TECHNOLOGY GUIDE TO MEET GDPR COMPLIANCE FOR DATA PRIVACY FOR EMAIL

General Data Protection Regulation

Prepared by technologists at **Frama** with
Foreward by the Association of Professional Compliance Consultants

Frama Communications, a specialist for technology related compliance and digital transformation, prepared this analysis considering its years of first-hand experience with the technologies considered and knowledge of the European General Data Protection Regulation. The Frama team has more than a decade hands-on experience with the latest IT-Security standards and compliance regulations for secure handling of financial and private information in today's digital world.

FOREWORD

In Europe, the new European General Data Protection Regulation (GDPR) creates an environment of heightened awareness of data privacy issues. It also brings an enforcement framework with enough teeth to change the way businesses that deal with consumer data protect consumer privacy.

GDPR defines what is to be achieved rather than how the requirements should be fulfilled. Consequently, it does not state a requirement to use a specific method of encrypting email, but it does require the handler of consumer non-public and personal information to maintain not only privacy of that information, but also the ability to demonstrate compliance with the privacy requirements. These requirements are discussed detail in GDPR Article 5 Clause 1(f) and 2, and Article 32 Clause 1(a) and 1(d) which focus on the requirement to protect personal data during transmission with the ability to demonstrate fact of protection of personal data.

An easy target for GDPR enforcement is watching how organisations protect the privacy of information transmitted to external parties. Email is the primary means of business information delivery today. As such, privacy related to email will be one of the principal areas to be inspected in a compliance audit and, therefore, it will be essential for regulated companies to retain auditable proof of fact of private email transmissions.

Why is “proof” important? There are many ways to encrypt email, nearly all of which make it more complicated for the intended receiver to review the message. Therefore, a tendency for senders, unless there is consequence, is to not use email encryption systems that are in place and available for use. The fact of an email encryption system being available for use is not fact of use. “Fact of Use”, we believe, will be a key criterion in regulatory audits, and in any case, a basis to protect organizations from accusations of a data privacy or GDPR compliance breach.

This paper marks a significant contribution to the GDPR compliance debate, by providing a robust assessment of the concerns and a powerful methodology to guide practical compliance. It also offers useful parameters that an organization should consider in its selection of an appropriate solution and a perspective on several of the leading offerings.

Nick Hawke, Chief Executive Officer

Association of Professional Compliance Consultants

London, England

www.apcc.org.uk

SUMMARY OF FINDINGS

For the purposes of GDPR data privacy compliance related to e-mail, e-document delivery, and e-signing systems, the RMail® solution, and its related e-signature and digital forms services are an ideal solution.

> ***"RMail is the professional solution for secure email that everyone can use. Ticks all of the boxes, easy to manage, simple to deploy and very elegant."***
>
> ***- Robert Cohen, Futurae CEO, former CIO of Charles Russell Speechlys, London, England***

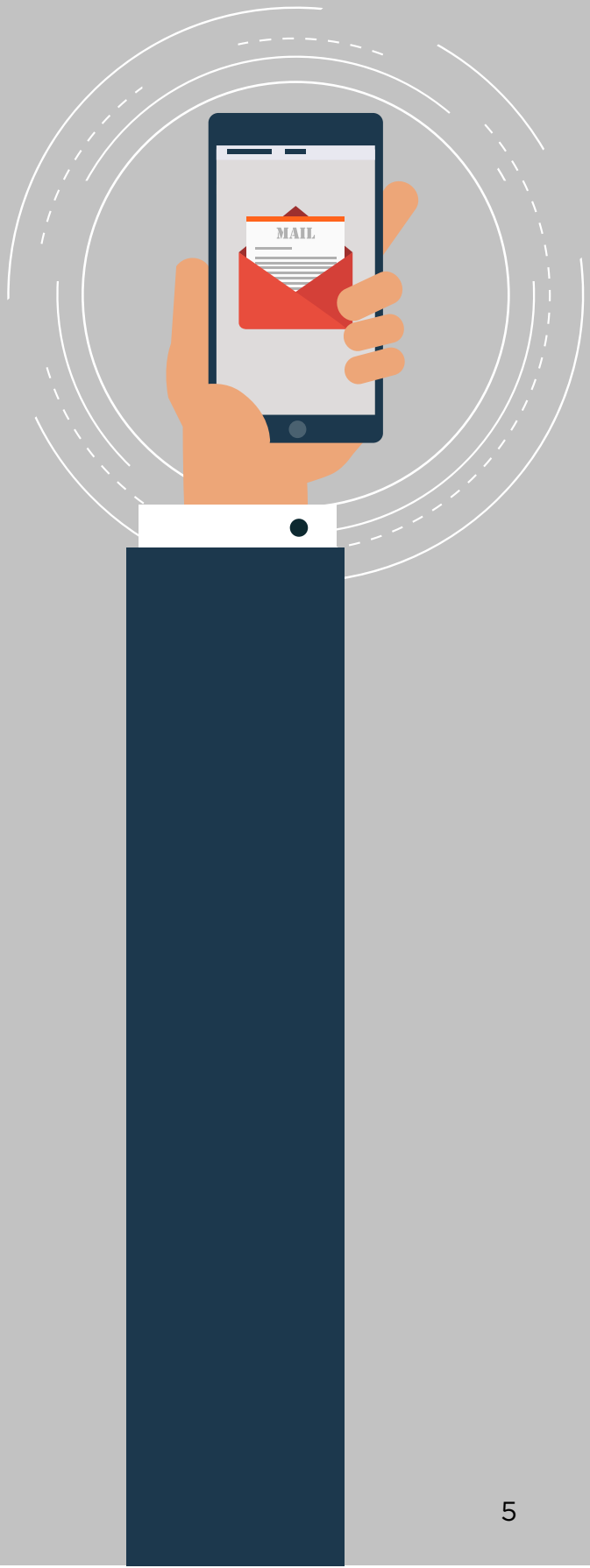
We find the RMail® solution ideal, after a thorough analysis of the degree in which different offerings satisfy criteria important to the financial services industry in the United Kingdom and Europe-wide. While GDPR's focus is in the broad financial services sector (including banking, lending, insurance, residential real estate, estate planning, investment management, and investment banking), we believe other sectors and businesses active in European markets covered by GDPR should likewise find RMail to be their top choice.

SCORECARD SUMMARY: CRITERIA WEIGHTED, TECHNOLOGIES SCORED, DISCUSSION IN GUIDE

Evaluation Criteria			Providers/Technologies							
Top Level	Next Level	Weighting	PKI	PGP	RMail	PDF	TLS	Link Retrieval	HTML Wrapper	File Sharing
Protection		3	**30**	**24**	**54**	**33**	**21**	**27**	**27**	**12**
	Interception		*5*	*5*	*5*	*5*	*3*	*3*	*3*	*2*
	Eavesdroppers		*5*	*3*	*5*	*3*	*2*	*3*	*3*	*2*
	Social Engineering		*0*	*0*	*4*	*0*	*0*	*0*	*0*	*0*
	Automated Rules		*0*	*0*	*4*	*3*	*2*	*3*	*3*	*0*
Utility		3	**42**	**30**	**72**	**48**	**45**	**24**	**27**	**24**
	Simple for Sender		*2*	*1*	*5*	*4*	*4*	*2*	*2*	*2*
	Simple for Receiver		*2*	*1*	*5*	*3*	*5*	*2*	*2*	*2*
	Peace of Mind		*4*	*2*	*5*	*3*	*1*	*1*	*2*	*1*
	No Storage		*5*	*5*	*5*	*5*	*5*	*1*	*1*	*1*
	Flexible Configurations		*1*	*1*	*4*	*1*	*0*	*2*	*2*	*2*
Audit-Ready Proof		2.5	**0**	**0**	**25**	**0**	**0**	**0**	**0**	**0**
	Certified Compliance		*0*	*0*	*5*	*0*	*0*	*0*	*0*	*0*
	Independent Authentication		*0*	*0*	*5*	*0*	*0*	*0*	*0*	*0*
Empowering		2	**6**	**2**	**28**	**6**	**0**	**10**	**10**	**12**
	Encrypted Reply		*3*	*1*	*4*	*3*	*0*	*3*	*3*	*2*
	Tracking		*0*	*0*	*5*	*0*	*0*	*2*	*2*	*2*
	Encrypted Productivity		*0*	*0*	*5*	*0*	*0*	*0*	*0*	*2*
Measurement		1.5	**0**	**0**	**15**	**0**	**0**	**3**	**3**	**3**
	Reporting		*0*	*0*	*5*	*0*	*0*	*2*	*2*	*2*
	Training Metrics		*0*	*0*	*5*	*0*	*0*	*0*	*0*	*0*
Total Score			**78**	**56**	**194**	**87**	**66**	**64**	**67**	**51**

RMail scores more than double its closest technical alternative when considering criteria most important to regulated businesses dealing with consumer information. RMail is designed to not only make it easy to enhance data privacy compliance in case of compliance audits or accusations of data breach, but also to provide an important tool to protect strategic business secrets.

