



## RMAIL PRODUKTSTECKBRIEF

# E-MAIL VERSCHLÜSSELUNG

## Einhaltung von TOMs und BSI Richtlinien

Verschlüsselte E-Mails direkt ins Postfach des Empfängers: Wenn Sie gesetzlich oder durch interne Regeln dazu verpflichtet sind, vertrauliche Informationen und personenbezogene Daten zu verschlüsseln, ist es wichtig, jederzeit nachweisen zu können, dass Sie die Regeln eingehalten haben. Das Verschlüsseln sensibler E-Mails und Anhänge mit RMail® bietet hohe Sicherheit und Einhaltung von Gesetzen und Vorschriften (DSGVO).

Mehr und mehr Unternehmen nutzen daher RMail für die Verschlüsselung und für den Nachweis der Compliance. RMail ist einfach zu nutzen und erreicht höchste Akzeptanznoten beim Empfänger. Der Service bietet eine einmalige Kombination von:

- **Compliance:** einzigartiger Zustellungsnachweis (Nachweis zur Einhaltung der DSGVO). Enthält alle Fakten zur E-Mail-Kommunikation einschließlich Absender- und Empfängerinformationen, Zeitstempel, Verschlüsselungsstufen, Nachrichteninhalte mit Anhängen sowie Track & Trace-Informationen. Dient als Beleg für die Einhaltung der Vertraulichkeit und gilt im Schadensfall als gerichtsfester Beweis.
- **Empfängerakzeptanz:** National und international nutzbar. Erfordert keinerlei Vorkehrungen auf Empfängerseite - keine zusätzliche Softwareinstallation, Kontoeröffnung oder Registrierung über zusätzliche Website. Zu Öffnen mit jedem E-Mail-Programm und jedem E-Mail-Client!
- **Empfängersicherheit:** Empfänger kann via SecureReply jederzeit durch vorkonfiguriertem Webmailer verschlüsselt antworten (inkl. mit allen Nachweisen, ohne Kontoeröffnung etc.)
- **Bedienung:** Plugin für bestehendes E-Mail-Programm (oder automatisiert für erweiterte Business-Applikationen z. B. für ERP und CRM-Systeme). Verschlüsselung vom Absender direkt zum Posteingang des Empfängers.
- **Automatisierung-Funktionen:** Systeme können einfach auf definierte Betreff-Codes und Adress-Erweiterungen zugreifen um alle Services zu nutzen (ERP Lösung).
- **Einrichtung:** Kinderleichte Integration: Kein Programmieren, kein extra IT-Support für die Einrichtung und Automatisierung nötig. Eigene Verwaltung von Unternehmens- und Benutzereinstellung möglich.
- **Direktzustellung:** Ende-zu-Ende Verschlüsselung über RMail Server (hosted in Frankfurt)
  - keine Speicherung von Kopien der Nachricht oder Anhängen, DSGVO-konform.



RMail lässt sich kinderleicht dank API in Ihre Geschäftsprozesse integrieren und beinhalten rechtssichere Nachweise auf die wichtigen internationalen Datenschutzverordnungen wie DSGVO oder eIDAS.

# Ihre Vorteile auf einen Blick

Verschlüsselung ist der bewährte Weg, E-Mails vertraulich zu behandeln. Doch wie nützlich ist ein E-Mail-Verschlüsselungsservice, wenn es umständlich und unkomfortabel ist, die verschlüsselte Nachricht zu versenden? Oder wenn Ihre Empfänger ständig Hilfe benötigen, Ihre E-Mails zu öffnen? Frama macht für Sie und Ihre Empfänger die sichere E-Mail-Kommunikation einfach, sicher und komfortabel.

## Verwendung der eigenen E-Mail-Adresse

### Nutzen Sie RMail direkt aus Ihrem bestehenden E-Mail-Programm.

- Microsoft Outlook 2007, 2010, 2013, 2016, 2019, Office 365 (auch MAC)
- Microsoft Exchange
- Google Mail
- Weboberfläche mit Mail-APP für Mobile Devices (z.B. für Android & IOS Plattformen)
- ERP Anbindung in sämtliche Umgebungen



**Einfach zu bedienen:** Der Empfänger benötigt zum Empfangen oder Lesen Ihrer E-Mail weder spezielle Software noch müssen Websites besucht oder Webservices mit Accountregistrierung benutzt werden.

### Starten Sie sofort!

RMail ist einfach einzurichten, intuitiv zu bedienen und für den Empfänger extrem benutzerfreundlich.



