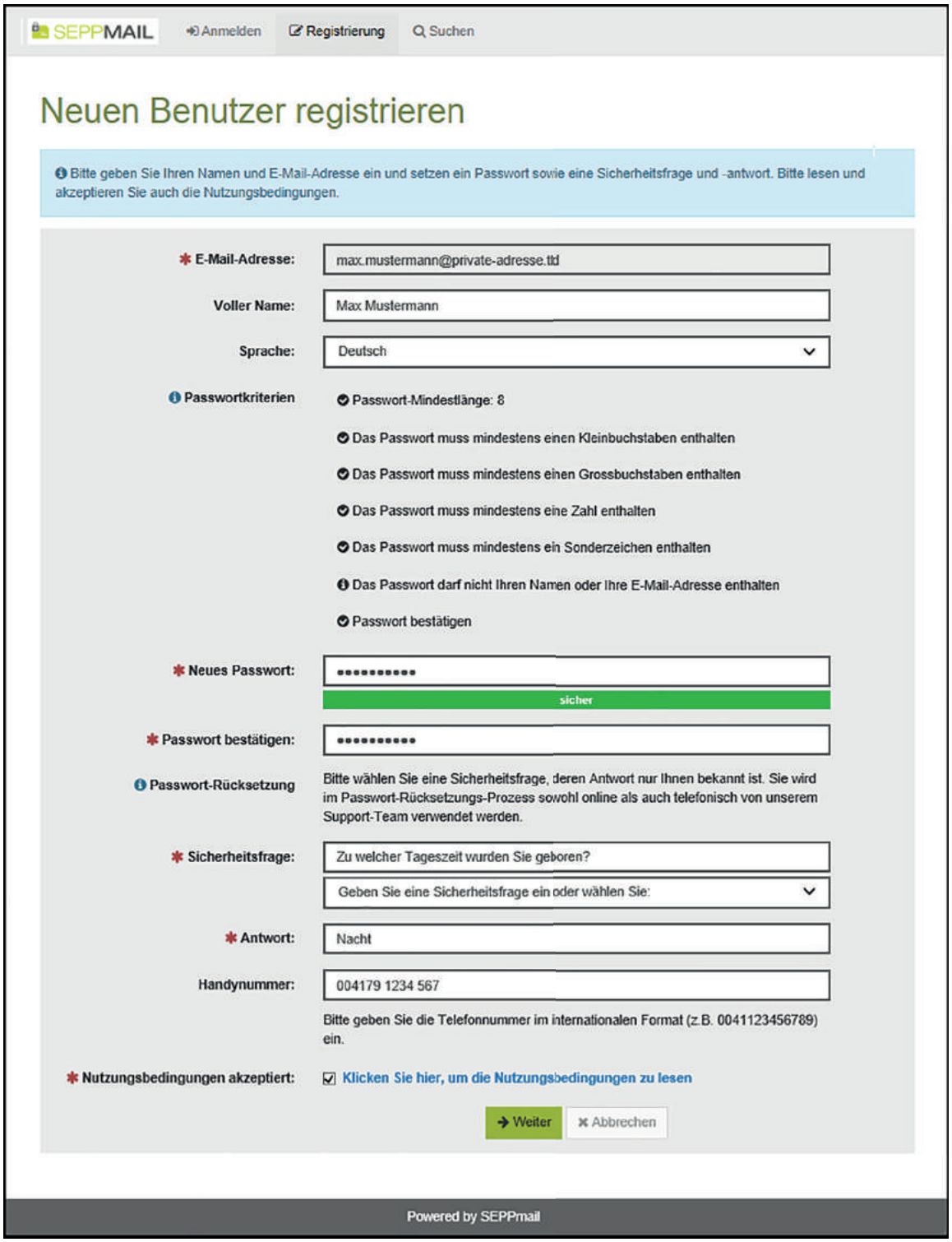
## a) GINA ist plattformunabhängig

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.