> ***"RMail is easy to integrate, provides state-of-the-art technology, and it makes it easy to encrypt email; importantly encrypting email in a way that automatically provides audit-ready proof of GDPR compliance on a message-by-message basis for the transfer of personal data. Recipients' acceptance and the simplicity in communicating with third parties have convinced us to use RMail extensively in our company."***
>
> ***- Kemal Webersohn CEO WS-Datenschutz GmbH, Berlin, Germany***



CONTENTS

GDPR CREATES HEIGHTENED ENFORCEMENT, MEANINGFUL FINES

The General Data Protection Regulation (GDPR), Regulation ((EU) 2016/679) calls for penalties of up to 4% of global turnover with a maximum of fine of 20 million Euros. Considering the potential of a fine tied to a percentage of global turnover, compliance consultants should educate their clients on the importance of maintaining a record of 'proof of data privacy compliance'; better yet, automated, demonstrable proof on a message by message basis (as described in GDPR Article 5 Clause 1 & 2 and Article 32 Clause 1) as accountability is a key requirement of the GDPR directive.

Businesses dealing with consumer information will now be compelled not only to transmit information securely, but also to retain auditable proof of compliant, secure email delivery. For many businesses, new requirements will require them to change email encryption services altogether. Auditable proof of encryption compliance will be needed to deal with compliance audits and the potential of accusations of data breach; particularly when the fines prove to be as steep as the regulators have declared they will be.

The main industries that will be targeted are those dealing with third-party consumer financial or health information --- broadly speaking, those businesses dealing in consumer health care and financial services (banking, lending, investment advisory, insurance, residential real estate, etc.), and in functional business areas, such as, human resources and customer service.

> ***"Having deployed RMail for over a decade while CIO of one of the largest European law firms dealing with private wealth and corporate clients, I see RMail as an essential piece of any company's data privacy and compliance plan. RMail takes a smart, different approach; and belongs even if other secure systems are already in place."***
>
> ***- Robert Cohen, former CIO of Russell Speechlys, London, England***

TECHNOLOGY EVALUATION CRITERIA

The following five evaluation categories (protection, utility, audit-ready compliance proof, empowering, and measurement) are the most important elements of an email encryption technology or service considering the requirements in GDPR for protecting personal data; in particular Article 5 for security, confidentiality, and accountability, and Article 32 for encrypting and assessing the effectiveness of technical measures to ensure securing.

Article 5 Clause 1(f) calls for maintaining the confidentiality of personal data, stating, "personal data shall be processed in a manner that ensures appropriate security of the personal data...using appropriate technical or organisational measures ('integrity and confidentiality')".

Article 5 Clause 2 creates the need to maintain demonstrable proof of compliance with the confidential treatment of personal data, stating, "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

"*Article 32 Clause 1(a) specifies use of encryption to secure personal data, stating, "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data".*

Article 32 Clause 1(d) calls for regular assessments to ensure the security of the processing, stating, "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

1 PROTECTION

A **Protect from Interception** – protect the message in transit across the Internet, regardless of server, provider, or settings, at the recipient. This should also protect against common interception tactics that defeat standard TLS server sending, such as TLS Downgrade Attacks that are most successful when there is no built-in fall back to another encrypted delivery method if the recipient server always or intermittently reports that it cannot accept a TLS transmission.

B **Protect from Eavesdroppers** – option to protect the message as it transfers from sender through sender organisation and as it transfers through to the recipient destination. There are different categories of eavesdroppers ---- it could be curious staff inside a sender or receiver organization, Internet criminals, or practices of an outsourced provider that has access to email. In the latter example, consider if a recipient uses Gmail, and the sender's message is encrypted to the receiver's email provider (Gmail in this case). In this example, the receiver's provider offers a free email service known to rely on marketing user information. The message content at the receiver will be analysed by Google, with elements recorded, and a profile sold in the point of "improving" the service (aka the marketing profile of sender and/or recipient based on content of the email associated with the email addresses and other data collected).

C **Protect from Socially Engineered Leaks** – a data protection plan should also consider how to protect from an imposter email received by human resources, finance, or other staff that deal in customer sensitive information, which lures them into replying with sensitive data attached. A common tactic is for an Internet criminal to pretend that they are an employee asking for benefits or tax information, by email to the human resource department, and the reply email is configured so the staff's reply with the information, unknowingly routes to the internet criminal. The technology industry calls this a "whaling" attack – a more socially engineered approach to "spear-phishing". The Federal Bureau of Investigation calls this a type of Business Email Compromise attack. The best solutions will detect for this type of socially engineered data leak.

D **Automated Rules** – some may prefer the option for a sender to direct the server to encrypt a message using content added to the message before sending, such as a key word in the subject field, or based on matches of content in the message to content policies added at the server. This may be useful in certain situations.

2 UTILITY

A **Simple Enough that it is Used (and Enjoyed)** – if the service is too complicated for the sender, the sender may ultimately not use the service. If the sender, for example, needs to engage in an encryption key or certificate exchange with the intended recipient, service use will be dramatically limited. Simplicity of use is essential in today's business environment.

B **Simple for Recipient, Avoids Complaints** – if the service is cumbersome for the recipient, for example, mandating numerous steps to set up an account to retrieve messages, the receiver will naturally complain to the sender or may never pick up the sender's important message. This becomes critical when the sender is sending private information where they also need proof of delivery, for example information related to a customer account, investment risk disclosures, etc. In these cases, uploading to a portal or sending a link with a complex process to retrieve will not likely deliver the information to the recipient, and may not constitute successful compliance with delivery or notification requirements.

C **Peace of Mind** – providing the sender with proof of delivery, proof of fact of encrypted delivery; and providing the recipient with visible markings of fact that the sender elected to treat the information as sensitive and transmit it securely to the recipient. Simple use of TLS, for example, does neither of these.

D **No Storage** – most companies prefer there not to be another location where messages are stored in transit as this creates another risk where the message may be breached. The intermediate storage server security should be monitored, and it creates a potential point for subsequent data access depending on the intermediate server's data retention and deletion techniques. For example, if one uses a file sharing service to transmit a sensitive document, users rarely return to delete the document after transmission. The document remains accessible at the shared link for an extended period. Also, link-retrieval secure e-delivery systems often store a copy on an intermediate server until the document is retrieved (and it may never be), for extended periods of time, or even if retrieved, may not have optimal deletion processes. These can unnecessarily expose sensitive data.

E **Flexibility of Configurations** – for small businesses, default settings may suffice, but for mid-sized and large businesses, there may be a need to use different secure delivery methods depending on the message content, size, recipient, route (i.e. internal vs. external message), retention policy (visible content in archive or encrypted in archive), or even sender department or sender within a department (i.e. executive vs. staff customer account manager). The best systems will provide one-click options for a sender to alter the method of encrypted delivery based on a situation at their discretion; as well as provide administrators with the ability to force certain methods to occur for certain senders or for certain messages.

3 AUDIT-READY COMPLIANCE PROOF

A **Certified Proof of Compliance** – with the significance of GDPR fines for a data breach, it is imperative that the sender organisation has audit-ready proof of fact of encrypted delivery, on a message by message basis. Simply having a "policy" in place does not mean the policy was functioning properly. For example, a policy may automate the transmission by TLS, but that does not mean that the message went by TLS (consider a TLS Downgrade Attack). It does not mean the server was functioning properly if looked back upon months or years later, when a dispute or breach is being investigated. Audit-ready evidence on a message-by-message basis is most desirable, and preferably if this is easily demonstrated in a compliance review, compliance audit, or in case there is an accusation of a data breach by a sender (which can happen if there is a data breach at the recipient's system or after a receiver forwards a message onward).

B **Independent Authentication** – The importance of third-party verifiable evidence protects the sender organisation, in particular if the recipient claims a data breach occurred. If the sender organisation generates meaningful worldwide revenue, and the regulator provides "whistleblower" rewards as a percentage of fines for data breaches, the sender must retain easy-to-demonstrate third party evidence that any claim of a breach must have occurred after the message was received securely at the recipient's system (or after they forwarded it on). It is preferable to have a record on a message by message basis that can authenticate that content was successfully delivered encrypted and that can provide proof to mitigate risk of accusations of a data breach. This may minimise the sending organisation from being targeted.

4 EMPOWERING

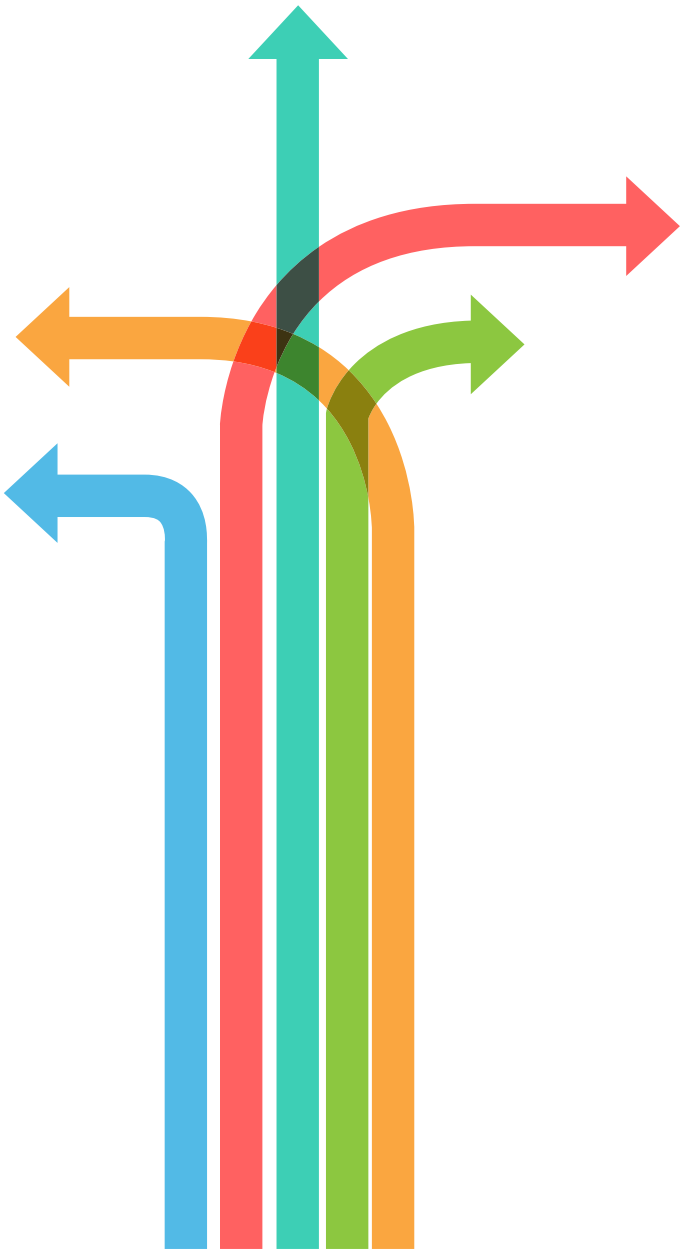
A **Tracking** – email open tracking and secure file download tracking provide insight and data to a sender that is useful to enhance a business process.