Mit Track & Trace Funktion (Sendungsverfolgung)

## Das sagen unsere Kunden

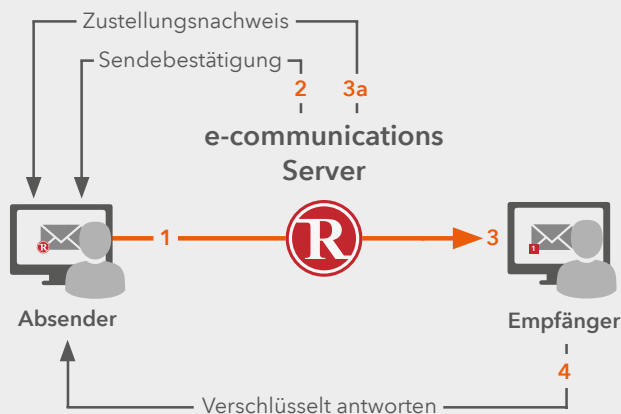
„Frama RMail ist leicht zu integrieren, bietet State-of-the-Art Technologie und erfüllt die Anforderungen der DSGVO für die Übertragung personenbezogener Daten. Die Empfängerakzeptanz und die Unkompliziertheit bei der Kommunikation mit Dritten hat uns überzeugt, sodass wir Frama RMail im Unternehmen breitflächig einsetzen.“

- Kemal Webersohn, CEO WS-Datenschutz GmbH -

# Schaffen Sie Vertrauen

**Datenintegrität ist für alle wichtig!** In Artikel 32 der DSGVO wird die Verschlüsselung explizit als Schutzmaßnahme bei der digitalen Kommunikation erwähnt. Zeigen Sie Ihren Mitarbeitern, Kunden und Geschäftspartnern, dass Ihr Unternehmen verantwortlich und datenschutzkonform mit vertraulichen Daten umgeht.

## Wie funktioniert es?



- 1 Der Absender versendet die Nachricht mit RMail
- 2 Die Sendebestätigung wird versendet
- 3 Die E-Mail wird in das Empfänger-Postfach zugestellt
- 3a Der Zustellungsnachweis wird versendet, nachdem der e-communications Server alle Server-Logs, Originalinhalte, sowie Zeit- und Datumstempel gesammelt hat
- 4 Der Empfänger kann auf verschlüsselte E-Mails verschlüsselt antworten, ohne sich zu registrieren oder etwas herunterzuladen

# Wann muss eine E-Mail verschlüsselt werden?



**Laut DSGVO müssen E-Mails dann verschlüsselt werden, wenn personenbezogene Daten versendet werden. Personenbezogene Daten sind z. B.:**

- Sexuelle Orientierung
- Ethnische Herkunft
- Politische Meinung
- Biometrische Daten
- Religiöse Überzeugung
- Informationen über den Gesundheitszustand

**Die Verschlüsselung von E-Mails sollte z. B. beim Versand folgender Unterlagen erfolgen:**

- Arbeitsverträgen
- Lohnbescheiden
- Krankmeldungen
- Ausweiskopien
- Vollmachen
- Bewerbungsunterlagen usw.

# Die wichtigsten Fragen zur Verschlüsselung

## **Frage: Müssen E-Mails laut DSGVO verschlüsselt werden?**

### **Die DSGVO fordert explizit eine Verschlüsselung!**

In Art. 5 Abs. 1 lit. f DSGVO wird festgelegt, dass personenbezogene Daten „(§1f) ... in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“); Das heißt konkret: E-Mails mit personenbezogenen Daten müssen in geeigneter Weise geschützt übertragen werden!

Darüber hinaus regelt Art. 32 Abs. 1 Satz 1 DSGVO, dass „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ sind. Art. 32 Abs. 1 lit. a DSGVO erwähnt dann sogar explizit die Verschlüsselung von Daten. Verschlüsseln Sie eine E-Mail mit personenbezogenen Daten nicht, gehen Sie das Risiko ein, dass andere Personen die E-Mail unbefugt mitlesen. Dies kann hohe Geldstrafen nach sich ziehen. Eine nicht verschlüsselte E-Mail ist vergleichbar mit einer handgeschriebenen Postkarte. Dies kann theoretisch von jedem, der sie in den Händen hält, gelesen werden.