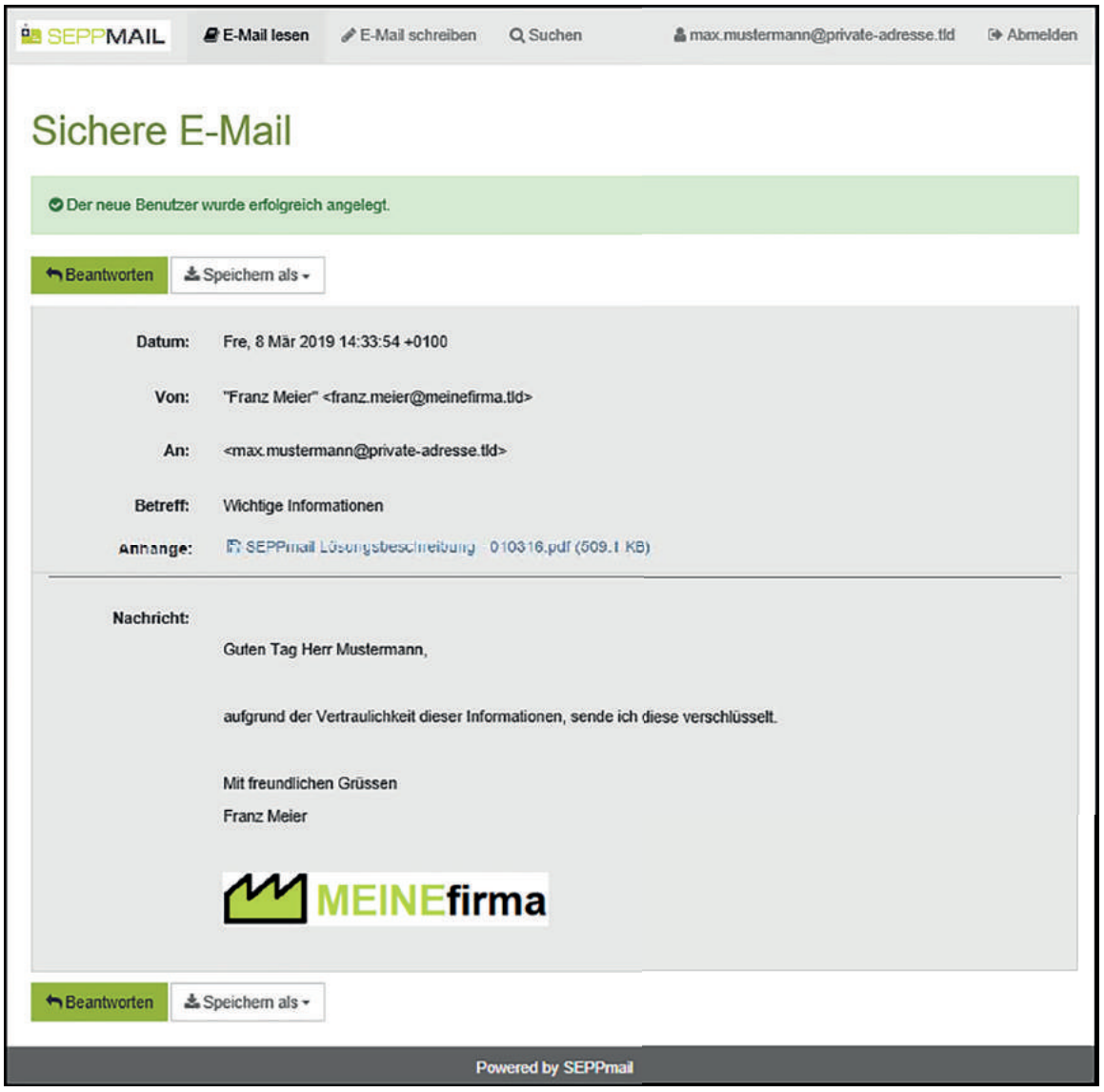
**Was passiert aber, wenn der Empfänger nicht über die Einrichtung zur Entschlüsselung verfügt?**
Genau für diese Fallkonstellation hat SEPPmail die GINA-Technologie entwickelt. Mittels GINA lassen sich verschlüsselte E-Mails auch zu Empfängern übertragen, die selbst über keine entsprechende Vorkehrung 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.