B **Timestamped Proof of Content Delivered (for Required Notices)** – in many situations, the information securely transmitted is required to be delivered to the recipient yet also contains sensitive data (i.e. payslip data, investment risk notices, financial account for delivery of account statement details, proof for delivery of loan terms).

C **Encrypted Reply** – it is important to consider the reply email. First, permitting the recipient to reply and add documents in a process that permits secure transmission back to the sender. Second, to minimise risk of inadvertent replies back to the sender that return the originally sent message thread content unencrypted back to the sender.

D **Encrypted Productivity Tools** – security that adds productivity empowers users. Having e-signature and large file transfer processes that can encrypt the entire transaction creates the opportunity for process improvement in a secure, compliant manner.

E **Record Consent** – it is useful to have a tool that also records recipient e-signoff or consent to data protection disclosure.



5 MEASUREMENT

A **Reporting of Use** – Automated reports that are granular enough for administrators to monitor who in an organisation is using secure messaging services and may indicate who in the organisation needs more training, and where to close potential security gaps.

B **Training Success Metrics** – Reports that track change in use (increase or decrease) can measure the success (or failure) of staff security training programs and may provide insight into areas of potential security gaps.

TECHNOLOGIES CONSIDERED

This analysis considered the main technologies used for encrypting email, and scored these technologies against the above criteria, with each criterion scored on a scale of 1 to 5, 5 meaning the criteria is satisfied at the highest levels.

A. **PKI:** Exchange of public keys generated by sender and receiver digital certificates, shared between sender and receiver prior to sending messages. These "keys" are often stored in the Microsoft Outlook program. Use generally requires sender and reviver to have an advanced email program such as Microsoft Outlook full desktop installation or Lotus Notes; generally, not Gmail or web email programs.
    - ***Providers:*** *Verisign, Globalsign*

B. **PGP:** Exchange of keys generated by sender and receiver. Generally, sender and receiver need email programs that are configured to manage the key exchange, or sophistication among users to deal with this type of encryption. Some services attempt to make this easier to use.
    - ***Providers:*** *Open X-Change, GMX*

C. **RMail:** Simple, automated encrypted email delivery system for secure and certified delivery from any sender email program to any recipient email program with default automation for the simplest user experience. There are automatic fall-backs and alternatives depending on the recipient system, type of message, preference of sender, preference of recipient, etc. RMail also makes it easy to encrypt internal and external email using the same interface and process --- an important function for those dealing in private client matters and strategic transactions (RPX option). RMail may use, depending on set-up, a combination of PKI, TLS, HTTPS and AES-256-bit PDF encryption, all designed to operate behind the scene to automatically configure for the simplest secure user experience.

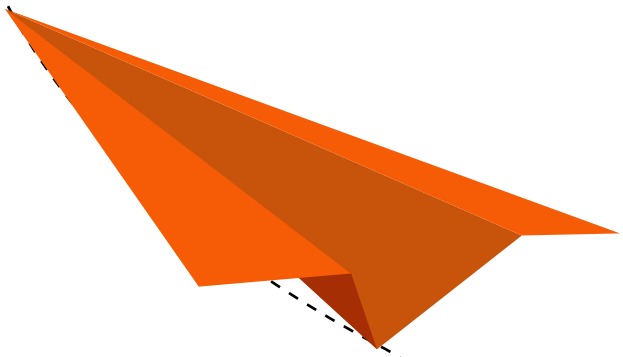
   - ***Providers:*** *RPost, Frama*

D. **PDF:** AES 256-bit PDF encryption, where the message is printed into PDF format, the attachments are embedded in their native format, and the PDF serves as an encrypted wrapper for the message body and all attachments. The encrypted PDF file is attached to the email delivered to the recipient, and the message remains encrypted inside the recipient inbox.

   - ***Providers:*** *RPost (RMail option with variety of configurations), UTM*

E. **TLS:** Transport layer security, connecting from sender server to recipient server via a secure encrypted transmission. This only secures to the recipient server and requires recipient servers to be configured to operate with this option (which is not ubiquitous or certain) and without a fall-back, is susceptible to TLS Downgrade Attacks (tricking the sender server into thinking the recipient server cannot accept a secure transmission, and then the sender server sends unencrypted).

   - ***Providers:*** *Office 365, RPost (RMail option has fall-back to PDF AES-256-bit encryption), MessageSystems*



F. **Link Retrieval:** Store and forward systems that send an email out with a link to request the recipient sign-up for an account, go through several required steps, all needed to view and download the sent message. This requires storage of the message by third parties while waiting for the recipient to download, and the messages are often abandoned as recipients without incentive to go through the steps to retrieve, tend not to.

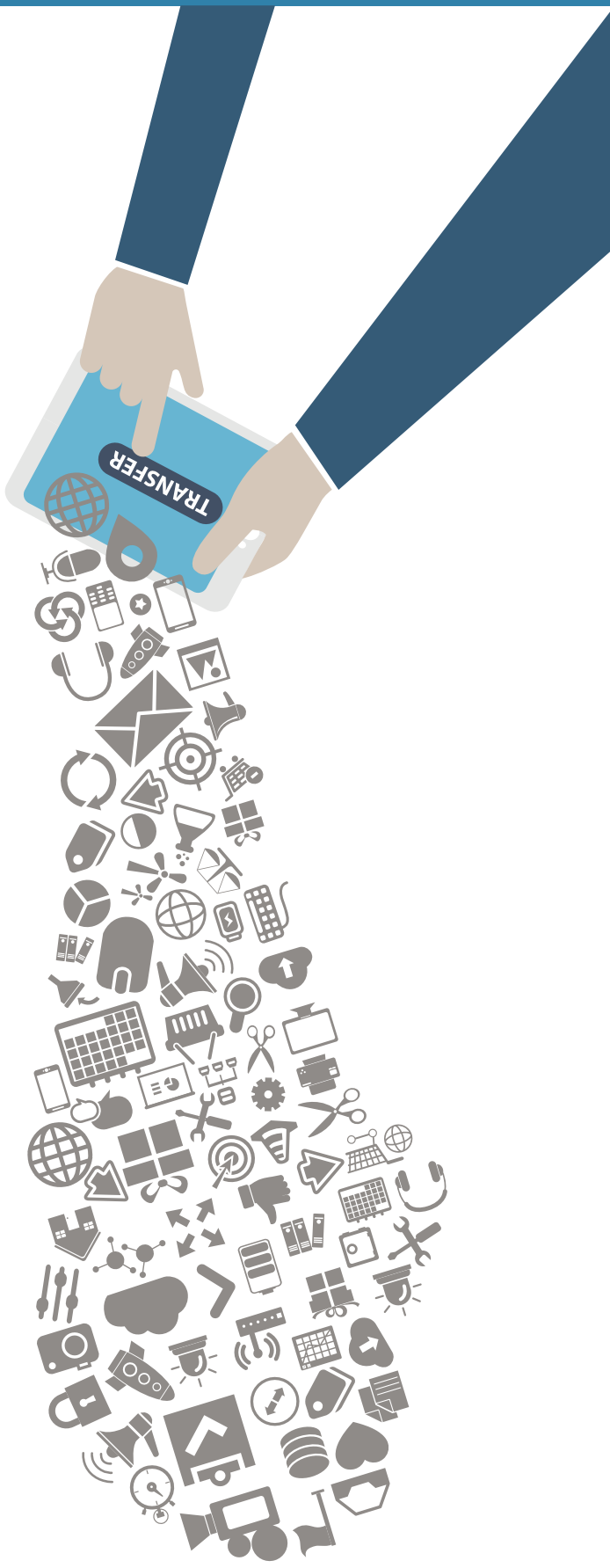
   - ***Providers:*** *Zix, Mimecast*

G. **HTML Wrapper:** Systems that send an email out with an HTML file attached, the HTML file being large as it contains the message and all attachments encrypted. When a recipient clicks on the HTML file, it brings the recipient to a webpage to sign-up for an account. After going through several required steps, the message is transmitted back from the recipient to the sending server, and then displayed in a browser from the sending server, for the recipient to view and download the originally sent message. Messages are often abandoned as recipients without incentive to go through the steps to retrieve, tend not to. If file attachments are several megabytes in size, the recipient system often locks up as files are transmitted from their email back to the sending servers.

