RPOST®

REGISTERED EMAIL™ TECHNOLOGY

AS LEGAL AND ADMISSIBLE REGISTERED ELECTRONIC DELIVERY, ELECTRONIC SIGNATURES, ELECTRONIC SEALS, AND OFFICIAL ELECTRONIC TIMESTAMPS

IN THE CONTEXT OF

eIDAS European Union Regulation No 910/2014

ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES

FOR ELECTRONIC TRANSACTIONS IN THE INTERNAL MARKET

AND REPEALING DIRECTIVE 1999/93/EC

www.rpost.com

CONCLUSION

The RPost's services built upon RPost's patented Registered Email™ technologies include services for email proof (delivery, content, official timestamp), email encryption for privacy, and electronic signatures for email, documents and contracts.

For every message transmitted, a return RMail® Registered Receipt™ email or RSign® e-signature certificate provides a verifiable, court-admissible record of the email transaction with high evidential weight – proof of precise content (message body and all attachments) and official time the email was sent and received by each recipient. Service features permit additional functions such as providing the recipient the ability to verify email authorship, original content, and original timestamp of transmission, and encrypting for data privacy. The service accomplishes this secure and certified proof of delivery without any extra recipient action or special settings or software on the recipient side.

In summary, services built upon the Registered Email™ technologies, offered inside platforms RMail®, RSign®, and RForms™ as well as under service name Registered Email™ service, return to the sender:

DELIVERY PROOF: The Registered Receipt email provides a record of sending and receiving in accordance with the Uniform Electronic Transactions Act and eIDAS European Union Regulation No 910/2014 Article 43(1), by recording the recipient's server's receipt and associating it cryptographically with the original message content, uniform timestamps, and forensic audit trail;

CONTENT PROOF: The encryption and tamper-detectability of a Registered Receipt email and Digital Seal mark preserves the contents of emails and their attachments so as to satisfy process requirements designed under the Uniform Electronic Transactions Act, eIDAS European Union Regulation No 910/2014 Articles 43(1), 35(1), and 36, and evidence law and to establish evidence of content;

OFFICIAL TIME STAMP: The Registered Email system link to a trusted, objective, and legal time source per eIDAS European Union Regulation No 910/2014 Articles 41, provides essential and credible evidence in disputes in which the time an email was sent or received is material to the case;

ADMISSIBLE EVIDENCE: Registered Receipt emails are court-admissible as to their fact of delivery, as to their legal time of delivery and as to authenticity of content; time stamp, seal, and electronic signature; per eIDAS European Union Regulation No 910/2014 Articles 25(1), 26, 35(1), 36, 41, and 43(1).

FUNCTIONAL EQUIVALENCE: Registered Email message receipts, under Electronic Signatures in Global and National Commerce Act serves as the functional equivalent of paper mail, which may be used in lieu of return receipt mail, private express mail services, fax logs and similar types of paper mail services; per eIDAS European Union Regulation No 910/2014 Articles 25(1), 26, 35(1), 36, 41, and 43(1).

ELECTRONIC ORIGINAL: A verified Registered Receipt email provides a true electronic original of the message content, message attachments, and transmission meta-data including the delivery audit trail.

ELECTRONIC SIGNATURE: The RSign electronic signature service and RMail service's handwritten, mouse-scripted electronic signature service and Digital Seal® service provide for valid electronic signatures on contracts, email, and documents as defined by eIDAS European Union Regulation No 910/2014 Articles 25(1), 26, 35(1), and 36.

ENCRYPTED FOR PRIVACY: Registered Email™ messages that are RPost encrypted comply with privacy requirements and return receipts for auditable proof of compliance.

RPost services implementation of eIDAS EUROPEAN UNION REGULATION No 910/2014, such that RPost technologies are considered to implement:

1. Advanced Electronic Signature adding legal effect as described in Articles 25(2), 25(3) by regulation.

2. Advanced Electronic Seal adding legal effect as described in Articles 35(2), 35(3) by regulation.

3. Advanced Electronic Time Stamp adding legal effect as described in Articles 41(2), 41(3) by regulation.

4. Registered Electronic Delivery Service as further described in Article 44, adding legal effect as described in Articles 43(2) by regulation.