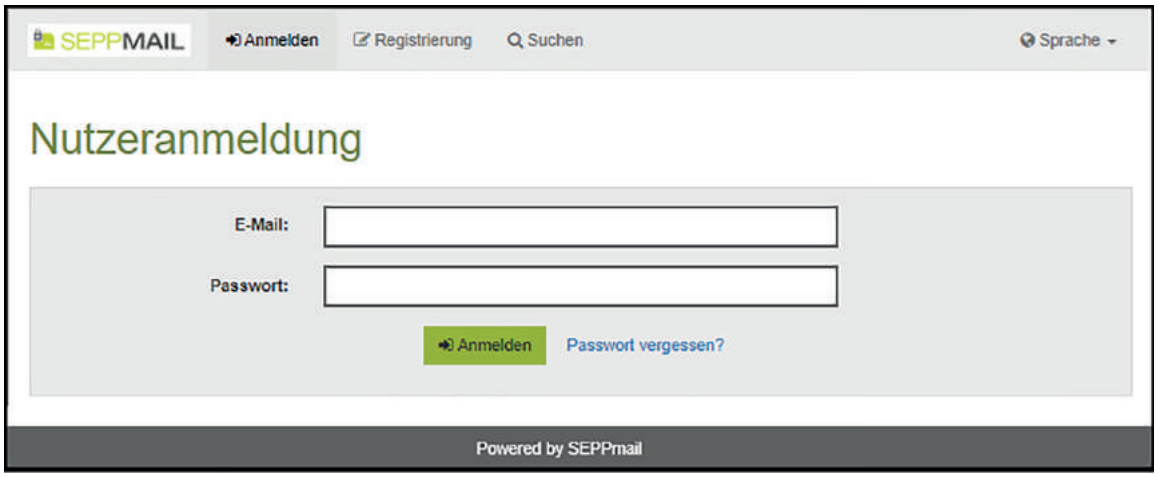
**Wenn für den Empfänger keine Schlüssel hinterlegt sind, oder dieser gänzlich „unbekannt" ist, greift automatisch die GINA-Technologie ein.**
Es wird ein AES-256 Key erzeugt, die vertrauliche E-Mail damit symmetrisch verschlüsselt und als HTML-Anhang an eine Standard-E-Mail beigefügt. Diese wird an 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 (gemeinsames Geheimnis) bleibt dauerhaft auf der Appliance und wird für die erste, wie für alle anderen GINA-Mails zum Verschlüsseln und Entschlüsseln für diese Empfangsadresse verwendet. Die komplette ursprüngliche E-Mail - inklusive Anhang – wird RFC-konform verschlüsselt und als HTML-Text-Anhang an eine neue Standardträgermail angefügt. Der Empfänger öffnet den HTML-Text-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-Text-Anhang 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 individuelles Passwort ist zu hinterlegen.




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.




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



## 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 geheimen Schlüssel (Geheimnis) abhängige Umwandlung von „Klartext" in einen „Geheimtext". Aus dem Geheimtext kann nur unter Verwendung des geheimen Schlüssels (Geheimnis) 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 Empfänger der verschlüsselten Nachricht, außer einem Client zum Empfangen von E-Mails nur einen Internetzugang und einen Browser. Beim Öffnen des HTML-Text-Anhangs und während der Eingabe des Zugangspasswortes, wird im Hintergrund über eine https-verschlüsselte Internetverbindung 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, dass 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 Technologien 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

Die dargestellten Alleinstellungsmerkmale können im Wesentlichen in drei Kundennutzen 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**

**Alleinstellungsmerkmale**

**GINA ist unabhängig**
Spontane E-Mail-Verschlüsselung nur mit einem Internetzugang und einem E-Mail-Client möglich.

**GINA ist sicher**
Die Verschlüsselung sichert die Vertraulichkeit von Daten.

**GINA ist vielseitig**
Alle Texte in der GINA-Oberfläche können angepasst und das Aussehen per CSS-Stylesheet verändert werden.

**Kundennutzen**

**Einfache Bedienbarkeit**
Es bedarf weder einer Softwareinstallation noch eines hohen Administrations- oder Schulungsaufwands.

**Sicherer Datentransfer**
Vollinhaltliche Verschlüsselung und Lesebestätigung bedeuten einen sicheren Datentransfer und eine genaue Dokumentation.

**Flexible Einsetzbarkeit**
Versendung von beliebigen Datenmengen ohne Konvertierung ermöglicht einen unkomplizierten Datenaustausch.

# 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 natürlicher Personen vor Beeinträchtigungen seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen. Die geltenden österreichischen Vorschriften zum Datenschutz sind im Datenschutzgesetz (DSG 2018) sowie in Spezialgesetzgebungen geregelt. Der Datenschutz in Österreich ist für jede natürliche oder juristische Person (privatwirtschaftliches Unternehmen), Behörde, Einrichtung oder andere Stelle verpflichtend vorgeschrieben, welche alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eingeführt wurde dazu der Begriff „Verantwortlicher".

**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 lief eine zweijährige Umsetzungsfrist. Seitdem gilt die Verordnung unmittelbar und zwingend in allen EU-Mitgliedstaaten. Bis dahin mussten die bereits in Kraft getretenen neuen gesetzlichen Anforderungen der europäischen Verordnung in die Praxis umgesetzt worden sein[5]. Darüber hinaus enthält die DSGVO einige sogenannte Öffnungsklauseln. Diese erlauben es den nationalen Gesetzgebern ergänzend zur unmittelbar geltenden DSGVO flankierende Regelungen als nationale Sondervorschriften zu treffen. Das Österreichische Datenschutzgesetz (DSG oder Datenschutz-Anpassungsgesetz 2018) wurde angepasst.