   - ***Providers:*** *HPE Voltage*

H. **File Sharing:** Systems that require the user/sender to upload a document to an online storage area, and then invite a recipient to have access to the online folder to view and download the file. This is a cumbersome process to send messages "as email" as the message body is not easily sent or read associated with the file exchange. Links further should be transmitted inside encrypted email (vs a regular email) and links should have password access, otherwise the links in emails sent could be accessed by bots to download files.

   - ***Providers:*** *Office 365 OneDrive, Microsoft Rights Management Server, Google Drive, Box, RPost (RMail has a secure file sharing option included that works around the noted drawbacks)*



IV ANALYSIS & SCORECARD

To identify the top recommendation, we considered GDPR compliance alongside hacker sophistication, and all the issues related to the abovementioned service evaluation criteria and considered technologies. The result is a scorecard that identifies the top recommendation.

In each technology category, we have listed several service providers or suppliers and at the end, we have provided a list of certified providers of our recommended technology.

We follow with a short description on how the recommended technology or service provider specifically meets each requirement. The short description is not meant to reflect all of the considerations for each criterion.

The chart below is also viewable on the following page in larger print.

SCORECARD

Evaluation Criteria			Providers/Technologies								
Top Level	**Next Level**	**Weighting**	**PKI**	**PGP**	**RMail**	**PDF**	**TLS**	**Link Retrieval**	**HTML Wrapper**	**File Sharing**	**Notes**
Protection		3	30	24	54	33	21	27	27	12	
	Interception		5	5	5	5	3	3	3	2	*PKI, PGP, RMail, PDF don't store messages, don't require link-registration processes*
	Eavesdroppers		5	3	5	3	2	3	3	2	*PKI and RMail are only ones that have the option to protect from sender desktop to recipient inbox*
	Social Engineering		0	0	4	0	0	0	0	0	*Only RMail includes Anti-Whaling email imposter detection.*
	Automated Rules		0	0	4	3	2	3	3	0	*PKI, PGP, File Sharing are not systems that facilitate automation*
Utility		3	42	30	72	48	45	24	27	24	
	Simple for Sender		2	1	5	4	4	2	2	2	*RMail has the most elegant user experience inside Office 365, Gmail, Zimbra, or by policy*
	Simple for Receiver		2	1	5	3	5	2	2	2	*RMail, TLS simplest recipient experience, PDF simple. PKI, PGP key management complex*
	Peace of Mind		4	2	5	3	1	1	2	1	*PKI, RMail provide best visibility of encrypted delivery for sender, receiver*
	No Storage		5	5	5	5	5	1	1	1	*Link, HTML, File Sharing require storage by service provider*
	Flexible Configurations		1	1	4	1	0	2	2	2	*RMail has most commercial-off-the-shelf configurations*
Audit-Ready Proof		2.5	0	0	25	0	0	0	0	0	
	Certified Compliance		0	0	5	0	0	0	0	0	*Only RMail provides certified proof of encrypted transmission*
	Independent Authentication		0	0	5	0	0	0	0	0	*Only RMail provides automated authentication of secure transmission forensics*
Empowering		2	6	2	28	6	0	10	10	12	
	Encrypted Reply		3	1	4	3	0	3	3	2	*Various elements to secure reply. RMail has most options*
	Tracking		0	0	5	0	0	2	2	2	*RMail tracking not relient on recipient compliant action; others require recipient to take compliant action*
	Encrypted Productivity		0	0	5	0	0	0	0	2	*RMail and File Sharing add elements of productivity, RMail adds encrypted e-signoff*
Measurement		1.5	0	0	15	0	0	3	3	3	
	Reporting		0	0	5	0	0	2	2	2	*Some service providers include reporting, RMail most robust*
	Training Metrics		0	0	5	0	0	0	0	0	*Only RMail focuses on optimizing training via metrics*
Total Score			78	56	194	87	66	64	67	51	

Scoring
Ratings are on a scale of 1 to 5, 5 being top rated
Weightings are on a scale of 1 to 3, 3 being most important criteria

Sample of providers:
PKI: Verisign, Globalsign, Entrust
PGP: Open X-Change, Enigmail, GMX
RMail: Futurae, RPost, Frama
PDF: RPost (RMail option), UTM
TLS: Office 365, RPost (RMail option), MessageSystems
Link Retrieval: Zix, Mimecast
HTML Wrapper: HPE Voltage
File Sharing: Office 365 OneDrive, Google Drive, Box

Technology Scorecard for GDPR Compliance For Data Privacy for Email

Evaluation Criteria			Providers/Technologies								
Top Level	Next Level	Weighting	PKI	PGP	RMail	PDF	TLS	Link Retrieval	HTML Wrapper	File Sharing	Notes
Protection		3	30	24	54	33	21	27	27	12	
	Interception		5	5	5	5	3	3	3	2	*PKI, PGP, RMail, PDF don't store messages, don't require link-registration processes*
	Eavesdroppers		5	3	5	3	2	3	3	2	*PKI and RMail are only ones that have the option to protect from sender desktop to recipient inbox*
	Social Engineering		0	0	4	0	0	0	0	0	*Only RMail includes Anti-Whaling email imposter detection.*
	Automated Rules		0	0	4	3	2	3	3	0	*PKI, PGP, File Sharing are not systems that facilitate automation*
Utility		3	42	30	72	48	45	24	27	24	
	Simple for Sender		2	1	5	4	4	2	2	2	*RMail has the most elegant user experience inside Office 365, Gmail, Zimbra, or by policy*
	Simple for Receiver		2	1	5	3	5	2	2	2	*RMail, TLS simplest recipient experience, PDF simple. PKI, PGP key management complex*
	Peace of Mind		4	2	5	3	1	1	2	1	*PKI, RMail provide best visibility of encrypted delivery for sender, receiver*
	No Storage		5	5	5	5	5	1	1	1	*Link, HTML, File Sharing require storage by service provider*
	Flexible Configurations		1	1	4	1	0	2	2	2	*RMail has most commercial-off-the-shelf configurations*
Audit-Ready Proof		2.5	0	0	25	0	0	0	0	0	
	Certified Compliance		0	0	5	0	0	0	0	0	*Only RMail provides certified proof of encrypted transmission*
	Independent Authentication		0	0	5	0	0	0	0	0	*Only RMail provides automated authentication of secure transmission forensics*
Empowering		2	6	2	28	6	0	10	10	12	
	Encrypted Reply		3	1	4	3	0	3	3	2	*Various elements to secure reply. RMail has most options*
	Tracking		0	0	5	0	0	2	2	2	*RMail tracking not relient on recipient compliant action; others require recipient to take compliant action*
	Encrypted Productivity		0	0	5	0	0	0	0	2	*RMail and File Sharing add elements of productivity, RMail adds encrypted e-signoff*
Measurement		1.5	0	0	15	0	0	3	3	3	
	Reporting		0	0	5	0	0	2	2	2	*Some service providers include reporting, RMail most robust*
	Training Metrics		0	0	5	0	0	0	0	0	*Only RMail focuses on optimizing training via metrics*
Total Score			78	56	194	87	66	64	67	51	

Scoring

Ratings are on a scale of 1 to 5, 5 being top rated

Weightings are on a scale of 1 to 3, 3 being most important criteria

Sample of providers:

PKI: Verisign, Globalsign, Entrust

PGP: Open X-Change, Enigmail, GMX

RMail: Futurae, RPost, Frama

PDF: RPost (RMail option), UTM

TLS: Office 365, RPost (RMail option), MessageSystems

Link Retrieval: Zix, Mimecast

HTML Wrapper: HPE Voltage

File Sharing: Office 365 OneDrive, Google Drive, Box

ENDORSEMENT

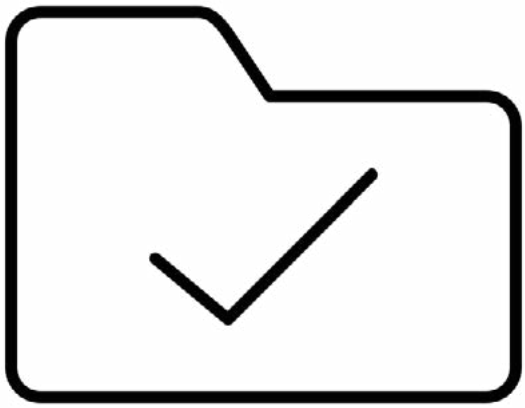
With a top result and a comparative score that is more than double the closest alternative, RMail services are the obvious choice for GDPR data privacy compliance for email, in particular, for regulated financial services or health care organisations.

Those in Europe that are covered by GDPR across industry should review this analysis and also consider use of RMail services as part of their GDPR compliance initiatives.

"As a growing accountancy practice we were looking for a secure email product at an affordable price to help us comply with GDPR. We chose RMail as it returns proof of fact of encrypted delivery to protect the organisation in the event of an external compliance inspection. After a quick and easy to follow training session, we were up and running in no time at all. RMail is easy and straightforward to use, with the knowledge that you are sending sensitive data securely to your clients. RMail is an excellent product and service."

-- ACG Accounting Services, London, England (Member of the IFA).