## **Frage: Muss ich als Versender nachweisen, wer, wann was, wie an wen versendet hat?**

### **Ja, der Versender hat die Pflicht dies zu jeder Zeit nachzuweisen.**

Risikovermeidung: Der Versender muss die vollständige E-Mail-Versandkette dokumentieren können laut DSGVO (Compliance).

(Versandkette: Anwender - E-Mailserver Anwender - Internet - E-Mailserver Empfänger - Empfänger) Im Gegensatz zum BDSG fordert die DSGVO „to demonstrate“, also eine aktive Rechenschaftspflicht! Art. 5 Abs. 1 Satz 1 DSGVO

## **Frage: Welche Probleme treten bei der E-Mail-Verschlüsselung in der Praxis auf?**

Sie richten eine E-Mail-Verschlüsselung ein und diese funktioniert tadellos? Achten Sie darauf, dass Sie eine ganzheitliche Lösung schaffen. Komplizierte Lösungen taugen nicht viel; Ihre Mitarbeiter vernachlässigen die Umsetzung gerne. Problematisch wird es, wenn Sie ein System nutzen, das nicht sonderlich kompatibel ist. Viele Lösungen scheitern schlicht am Empfänger (Kunde, Lieferant, Partner)!

**Tipp:** Wählen Sie eine Verschlüsselungsmethode, die gängige Plattformen, Server und E-Mail-Clients unterstützt.

Fazit: Das Benutzererlebnis auf Empfängerseite entscheidet über die flächendeckende Akzeptanz der Lösung. Nur somit können Sie auch einen zuverlässigen Datenschutz in Ihrem Unternehmen gewährleisten.

## **Frage: Ist eine Verschlüsselung bei einer Datenpanne vorteilhaft?**

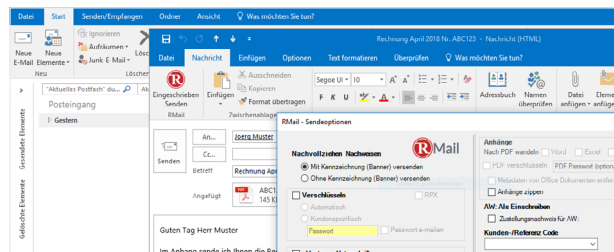
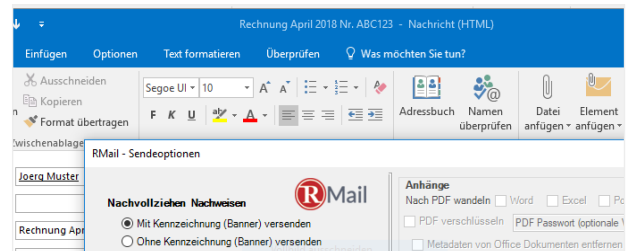
**Ja, in der Tat.** Nach einer Datenpanne müssen Sie die Datenschutzaufsichtsbehörde Ihres Landes und die betroffenen Personen nach spätestens 72 Stunden über den Vorfall informieren.

In diesem Fall findet die Meldepflicht der DSGVO: Art. 33 Abs. 1 DSGVO Anwendung.

# RMail Standardfunktionen im Überblick

## Verschiedene Verschlüsselungs-Ebenen

Ihre Nachricht und alle Anhänge werden mit einem 56-Bit-AES PDF-Wrapper verschlüsselt und direkt in den Posteingang des Empfängers (Ende-zu-Ende Verschlüsselung) geliefert. Somit müssen diese weder von einem externen Sever noch über eine Website abgerufen werden!

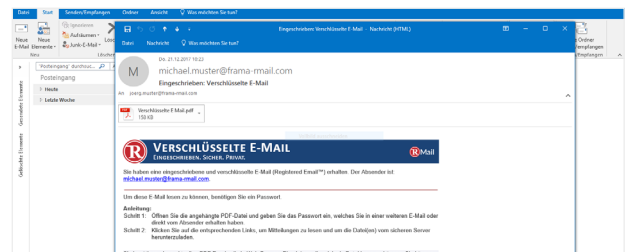


## Mehrere Passwort-Möglichkeiten

Wählen Sie zum Beispiel Ihr eigenes oder ein vom System generiertes Passwort, das automatisch an den Empfänger gesendet wird. Weitere Möglichkeiten der Übermittlung des Passwortes können unter anderem auch individuell festgelegt werden.

## Automatische Verschlüsselung TLS

RMail kann - nach entsprechender Konfiguration - automatisch mit TLS 1.2 Verschlüsselung versenden, wenn TLS von den Servern des Senders und des Empfängers unterstützt wird.