BACKGROUND

The aspects of eIDAS European Union Regulation No 910/2014 most relevant to the Registered Email service are Articles 25(1), 26, 35(1), 36, 41, and 43(1), which are consistent with US and UK e-commerce laws and standards - - Uniform Electronic Transactions Act (UETA), Electronic Signatures in Global and National Commerce Act (ESIGN) and British Standards Institute 'Legal Admissibility' Code of Practice – BIP 0008. Two independent reviews speak to the strength and integrity of the Registered Email system from a legal perspective under US and European e-commerce laws:

• *RPost's Registered Email services and Evidence issues within the United Kingdom Legal System* by Alan Shipman, author, British Standards Institute 'Legal Admissibility' Code of Practice – BIP 0008

• *Confidential Memorandum – Legal Review of RPost Registered Email service in context of Electronic Law relative to Authentication / Admissibility Requirements* by Jon Neiditz, et al of Locke Lord Bissell & Liddell, LLP.

These opinions focus on three areas of electronic law that are most useful for users:

A. Validity and Definition of Electronic Signatures, Timestamps and Seals

B. Concept of Functional Equivalence

C. Definition of Legal Time Sent and Received by Email

[The two above cited legal opinion reference documents are available for review from RPost]

US AND EUROPEAN ELECTRONIC LAW

In the United States the enforceability of electronic transactions is governed by the Electronic Signatures in Global and National Commerce Act (ESIGN), a federal law enacted in 2000 that largely preempts inconsistent state law, and the Uniform Electronic Transactions Act (UETA), a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws in 1999. In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999 and the Electronic Commerce Directive adopted in 2000; and in 2016, European Regulation No 910/2014.

The force of these statutes is to remove barriers to the use of electronic transactions and to stipulate that electronic records and electronic signatures cannot be denied legal effectiveness solely on the ground that they are in electronic form.

ESIGN states that, notwithstanding any other rule of law, "a signature, contract, or other record relating to [a] transaction….may not be denied legal effect, validity, or enforceability solely because it is in electronic form."

UETA provides that "a record or signature, contract, or other record relating to [a] transaction…may not be denied legal effect, validity, or enforceability solely because it is in electronic form." UETA goes further, affirmatively stating that "if a law requires a record to be in writing, an electronic record satisfies the law," and "if a law requires a signature, an electronic signature satisfies the law."

The European Regulation requires member states to "ensure that an electronic signature is not denied legal effectiveness…solely on the grounds that it is in electronic form."

A. Validity and Definition of Electronic Signatures:

• See Locke Lord Bissell & Liddell LLP memo page 7, "Issues and Conclusions" #7 for a discussion of electronic signatures relative to US law. The referenced memo is available from RPost.

• See Locke Lord Bissell & Liddell LLP memo pages 16 thru 20 for a more detailed discussion of "Functional Equivalent of Electronic Signatures and Notices."

B. Concept of Functional Equivalence:

• See Alan Shipman white paper that speaks throughout to the point of functional equivalence in discussing electronic transactions. The referenced white paper is available from RPost.

• See Locke Lord Bissell & Liddell LLP memo pages 7 thru 29 with a specific reference to "Functional Equivalent of Electronic Signatures and Notices" on page 16.

C. Definition of Legal Time Sent and Received for Email:

• "Legal Delivery" means the time instance that the law notes as to when the email has been legally sent and legally received. See Alan Shipman white paper page 4 "Code of Practice Compliance Provisions" as he discusses proof of delivery.

• See Locke Lord Bissell & Liddell LLP memo page 6 "Issues and Conclusions" for reference to "sent" and "received" email under US law. Pages 10 thru 13 speak to evidence of "sending" and "receipt" of email.

EUROPEAN REGULATION NO. 910/2014

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014, we consider the following sections to be most relevant in reviewing its service capabilities for compliance and utility with regards to RPost technologies:

A. Legal Admissibility and Validity of Electronic Signatures, Timestamps and Seals

B. Definition of Legal Time Sent and Received for Email

The following are some excerpts from REGULATION (EU) No 910/2014, followed by a summary mapping RPost services to the Regulation.

Article 25: Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26: Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a)   it is uniquely linked to the signatory;

(b)   it is capable of identifying the signatory;

(c)   it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d)   it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

> ➢ **Per Article 25(1), RPost's electronic signature services, offered under on the platforms RMail, RSign, and RForms, return to both sender and signers an legal record of electronic signature that may serve as proof with high evidential weight, admissible in legal proceedings in Europe.**

> ➢ **Per Article 26, RPost's electronic signature services, offered under on the platforms RMail, RSign, and RForms, return to both sender and signers a legal record of electronic**

signature that may serve as proof with high evidential weight, admissible in legal proceedings in Europe; and may serve as an advanced electronic signature as the signature (a) is uniquely linked to the signatory; (b) is capable of identifying the signatory; (c) is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Article 35: Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36: Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

(a)   it is uniquely linked to the creator of the seal;

(b)   it is capable of identifying the creator of the seal;

(c)   it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d)   it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