- *The Institute of Financial Accountants (IFA) is endorsing the use of RMail secure and certified electronic messaging services to support GDPR compliance. www.ifa.org.uk*



VI RMAIL RECOMMENDATION SUMMARY

In the opinion of Frama, RMail has the best approach in terms of simplifying the user experience yet permitting automated fall-back options in case another method of secure delivery is required, or desired on a message-by-message basis.

Simple to use for the sender. *Consider the importance of user simplicity -- ease of use by sender and recipient means more use and less exposure. The "secure encrypted email dilemma" is how to deliver the message securely without negating key benefits of email – simplicity and ubiquity – so it is simple enough that it is used in practice, yet secure enough to protect and comply. There is often a trade-off between security and simplicity – and often "simplicity" loses the battle, until people realise that their "secure" system is underutilised due to user complexity. More secure, but too cumbersome, means less used and potentially more exposure.*

RMail includes all of the automation options and configurations any organisation may need now or in the future, accessible via its Microsoft Outlook and Office 365 add-in, Gmail, Zimbra, Web Apps, Mobile, or Security Gateway. RMail's management interface for administrators provides for robust automated reporting, useful for training and optimising usage.

Consider how well the solutions protect from fines in a data breach. *With a data breach, consider two points: A data breach when the data is: (a) within the sender's control (i.e. where the email is sent from sender to recipient - "security of sender-controlled data"); and (b) after the data leaves the sender's control (i.e. if there is a data breach on the recipient's system or after the recipient forwards the information on to others - "downstream data breach"). The important concept to consider is not which service is more secure (assuming they all meet the security baseline); it is how well they protect from fines in a compliance audit, GDPR examination, or after a reported breach of private information.*

The need here is "Auditable Proof of Compliance" with data privacy rules – there is no "halfway" when it comes to compliance. The importance is to ensure you have an auditable record of precisely what message content (body text and attachments) was in fact sent and received in an encrypted manner to each intended recipient -- and for some notices, precisely when received and opened. This is important because in a data breach after the email has reached the recipient (in the recipient's environment, or after they have passed the information along to others), the sender will need to prove that the breach did not happen "on their watch".

Consider the following: You send an email encrypted with an attached document. The document contains private consumer information. The document is on your letterhead or otherwise shows it originated from you. The recipient forwards the email, or otherwise exposes the information inadvertently, through unauthorised access to their system, or otherwise. There is a claim of a data breach or GDPR violation. Fines are threatened, and, as the document is on your letterhead, you are implicated. How do you protect from being implicated in fines? RMail's "Auditable Proof of Compliance" returns proof of data encryption in case of implication in a breach and can protect you from risk and exposure to fines.

For business compliance use, one should avoid services that do not have a robust audit trail of delivery that can be independently verified as to fact of encrypted delivery, message content delivered and uniform timestamps of sending and receipt. Avoid 'store-and-forward' email systems as they require the recipient to take significant action for the recipient to retrieve the email. Avoid service providers that lack historical track record and substance – be wary of private label resellers of others' services unless you can assess the source. Not all email encryption services and e-delivery providers are the same.

In our opinion, RMail is the only option that empowers users with important secure productivity solutions including the most advanced legal e-signature, Registered Email™ legal timestamped content and e-delivery proof, and secure file sharing for large file e-delivery with certified tracking. These empower users with more productivity with security underlying each.

RMail map to the advanced standards for eIDAS (electronic IDentification, Authentication and trust Services), an EU regulation on electronic identification and trust services for electronic transactions in the internal market established in EU regulation No 910/2014 of 23 July 2014 on electronic identification. RMail's Registered Receipt record is the ultimate in protection in case of any accusation of a data breach or a compliance audit; and maps the British Standards Institute 'Legal admissibility' Code of Practice – BIP 0008.

VI RMAIL WITH MICROSOFT OFFICE 365

As the analysis shows, neither Microsoft Office, Office 365, and Microsoft Outlook (nor Gmail or Zimbra) come with the protection that this Guide recommends. It is important that businesses do not accept superficial and inadequate attempts to solve these problems. Simple TLS (as the chart shows) is nice, but not good enough. Link-retrieval services with policy-based routing may seem nice, but again, not enough (as the chart shows). Rights management server options, OneDrive file sharing, and Read Receipts provide some security and/or tracking; yet they are no replacement for the right encrypted email service combined with Registered Email receipts; in our opinion, standard Microsoft options or advanced features are no replacement for the level of security that RMail provides.

This section provides a guideline for those that may be asked the question, "Isn't Microsoft Office 365 good enough?"

Why install RMail inside Office 365?

RMail® makes Microsoft better for business, adding specialised security for privacy, compliance, and to prevent targeted threats, certified e-delivery tracking and proof, secure large file sharing, and legal e-signatures, all-in-one. RMail installs to run inside Microsoft Office 365 and all versions of Outlook, adding critical email security and business productivity tools that are not included inside Microsoft.

- **Specialised security** — RMail encryption automatically delivers email in a unique way to each recipient, always creating the simplest user experience for the recipient while also returning auditable proof of privacy compliance to the sender; going far beyond basic TLS and link-retrieval systems which store sensitive message content. RMail includes targeted spear-phishing detection specifically designed to prevent imposter email wire fraud and other lures.

- **Certified e-delivery tracking and proof** — RMail includes Registered Email™ advanced open and delivery tracking, returning court-admissible timestamped proof of precise message content successfully delivered – importantly, without requiring any action or setting at the recipient.

- **Secure large file sharing** — With RMail, it is simple to attach up to 1Gb of files to an Outlook email and send securely. RMail file sharing is perfect for security and compliance as it creates a one-time download box that eliminates the risk of inviting download recipients to be able to see the sender's cloud storage file structure, reduces risk by auto-purging files after a pre-set time, includes automatic encryption options, and returns proof of delivery and download.

- **Electronic signatures** — RMail encourages e-signature use as it includes the easiest e-signature process available. Senders simply attach any document in Outlook and one-click send for recipient e-signoff. With RMail e-signatures, there is no need for the sender to set up or pre-configure the document. For those that are looking for more e-sign automation, templates, rules or e-signatures with complex forms, RMail users can access RSign with one extra click. RSign® is an advanced web-based e-signature platform.

- **RMail® is proven** — RMail has been enhancing customer security, compliance and productivity for more than a decade, powered by RPost® patented Registered Email™ technology.

RMAIL FEATURES ARE UNIQUE

What makes RMail email encryption unique, versus what is available in Office 365 packages?

RMail email encryption goes beyond basic TLS and is far simpler than common link-retrieval systems, adding email encryption designed to automatically adapt to ensure the simplest user experience for the recipient.

RMail email encryption makes Microsoft better because it works regardless of the recipient system or action (unlike simple TLS) and it provides the option to send end-to-end encrypted (encrypted from sender's desktop through all email administrators and hosting providers, to the recipient inbox, and inside the recipient inbox) without the need for any digital certificates, key sharing, or download/log-in links.

Specifically, RMail provides:

1. **Simpler user experience for sender and recipient**
    a. RMail is not a store-and-forward link retrieval system (no storage)
    b. RMail email encryption goes beyond basic TLS and is far simpler than common link-retrieval systems, adding email encryption designed to automatically adapt to ensure the simplest user experience for the recipient.
    c. Sender has confidence (and audit-ready proof of compliance) that the email was sent encrypted.
    d. Recipient always has confidence the message was submitted securely. RPost messages are stamped "transmitted securely" to add a layer of visibility to the end-recipient.
    e. Recipients are always given the option to securely reply with the convenience of a one-click secure reply process.

2. **Message — Level Toggle:** from simplest security for business compliance (GDPR) to protecting strategic secrets externally and internally (protect from the RPX feature "Panama Papers" type of situation; the RPX feature permits the sender to force the email to remain encrypted inside the recipient inbox and the recipient archive). Senders can have encryption-at-rest security at the recipient by simply checking a box in the sending process.

> ***"For law firms and those financial services firms engaged in private client matters and financial transactions, it can often be as important to have information barriers internally as it is externally. Unlike services that encrypt at the email gateway, RMail is system that is not only simple and familiar to use, encouraging the wider use for all confidential information, but also permits users to maintain end-to-end encryption for matters that should remain private inside the sender or recipient organizations. This is yet another reason why RMail scored top of the charts."***
>
> ***- Robert Cohen, Futurae CEO.***
> ***RMail end-to-end encryption (RPX) secures the message content at the sender Outlook user interface, through the sender and receiver organizations, through the internet, and while inside the recipient's inbox., former CIO of Charles Russell Speechlys. RMail end-to-end encryption (RPX) secures the message content at the sender Outlook user interface, through the sender and receiver organizations, through the internet, and while inside the recipient's inbox.***

3. **Audit-Ready Proof of Data Privacy Compliance**, message by message. The Registered Receipt™ returned to sender is an email record that provides evidence of fact of GDPR data privacy compliance for transmitted messages.

4. **Email delivery tracking is exposed to sender**, packaged as verifiable proof of delivery. This eliminates requests and investigations that otherwise might need to be conducted by email administrators when important email reported to have been sent, goes missing. This puts the email tracking in the hands of the sender end user, empowering them with more visibility.