**ZUSTELLUNGSNACHWEIS**  
EINGESCHRIEBENER NACHWEIS ÜBER ZUSTELLUNG, INHALT & ZEIT

Dieser Zustellungsnachweis ist ein verifizierbarer Nachweis Ihrer eingeschriebenen E-Mail. Der Zustellungsnachweis ermöglicht dem Besitzer, die gesamte Transaktion inklusive Zustellung, Öffnung, Inhalt und Zeitstempel nachzuvollziehen. Je nach Service enthält der Zustellungsnachweis auch die Angaben bezüglich Verschlüsselung und/oder elektronischer Unterschrift.

Um diesen Zustellungsnachweis zu verifizieren, leiten Sie ihn weiter an [verify@r1.post.net](mailto:verify@r1.post.net)

| Status der Zustellung       |                         |         |                              |                              |                  |
|-----------------------------|-------------------------|---------|------------------------------|------------------------------|------------------|
| Adresse                     | Status                  | Details | Zugestellt (UTC*)            | Zugestellt (lokal)           | Geöffnet (lokal) |
| joerg.muster@frama-mail.com | Gesendet an Mail Server |         | 14/12/2017 12:38:17 PM (UTC) | 14/12/2017 01:38:17 PM (1.0) |                  |

\*UTC steht für Coordinated Universal Time.

Messano Erueflonn

## Zustellungsnachweis (Registered Receipt)

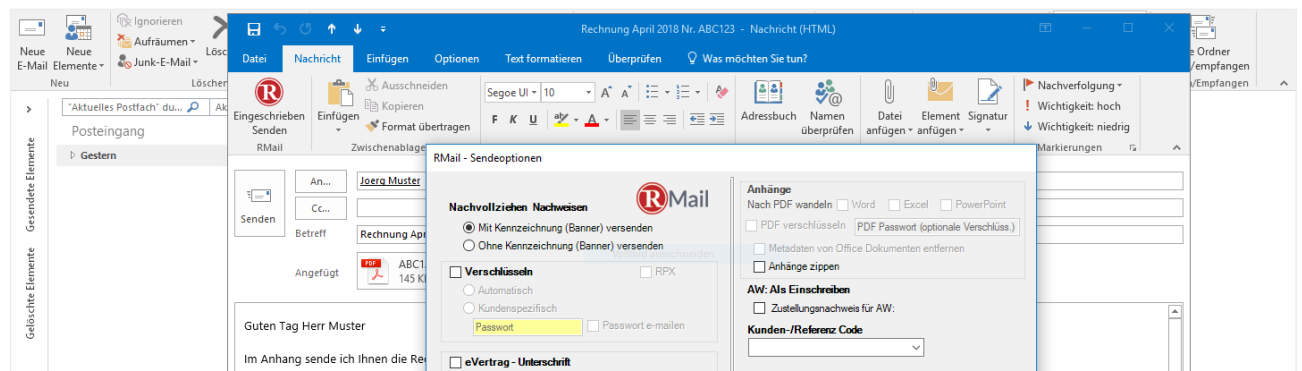
Nur mit dem RMail Zustellungsnachweis erhalten Sie für jede E-Mail, die Sie versenden, einen Bericht über den Zustellungsstatus, den Zeitpunkt der Zustellung und über den Originalinhalt. Dieser Bericht hat vor Gericht eine hohe Beweiskraft.

# Das sagen unsere Kunden

„Mit RMail sehen wir uns auf der sicheren Seiten und haben auch im Hinblick auf den Datenschutz unsere vertrauliche digitale Kommunikation DSGVO-konform aufgestellt.“