> ➤ **Per Article 35(1), RPost's electronic seal services, offered under on the platforms RMail® with its Digital Seal® feature, applies a legal electronic seal that may serve as proof of sender, original content, and timestamp (for sender and recipient) with high evidential weight, admissible in legal proceedings in Europe.**

> ➤ **Per Article 36, RPost's electronic seal services, offered under on the platforms RMail® with its Digital Seal® feature, applies an advanced electronic seal that may serve as proof of sender, original content, and timestamp (for sender and recipient) with high evidential weight, admissible in legal proceedings in Europe, as the electronic seal (a) is uniquely linked to the creator of the seal; (b) is capable of identifying the creator of the seal; (c) is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.**

Article 41: Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.

2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42: Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:

(a)   it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b)   it is based on an accurate time source linked to Coordinated Universal Time; and

(c)   it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

> ➢ **Per Article 41, RPost's electronic time stamp services, offered under on the platforms RMail®, RSign, and RForms, applies a legal electronic time stamp that may serve as proof of the time of sending and receiving (for sender and recipient) with high evidential weight, admissible in legal proceedings in Europe.**

Article 43: Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

> ➢ **Per Article 43(1), RPost's electronic registered delivery services, offered under the service name "Registered Email™" and "Certified Email™", return a proof receipt by email that may serve as proof with high evidential weight, admissible in legal proceedings in Europe.**

SERVICE DEFINITIONS

Registered Email™ service: This service proves to the sender official uniform time and message content (including all attachments) an email was legally sent, legally received, with evidence that can be independently verified and can re-construct the original message and underlying Internet forensic records, all without any other party storing a copy of the content. (For clarity, RPost does not store any message content).

Digital Seal® service: This service cryptographically provides the recipient of an email with a simple means to verify and prove sender, prove original transmitted message content and attachments, and prove official uniform time of transmission analogous to a postmark.

Non-repudiation: The Registered Email™ service with the Digital Seal® service option; when used together, provide non-repudiation of sender, non-repudiation of delivery, non-repudiation of received content and attachments, and non-repudiation of times associated with receipt. When used together, you have full accountability for both parties (sender and receiver).

Registered Receipt™ email: This is the resulting evidentiary record returned to the sender when the sender sends a Registered Email message. It includes the underlying Internet forensics (server-level delivery audit trail, IP addresses, official uniform times), and uses mathematical methods and cryptography to associate the message content and attachments (back and forth) with the Internet forensics. This provides non-repudiation of delivery and non-repudiation of replies or signatures depending on the service selected. The Registered Receipt, at any time, can be independently (third-party) authenticated and if validated, will reconstruct the electronic originals – original message text, attachments, and Internet forensic records all in native format.

Receipt Authentication™: This Registered Receipt™ record is portable so that, in a dispute resolution situation, the Receipt can be forwarded by email to any opposing party, counsel, arbitrator, mediator or judicial officer, and that party can, independent of any cooperation or complexity, simply forward the Receipt to an RPost verify email address to have the Receipt authenticated with original content returned to the party requesting authentication. The Receipt authentication process provides a true electronic original of the message content, message attachments and transmission meta-data including the delivery audit trail. The form in which RPost packages this Registered Receipt email is such that the RPost system does not store any information (yet the Receipt can re-construct the electronic original content when authenticated). RPost is Safe Harbor Certified.

RMail® and RSign® E-Signatures: These services electronically apply the recipient or multiparty recipients' handwritten (mouse scripted) signatures to a contract. The recipient can, in their web browser and with a few mouse-strokes, handwrite a mouse-scripted signature that becomes electronically sealed to the contract. The end result (the signed-off contract) has the precise look of a traditional pen-and-ink signature on a contract, with the added benefits of RPost's Registered Receipt forensics for future authentication. This service records the message content, time of delivery, and permits the recipient to click in the email body as an indication of acceptance; then packages a PKI digitally signed PDF record with a watermark seal and timestamp on each page, recording the content of any attached agreements and the correspondence in the message body. This record, returned to the

sender as a PDF, may be used for workflow purposes and can be independently verified for non-repudiation of agreement between parties. This version of the RPost service provides a verifiable record with high evidential weight, of the recipient's handwritten signature on a set of terms attached to an email or in the body of an email. Here, the biometric signature can be forensically identifiable to an individual who is signing in the same manner a handwriting expert might do for a pen-and-ink signature on paper. One may view this resulting signature on "electronic paper" or a PDF, no different in terms of legal standing as pen-and-ink signature on paper that is then transmitted by fax, or a pen-and-ink signature on paper that is then scanned and stored as a PDF record.