5. **Enterprise Security Options**

   a. End user settings, administrator settings, pre-set configurations at installation, etc.

   b. Outbound from sender desktop via SMTP (preserving enterprise outbound policies) with options to encrypt messages at the sender's desktop through and inside recipient inbox (so email outsourcers and email archive companies cannot access email content), to preserve an unencrypted version in sender's archive, or to encrypt to recipient's gateway.

   c. Network administrators can utilise gateway DLP solutions to scan message content and relay certain messages for special RMail processing (encryption, proof of delivery, e-signoff), automatically based on content in the message or based on a sender indication in the message subject field.

What makes RMail large file sharing unique versus Office 365 cloud storage or other cloud storage file share services?

RMail secure large file sharing services include unique auto-purge technology to eliminate risk associated with orphaned documents remaining accessible from old shared links. RMail's large file sharing service includes:

- **One-time Box.** With RMail, the sender does not need to worry about whether the recipient will be able to view their file structure or file directory names.

- **Auto-purge.** With RMail, the sender does not need to go back after the sharing to delete old folders or remove files from folders, improving security and compliance protections.
- **Elegant outlook integration.** User can manage sending elegantly inside Microsoft Outlook.
- **Additional features included.** Email encryption, password access, download/open tracking, and certified delivery tracking and proof.

What makes RMail email tracking unique, versus native Outlook read receipts?

RMail Registered Email™ service provides peace of mind with certified e-delivery proof and visibility of email open tracking information.

RMail also returns proof of compliance (with data privacy requirements related to email transmission, proof of delivery of required notices, etc.). This proof is in a Registered Receipt™ email record returned for every RMail message sent, providing auditable proof of data privacy and e-delivery compliance.

- **Outlook Read Receipts rarely work for external recipients and are very limited.** With Outlook Read Receipts, the open receipt is only returned if the recipient sets their settings to return it (most do not), and even if the receipt is returned, it is not easy to associate it with the original message content, and in fact not possible to irrefutably prove the delivery, uniform time of sending and receipt, and content associated. The Outlook read receipt, if even returned, is simple text that tells little and can be altered with a few keystrokes.
- **RMail tracking works for any recipient without any compliant action at the recipient**. RMail Registered Receipt records include open-tracking without requiring any recipient response, settings or action.
- **RMail Registered Receipt is durable, verifiable, and self-contained authenticatable proof of delivery**, including proof of content (and attachments) and timestamps of sending and receiving, with open tracking.

> *RMail proof of delivery and tracking also provide an independently verifiable record of the content transmitted, regardless of recipient settings to view images; far more powerful and reliable then image tracking gifs that rely on recipients using Microsoft Outlook, for example, to display images. Further, even if images are set to display, these services do not provide a verifiable record of the content delivered/opened or secure transmission.*

What makes RMail e-signatures unique versus Office 365 or other e-signature services?

E-signature services are designed to permit a sender or administrator to be able to control the electronic signoff process among multiple signers. Office 365 does not include e-signature services. Outlook “digital signatures” are very different in that they permit a sender to apply their “identity stamp” to a message or document if they have installed a unique digital certificate.

- **RMail includes e-signature services that make it as easy as attaching a document to a message and sending** to multiple recipients for e-signoff. There is no need to visit websites to upload or configure documents for signing.

- **RMail includes advanced e-sign functionality with different services depending on the sender's needs. RMail** attach-and-send e-signature services enhance productivity without the complexity of web-portals, making it by far the simplest to use for ad-hoc documents. **RForms™** is the simplest way to force signers to sign in specific locations on documents, forms or templates. **RSign®** is a full featured web-based e-signing system more similar to others in the marketplace, yet designed with a simpler user experience and all of the automation features the most sophisticated users require. All provide the most robust forensic authentication records of the e-sign transaction, legal under eIDAS for Europe, and other court admissibility and e-sign laws.

Is RMail's email imposter protection unique?

RMail Anti-Whaling™ email imposter protection is not included in any other email security package or in Office 365. RMail Anti-Whaling is advanced security that detects today's most sophisticated "spear-phishing" imposter email lures targeting finance and HR departments. These lures often trick users into sending money to the wrong party, paying fake invoices, or sending sensitive employee data (tax, pay, health) to adverse parties. It alerts when the user is about to reply or forward a "BEC-type" of imposter email.

RMail's Anti-Whaling technology operates in the full installation version of Microsoft Outlook or Office 365 Outlook. It inspects every message that is replied to, for a specific type of imposter email lure, even when the "Send RMail" button is not selected.

VIII

RMAIL WITH ZIMBRA, GMAIL, MIMECAST, SYMANTEC CLOUD, DROPBOX

Similar to the Microsoft analysis above, other systems that may tout GDPR compliance or try to "check-the-box" for email security do not do it in a way that empowers users with security that will in fact make them more productive --- and most provide superficial security that works in some situations and not others.

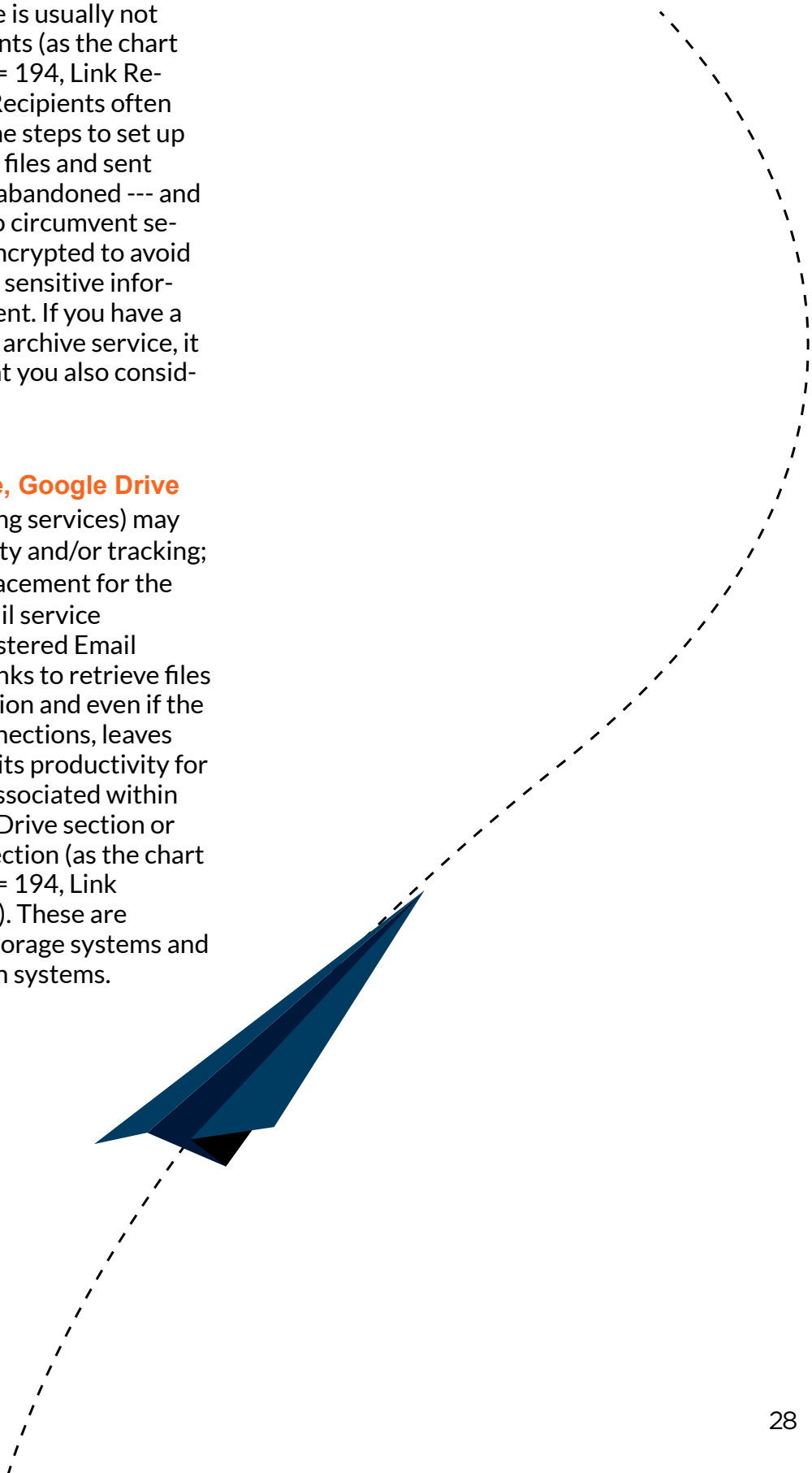
> ***"Professional services firms have a deep commitment to protect their client's information, at rest and in transit. Since professional service firms will have a wide mix of clients using different email systems, it is important to have a system that works equally well in Outlook as it does in Gmail, and regardless of systems that a receiver may have. Simplicity is key. With RMail there is little or no training needed, it secures messages internally and externally, it is a system that provides proof of delivery as well as proof of encrypted delivery, and it looks and feels like your native email application."***
>
> ***Robert Cohen, CEO of Futurae***

Zimbra, as an email platform, does not contain any of the security, compliance and productivity capabilities that RMail adds. It is recommended that companies using Zimbra email platform add the RMail add-in for Zimbra and if policy-based encryption is desired, additionally the RMail Security Gateway. Other email security gateways have the same limitations with any added encryption as noted in the above analysis for "link-retrieval" systems. Link-retrieval services with policy-based routing may seem nice, but again, do not provide enough (as the chart shows, RMail score = 194, Link Retrieval score = 64).