- Sarah Bartel, Ressortleitung Media FACTS Verlag -

# RMail Sendeoptionen



- **Nachvollziehen und Nachweisen:** Zustellnachweis/ Sendebestätigung für Verarbeitung der E-Mails anfordern, Nachweise in separatem Outlook-Ordner speichern.
- **E-Mails mit Banner kennzeichnen:** Banner kennzeichnet die Mails als sicher verschickte und verschlüsselte E-Mail, erweckt Vertrauen beim Kunden. Verschlüsselung: Übertragungsweg TLS min. Version 1.2/Secure PDF. Die gängigsten Varianten sind TLS - Transportwegverschlüsselungen.
- **E-Sign:** Unterschreiben via Maus, E-Mail, Platzhalter, sequenzielles unterschreiben in Reihenfolge der „AN:“ Empfänger.
- **LargeMail:** Mails mit bis zu 1GB großen Dateianhängen verschicken und automatisch erstellen lassen, wenn Dateien größer als „x“ MB.
- **SideNotes:** Privatnotiz für Cc und Bcc Empfänger einfügen. (Post-It sieht der Hauptempfänger nicht)
- **Anti-Whaling:** Warnungen bei eingehenden E-Mails anzeigen, wenn der Absender ein anderer ist als er vorgibt zu sein, Icon im Sende-Dialog anzeigen, Sicherer Absende-Button im RMail Dialog anzeigen. Zusätzlicher Schutz zu ihrem Antiviren Programm.
- **Digital Seal:** E-Mail-Empfänger kann Absender, Zeiten und Inhalt authentifizieren lassen .
- **Eingeschriebene Antworten:** Erlauben Sie ihrem Empfänger auf gleichem Weg zu antworten.
- **Kunden-/Referenz Code:** Fügen Sie Referenzen in E-Mails ein und diese werden in Belegen und Reports gespeichert.
- **Anhänge:** Automatische PDF-Konvertierung von Anhängen, Metadatenlöschung und komprimieren von ZIP-Dateien.
- **Unterschriftenfeld:** Eingeschriebene E-Mails mit Unterschriften werden extra gekennzeichnet, eigene Signatur als Standard abspeichern und voraussetzen!
- **RMail Recommends:** Wählen von bestimmten Trigger-Wörter oder Empfänger und automatisches versenden einer verschlüsselte E-Mail. Unter RMail-Tipps können Sie zusätzlich auswählen, welche der Standardfunktionen (E-Sign+ SideNote) Sie erlauben.
- **Sprachen:** Wählen Sie zwischen Deutsch, Englisch, Französisch, Italienisch, Spanisch, Niederländisch, Polnisch und Portugiesisch.
- **Erweiterte Einstellung:** Vereinfachen Sie den Usern die Auswahl der Funktionen und legen Sie standardmäßig fest, welche Funktionen erlaubt bzw. automatisch genutzt werden. Das PlugIn Fenster wird nicht mehr angezeigt und erleichtert den Versand durch direktes Klicken auf den Sendebutton.

**RMail-Konto und Support:** Einmaliges Login wird beim Start nach Installation des PlugIn erforderlich. Sollten Sie ihr Passwort vergessen, können Sie es hier in den Einstellungen zurücksetzen und sich neu verifizieren lassen. Bei allen Problemen können Sie uns einfach eine Support-Anfrage schicken. Das System übermittelt uns dabei alle Logfiles und wir erhalten Informationen zur Version und eventuelle Fehlermeldungen. Gerne helfen wir hier auch telefonisch weiter.

# Spezifikationen

## Serverstandort

- Frankfurt am Main

## Maximale Anzahl Empfänger pro Versand

- 100 pro Versand (Massenversand verfügbar)

## RMail „Unit“

- Versendete E-Mail: Ein Empfänger pro Nachricht und pro 5 MB
- Antwort E-Mail: Ein Empfänger pro Nachricht (E-Sign Antwort, Eingeschriebene Antwort und verschlüsselte Antwort) pro 5 MB

## Maximale E-Mail und Anhanggröße

- Eingeschrieben: 25 MB
- Verschlüsselt: 25 MB
- E-Sign: 10 MB (5 MB für .csv und .xls Dateien)
- LargeMail: 1 GB (ein Empfänger pro Nachricht)

## Standard-Dateiaufbewahrungszeiten

- Händische Unterschrift: Bis zu 30 Tage nachdem der e-communications Server die Nachricht verarbeitet hat oder nachdem der Unterschriftenprozess abgeschlossen wurde
- LargeMail File Transfer: Standardmässig 14 Tage (Einstellungsmöglichkeit 1-90 Tage)
- E-Mail Archiv: Auf Anfrage. Für Nachrichten, Dokumente oder Zustellungsnachweise gibt es kein Archiv, außer wenn ein solcher Service zusätzlich bestellt wird

## Zustellzeiten Zustellungsnachweis

- Zustellungsnachweis: Wird spätestens zwei Stunden nach dem Erhalt und der Bearbeitung durch den e-communications Server generiert und dem Absender oder einer vordefinierten Adresse zugestellt
- Öffnungsnachweis: Nach Generierung des Zustellungsnachweis weiteres Tracking für maximal 30 Tage
- Eingeschriebene Antwort: Die Antwort kann nur für maximal 30 Tage nach Verarbeitung durch den e-communications Server als Eingeschrieben versendet werden