Aufgrund einer fehlenden 2/3-Mehrheit blieben die bisherigen Verfassungsbestimmungen des DSG 2000 weiterhin in Kraft. Dies hat in Österreich zur Folge, dass die im Verfassungsrang stehende Bezeichnung „Jedermann" weiterhin Rechtsgültigkeit hat und als Konsequenz der Datenschutz in Österreich auch juristische Personen schützt. Durch die DSGVO kommen neue bzw. erhöhte datenschutzrechtliche Pflichten auf Verantwortliche zu. Die zentrale Hauptforderung liegt in der durchgängigen Rechenschafts- und Nachweispflicht sowie in der Pflicht, die technischen und organisatorischen Maßnahmen an Risiken auszurichten – Dokumentation und Nachweis inbegriffen. Dies erfordert die Einführung eines Datenschutz-Management-Systems, um alle technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen über die Zeit hinweg kontrollierbar zu machen.

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 Datenschutzverstoßes sind empfindlich erhöht worden.

4 https://dejure.org/gesetze/DSGVO
5 Art. 99 Abs. 2 DSGVO
6 Website des Bayerischen Landesamtes für Datenschutzaufsicht, https://www.lda.bayern.de/media/baylda_DSGVO_7_sanctions.pdf

Es drohen den Unternehmen seit Mai 2018 bei Datenschutzverstößen Geldbußen von 10 bis 20 Millionen Euro oder von 2 bis 4 Prozent des unternehmerischen Jahresumsatzes. Maßgeblich ist dabei der Jahresumsatz der gesamten Unternehmensgruppe, nicht der einzelnen verantwortlichen Gesellschaft.

**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 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 Z 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 Z 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 des Weiteren 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 E-Mail-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 E-Mail-Kommunikation 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. Es ist demzufolge ein risikobasierter Ansatz bei der Wahl der technischen und organisatorischen Maßnahmen anzuwenden. 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) (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.*

Da E-Mail-Verschlüsselung nach Ansicht der Datenschutzaufsichtsbehörde inzwischen Stand der Technik ist, ist davon auszugehen, dass E-Mail-Verschlüsselung in den Rang einer Pflicht kommt. Aktuell wird diese Auslegung noch von den Experten diskutiert. Die Formulierung des Art. 32 DSGVO lässt Spielraum für Interpretation und einzelfallbezogene Abwägungen. Welche konkrete Sicherheitsmaßnahme im Einzelfall als angemessen einzustufen ist, ist im Rahmen einer Abwägung unter Berücksichtigung der Risiken zu ermitteln. Bei Nichtbeachtung der datenschutzrechtlichen Vorgaben 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 eindeutigere 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.“ [7]

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.[8][9] 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-Kriminalität11, 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.

7 Zitat Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH, vgl. https://www.seppmail.de/eu-dsgvo-e-mail-verschluesselung-ist-pflicht/
8 Spies, MMR-Aktuell 2011, 313727, Kroschwald, ZD 2014, 75, 78; Körffer in Gola/Schomerus, BDSG, 12. Auflage 2015, § 3 Rn. 10a
9 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, bei dem 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), Vertauschungen (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.[10] Die Blockchiffren AES-128, AES-192 und AES-256 werden zur Verwendung in neuen kryptographischen Systemen empfohlen.[11] 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.

10 Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", (BSI TR02102-1), Januar 2018, S. 16
11 Bundesamt für Sicherheit in der Informationstechnik (BSI) Technische Richtlinie, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", (BSI TR02102-1), Januar 2018, S. 16

# 4. 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. 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.

# IV. Fazit

Die Technologie von GINA bietet den Unternehmen 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 GINA-Technologie**

**Datenschutzkonformität**

**Vertraulichkeit**
Die symmetrische AES-256 Verschlüsselung sichert die Vertraulichkeit von personenbezogenen Daten und wertvollen Geschäftsdaten.

**Prävention**
Durch die angemessene Verschlüsselung kann ein drohender Datenschutzverstoß verhindert werden.

**Beweisfunktionalitäten**

**Authentizität und Integrität**
durch die Funktion der fortgeschrittenen elektronischen Signatur.

**Beweiserleichterung**
durch die Funktion der automatischen Lesebestätigung.

**KOMDAT Datenschutz GmbH**
Linzer Strasse 74
4614 Marchtrenk
Austria

E-Mail: office@komdat.at
Telefon: +43 / (0)7243 / 54300
Fax: +43 / (0)7243 / 54300-9
Web: www.komdat.at