Gmail or G Suite for business does not contain any of the security, compliance and productivity capabilities that RMail adds. It is recommended that companies using Gmail or G Suite for their email platform add the RMail Chrome extension for Gmail. Gmail and G Suite include use of TLS, but this has the same limitations noted in the above analysis for "TLS" systems. Again, simple TLS is nice, but not good enough (as the chart shows RMail score = 194, TLS score = 66).

Mimecast, Symantec Cloud (and other perimeter security/archive services) may offer email encryption using a link retrieval system. From our experience, having a store-and-forward link-retrieval service is usually not preferred by recipients (as the chart shows, RMail score = 194, Link Retrieval score = 64). Recipients often do not go through the steps to set up accounts to retrieve files and sent messages are often abandoned --- and senders tend then to circumvent security and send unencrypted to avoid delays in getting the sensitive information to the recipient. If you have a perimeter security / archive service, it is recommended that you also consider adding RMail.

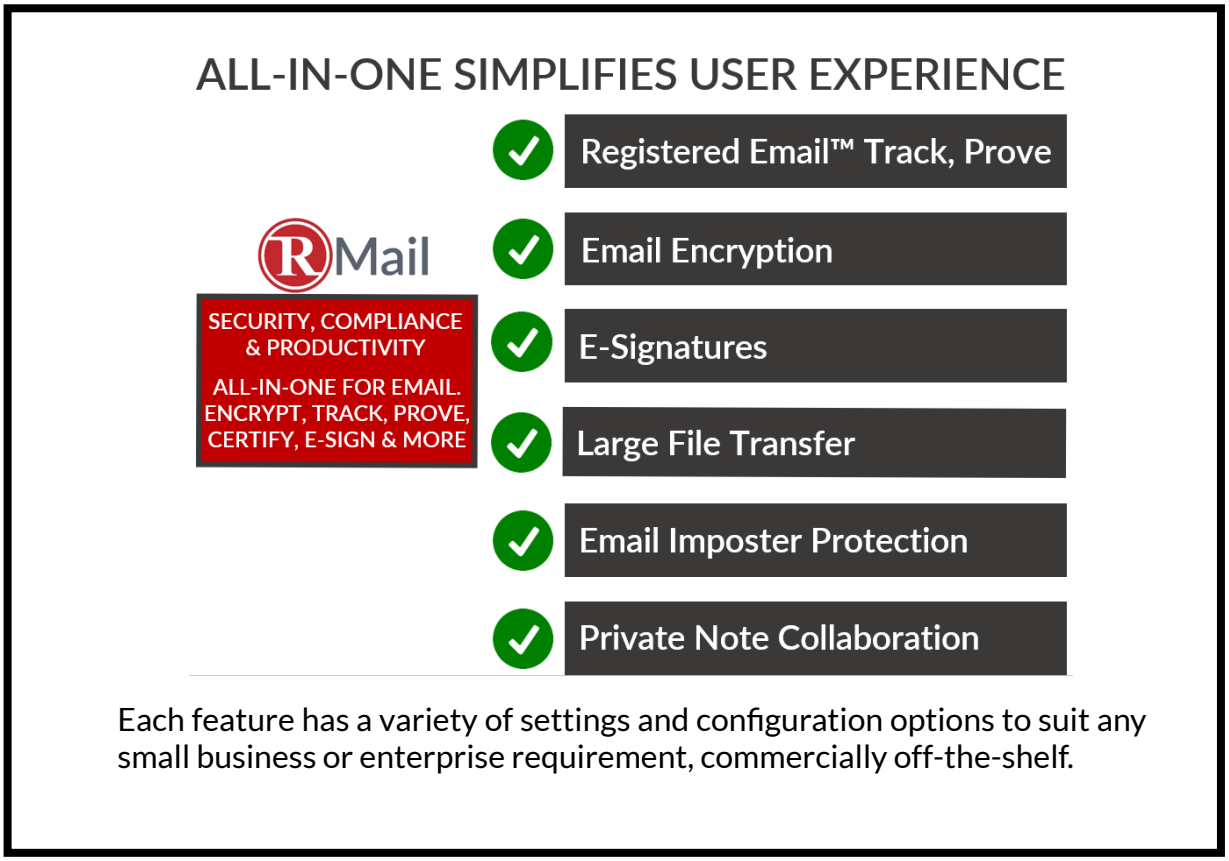
Dropbox, OneDrive, Google Drive (and other file sharing services) may provide some security and/or tracking; yet they are no replacement for the right encrypted email service combined with Registered Email receipts. Send-ing links to retrieve files is not email encryption and even if the links are secure connections, leaves exposure and/or limits productivity for reasons discussed associated within the Office 365 One Drive section or the Link Retrieval section (as the chart shows, RMail score = 194, Link Retrieval score = 64). These are document and file storage systems and not email encryption systems.



IX APPENDIX: ABOUT RMAIL SERVICES

RMail adds Essential Features to Existing Email Programs

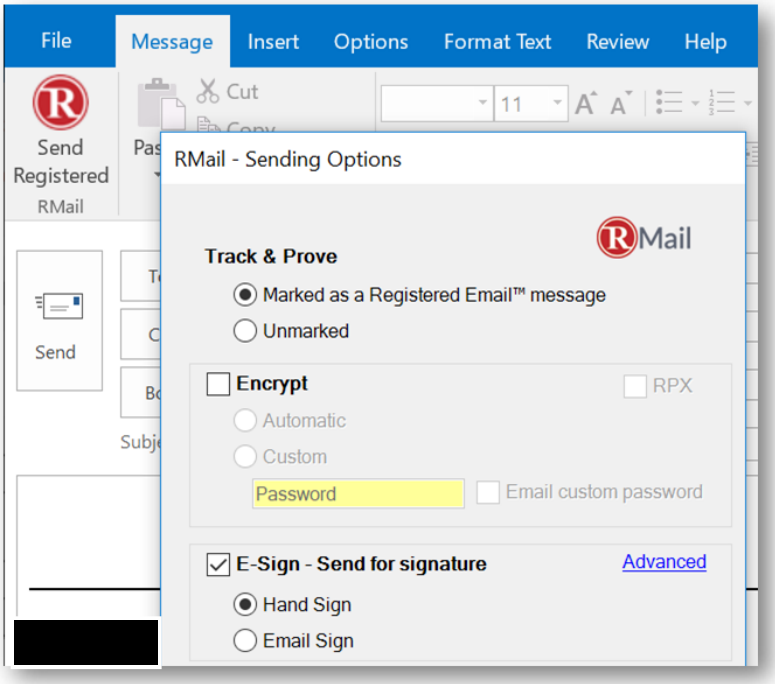
RMail is a logical cybersecurity extension that adds advanced security and productivity features all-in-one. Each main feature on its own is rated among the best in the world by analysts and industry organisations. Customers further benefit with all features included in one app, the RMail app, with the all-in-one aspect of the RMail solution providing a more elegant user experience and a more economical approach (as compared to trying to piece together different features from different vendors if even available). Main RMail features[1] include:

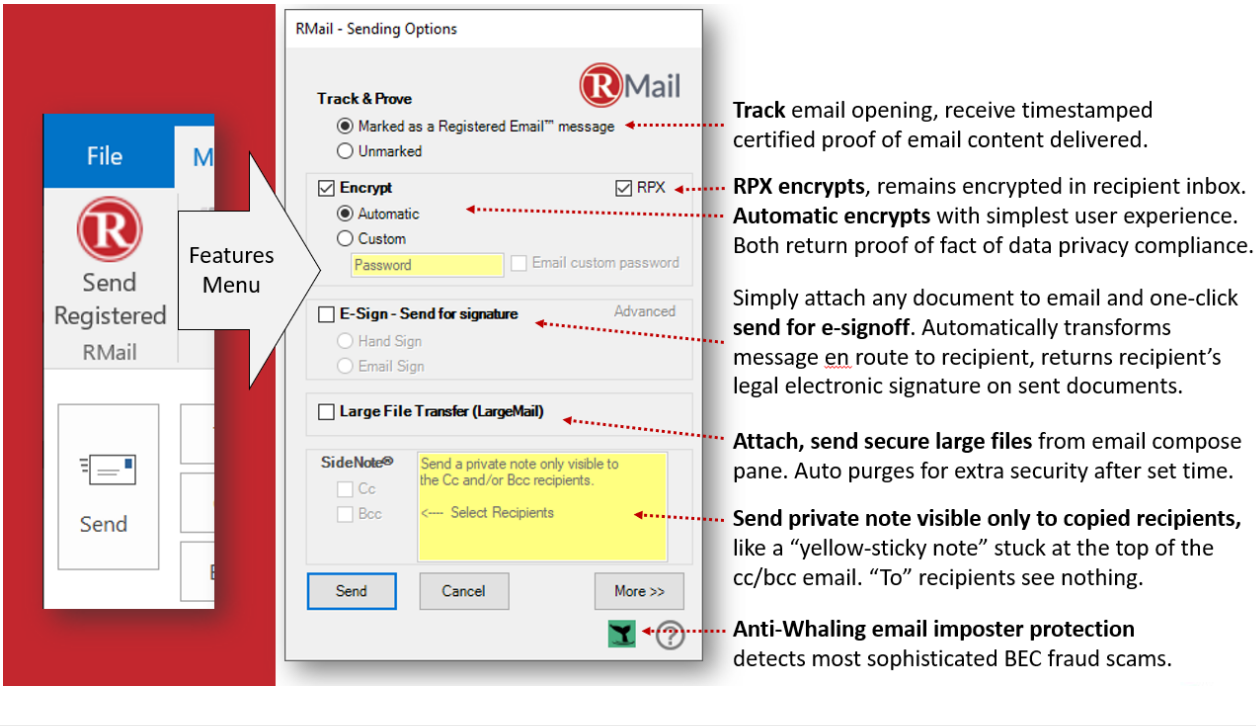


Each feature has a variety of settings and configuration options to suit any small business or enterprise requirement, commercially off-the-shelf.