## Dateigröße Zustellungsnachweis

- Standard Versand: Der Zustellungsnachweis wird als Standard E-Mail versendet, wenn die Größe unter 10 MB liegt
- LargeMail Versand: Beträgt die Größe mehr als 10 MB, wird der Zustellungsnachweis per LargeMail versendet

## Verifizieren des Zustellungsnachweises

- Benutzer können den Zustellungsnachweis (oder DigitalSeal®) bis zu 5 mal verifizieren
- Frama behält sich das Recht vor, für zusätzliche Verifikationen Gebühren zu erheben, wenn die verifizierende Person kein RMail Abonnent (kostenpflichtiger Account) ist
- Die Zustellungsnachweise können vom Zeitpunkt der Bearbeitung durch den Server 10 Jahre lang authentifiziert werden, wenn nichts anderes mit Frama vereinbart

## Verschlüsselungs-Service

- Auto-TLS mit Secure PDF Fallback
- Verschlüsselung basiert auf einem Secure PDF Wrapper, welcher 256-Bit salted verschlüsselt wurde  
Mehrere Passwort-Optionen verfügbar
  - Passwort E-Mail
  - Kundenspezifisches Passwort
  - Passwort Abfrage
- Filter Modus auf Anfrage verfügbar

## Unterstützte Dateitypen für händische Unterschrift

- Microsoft Office: .doc, docx, xls, xlsx, ppt, pptx
- Text: .txt, .xml
- CSV: .csv
- TIFF: .tif, .tiff
- PDF: .pdf
- Bilder: .png, .gif, .bmp, .jpeg

## SideNote® Privatnotiz

- Maximale Zeichenlänge: 512 Zeichen inkl. Leerzeichen
- Die Privatnotiz wird nicht im Zustellungsnachweis, in Reports oder in der gesendeten Nachricht aufgeführt

# Der Gewinn für Ihre digitale Kommunikation

- **Optimieren Sie Ihren Datenschutz:** Versenden Sie durchgehend verschlüsselte Nachrichten und verfügen Sie z. B. mit Diensten für eine vollständige Löschung von Metadaten über einen optimalen Schutz vor Datenlecks.
- **Minimieren Sie Ihr Risiko:** Ihre wichtigen E-Mails und Transaktionen können sehr beweiskräftig verwendet werden. Der „Eingeschriebene Zustellnachweis“ enthält alle Nachweise, wer wann was zu wem gesandt hat.
- **Erhalten Sie Gewissheit:** Durch den „Eingeschriebenen Zustellnachweis“ wissen Sie jederzeit wann Ihre elektronischen Dokumente versandt, zugestellt und geöffnet wurden. Das lästige telefonische Nachfragen, ob wichtige E-Mails auch wirklich angekommen sind, gehört der Vergangenheit an.
- **Steigern Sie Ihre Effizienz:** Sie benötigen keine extra Webaccounts oder Software, um den Versand oder Empfang von vertraulichen E-Mails zu managen. Alle E-Mails werden zentral bei Ihnen gespeichert. Das zusätzliche Kopieren von Dokumenten entfällt.
- **Erhöhen Sie Ihren Erfolg:** Schnellere Vertragsabschlüsse bedeuten frühere Einnahmen und bessere Absicherung gegenüber dem Wettbewerb in der Angebotsphase.
- **Sparen Sie Zeit:** Verschenden Sie keine Zeit mehr für Bemühungen am Faxgerät, für Gänge zum Postamt oder das Warten auf die Gegenzeichnung und Zustellung. Alle Transaktionsnachweise werden elektronisch geliefert und automatisch sortiert.

## Unser Versprechen

### Auf allen Wegen sicher kommunizieren!

Frama ist seit mehr als 50 Jahren in der Kommunikation zu Hause. Wir bieten Ihnen qualitativ hochwertige Produkte und Dienstleistungen für die digitale Kommunikation. Es ist unser Anspruch, Ihnen in allen Belangen einen ausgezeichneten Service zu bieten und Ihre Wünsche zu erfüllen.

### Sicher. Effizient. Einfach.

**Frama, die intelligentere Wahl für eine sichere digitale Kommunikation.**

### Kontakt

Frama Deutschland GmbH  
Christinenstraße 2  
40880 Ratingen

02102 8927-0  
info@frama.de  
www.frama.de