[1] *Patented and patent pending technologies. A sample of US patents granted by number: 7966372, 9432313, 8782154, 9596194, 8484706, 8504628, 8478981. A list of patents granted in 23 countries is available at www.rpost.com/patents . Pending patents include applications US 15/469,388 among others.*

RMail provides essentials that make email better for business running inside the email user interface (or automated by policy). A "Send Registered" or "Send RMail" button is installed, sitting above the normal "Send" button (see below). When selected, a full featured "RMail – Sending Options" menu pops up. This menu is configurable, and can be suppressed if only the track and encrypt features are desired.





Quick Guide to Benefits

RMail is a security, compliance, and productivity bundle that runs "Inside" Microsoft Outlook, Gmail, Zimbra and other platforms, and adds value for important messages. Each of the services featured below operate with encryption options. The Anti-Whaling feature operates on every message regardless as to whether the "Send RMail" option is selected.

RMail All-in-One Features:

- Encryption Compliance
- Certified E-Delivery Proof
- Email Open Tracking
- E-Signatures
- Secure File Share
- Imposter Email Detection, and more, all-in-one.

RMail Empowers Users:

- Creates Visibility: desire to track opening, delivery
- Empowers: irrefutable proof of who said what when
- Secures: encryption to protect against thieves
- Boosts Productivity: Registered Email™ e-delivery proof, e-sign, large file transfer inside

RMail Desirable Key Attributes:

- Simple enough for individuals
- Secure enough for the largest companies
- Universal – no recipient requirements
- No storage in transit by third parties
- All-in-One integrated offering simplifies

Standard Plan Features

- **Encrypt:** Easily encrypt sensitive emails and attachments for security or regulatory compliance. Includes a one-click encrypted reply option for recipients. Automatically detects and delivers with the simplest user experience for each recipient and provides a toggle option to maintain encryption inside each recipient's inbox. Provides auditable proof of data privacy compliance on a message-by-message basis.
- **Track & Prove:** Track, prove and certify your important emails by sending them as **Registered Email™** messages. Includes timestamped proof of delivery with proof of message body and attachment content. Know precisely when your email has been delivered with open tracking.
- **E-Sign:** Accelerate legally-binding signoff on documents and agreements with simple-to-use electronic signature features. Attach any document and send for recipient e-signoff, with no need to configure the document online. (See **RSign** for advanced online e-signature and automation services).
- **Secure Large File Transfer:** Simply attach large files and send from your email compose pane. With RMail, you may attach and send large files up to hundreds of megabytes per transmission, with options to encrypt. There is no need to visit online portals to create and share folders; there is no need to invite others to have access to your main file repositories. RMail automatically creates a one-time online folder per send for each recipient to retrieve files, and auto-purges the data after a selectable period of time to optimise security and compliance.

- **Imposter Email Protection:** Detects and alerts for the most sophisticated spear-phishing lures; alerting users when they are about to reply to a Business Email Compromise (BEC) imposter email. Users are protected with RMail's "Anti-Whaling" technology.
- **SideNote:** Insert private notes into an email visible only to Cc'd/Bcc'd recipients, to provide copied recipients with private context as to why they have been copied on the original message.
- **Auditable Tracking and Verifiable Proof:** A Registered Receipt™ email record is automatically generated and returned to the sender with every RMail message sent, to provide the sender verifiable and auditable proof of who said what when, who agreed to what when, or fact of data privacy compliance.

Business Plan Features

Includes all Standard Plan features optimised for power users, plus an online management console.

- **Power Users:** Optimised for higher volume senders.
- **Reporting Online:** View service use volume by user, by feature, by date range, by delivery status or by message element.
- **Custom Report Delivery:** Create custom use reports and schedule automated encrypted delivery in a variety of formats.
- **Productivity Enhancements:** Adjust advanced settings such as e-sign order for signoff (i.e. sequential signing where one person has to complete the signing process before the next person is invited to signoff), form field e-sign tags, larger file transfer limits (up to 1 GB per transmission) or length of time large file transfer data is available for recipients, and more.

Add-On: Security Gateway & Customisation

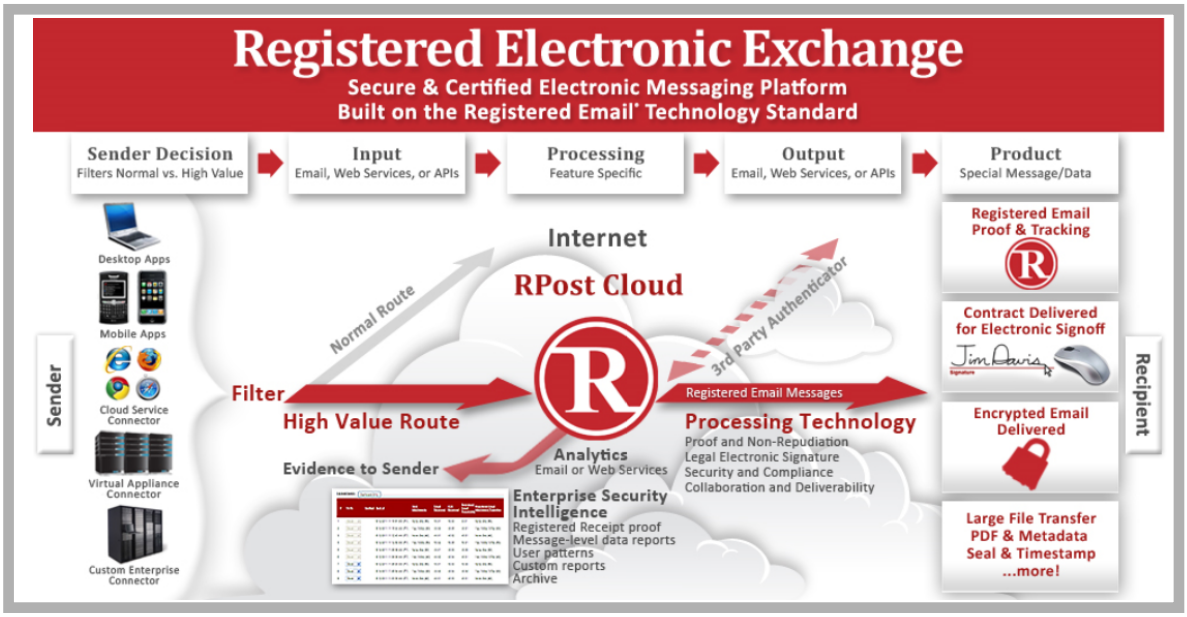
- **Security Gateway Features:** The RMail Security Gateway adds policy-based email encryption and much more, as an add-on for designated RMail Business Per User Plans and RMail Shared Volume Plans. For example, a company can create rules at the server to encrypt certain email based on a content indicator in the sender's email.

> *The RMail Security Gateway is installed as an add-on to the customer messaging server environment such that inbound and/or outbound message traffic passes through. This adds a native content policy engine to provide data loss prevention (DLP) content inspection and automated routing of content identified messages for encrypted delivery, for Registered Email certified e-delivery proof, or for recipient e-signoff. Automated encryption enforcement may be triggered based on sender, recipient, tags by user (e.g., adding "Secure" or "(R)" to the subject line), data classification tags, content inspection of messages or attachments, and combinations. The RMail Security Gateway also provides market leading messaging security including anti-spam, anti-virus, anti-spyware, anti-ransomware and other threat prevention scanning on in-and-outbound email traffic.*

- **Customisation:** Organisations that choose to have more control over the user experience may do so with an added advanced installation configuration file that permits the installer to customise defaults, user interface layouts, and more than 30 other specialised user experience options.

European Data Processing

RPost (www.rpost.com) is the worldwide operator of the RMail services. Messages sent by European users are processed in the RPost Cloud in an Amazon Web Services ("AWS") secure processing facility in Frankfurt, Germany.



RPost has been operating the RMail service for millions of users worldwide for more than a decade. The underlying RPost technology has been granted more than 50 patents in 23 countries, with additional patents pending. A list of the patents that have been granted is available here: https://www.rpost.com/patents . An example of patents granted include US Patent numbers 7,966,372; 8,782,154; and 9,432,313.

CERTIFIED RMAIL PROVIDERS

The following providers are certified offerors of RMail services in Europe, each provides a unique aspect of added value.

RPost UK: RPost's UK-based team supports enterprise customers and partners in the European region. Contact RPost at www.rpost.com

Advania: Advania is a leading Nordic IT-provider serving thousands of corporate clients in the public and private sector. Ask for RMail from Advania at www.advania.com

Ingram Micro: RMail is available through the Ingram Micro Cloud marketplace in many countries.

Frama: For those looking for professional support for custom configurations, or sales and account management support with local teams and that operate in local languages in England, France, Germany, Switzerland, Netherlands, Belgium, Italy, Austria, Denmark, or India, contact Frama at www.frama-rmail.com