



Additional Terms and Conditions QREMS

Versie: 1.2
Status: Final

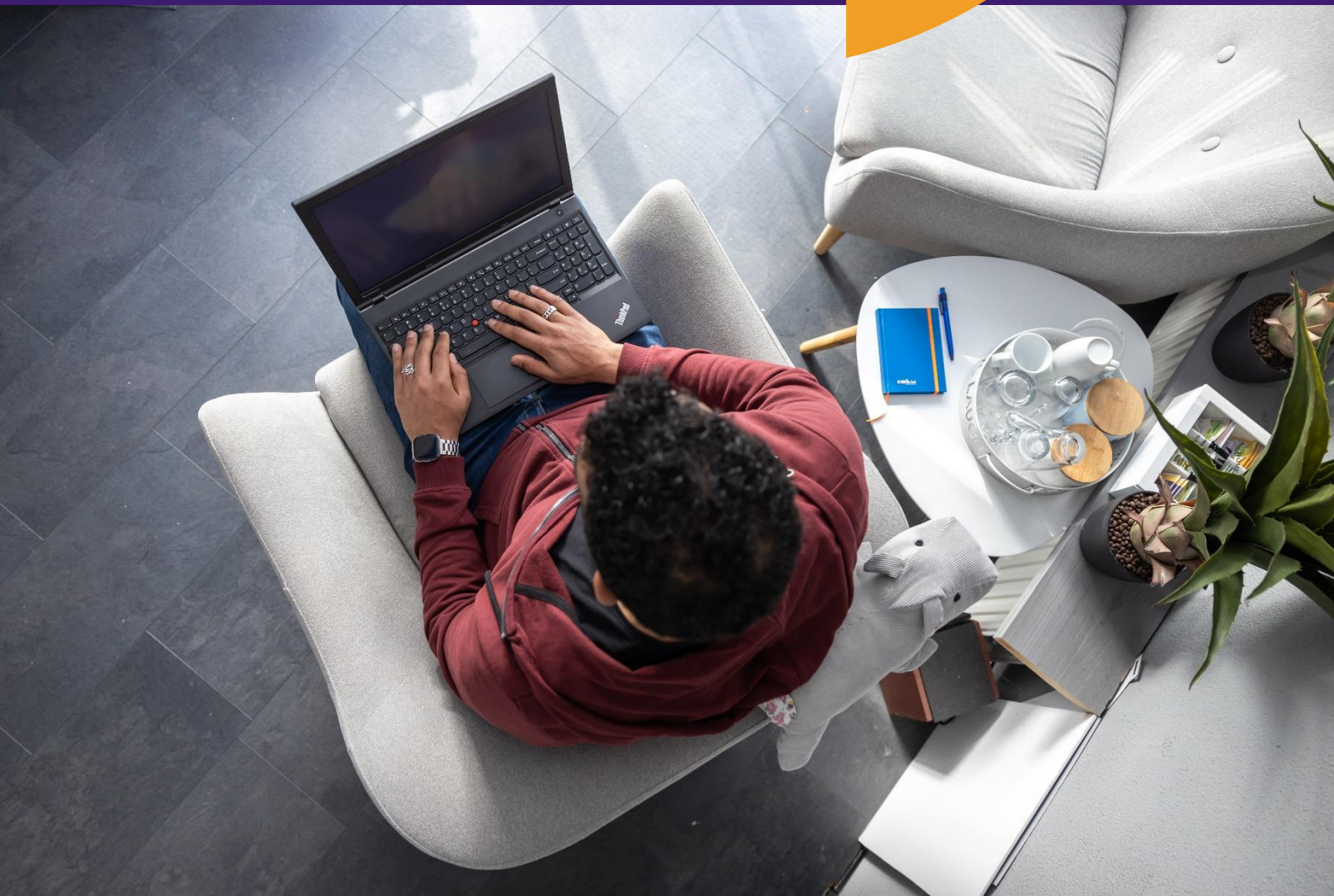


Table of Contents

1. Overview.....	3
1.1 Document name and identifier	3
2. Qualified Registered Email	3
2.1 Qualified registered electronic mail service.....	3
2.1.1 Successful delivery of electronic content.....	4
2.1.2 Protection	4
2.1.3 Availability	4
3. SecuMailer Obligations.....	4
4. Subscriber Responsibility.....	5
5. Amendment and Termination	5
5.1 Amendment of the additional terms and conditions.....	5
6. Policies and practices applicable.....	6
7. Accessibility. Logs. Audit/conformity assessment	6
7.1 Conformity Assessment.....	6
7.2 Availability	6
7.3 Logs.....	6
8. Publication of Information	7

1. Overview

These additional terms and conditions apply to the use of the QREMS service that SecuMailer provides.

1.1 Document name and identifier

The full name of this document is “SecuMailer QREMS Terms & Conditions”. The identifier for the document is:

Name	Object Identifier (OID)
SecuMailer QREMS Terms & Conditions	1.3.6.1.4.1.60954.2.1

SecuMailer ensures that it does not alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents, in any circumstances. SecuMailer follows an internal OID management procedure.

2. Qualified Registered Email

The Qualified Registered Email is a trust service allowing the transmission of data between third parties electronically and provides evidence with respect to the identity of the sender and the recipient of the transmitted data, the time of sending and receiving the data and protects the transmitted data against the risk of loss, theft, damage or unauthorized changes.

The service provides:

1. a high level of trust as regards the sender’s identification;
2. the sender’s identification before the delivery of the data;
3. The sending and receiving of data is secured through an advanced electronic signature or an advanced electronic seal of SecuMailer in a way excluding all possibilities for unnoticed change of the data;
4. Each data change necessary for the purpose of sending or receiving the data is clearly marked for the sender and for the recipient of the data;
5. The date and time of sending and receiving as well as any change of the data are indicated by a Qualified Electronic Time-Stamp.

When providing this service, SecuMailer creates, signs with an advanced electronic seal and gives to the sender proof (electronic advice of delivery) regarding the facts of the sending, receiving and integrity of the content transmitted.

This trust service of SecuMailer is provided in accordance with Art. 44 of Regulation (EU) № 910/2014.

The proof of the messages transmitted may be stored for the duration of the contract in SecuMailer’s repository.

2.1 Qualified registered electronic mail service

This service is provided by SecuMailer in accordance with Art. 44 of Regulation (EU) № 910/2014 and relies on technology that enables the delivery of qualified registered electronic mail via a specialized

electronic mail server (SMTP) and is accessible through standard mail clients such as Mozilla Thunderbird , etc., as well as through the web based Email application.

Specific requirements for the provision of a qualified electronic registered delivery service:

2.1.1 Successful delivery of electronic content

1. A successful delivery shall be considered to have taken place where the content sent by the sender has left the information system of the sender and is no longer under its control.
2. A delivery shall be considered to have been served where the content sent by the sender has successfully entered the information system of the recipient.
3. When using API integration, successful sending shall be considered the receipt of the electronic message on the SecuMailer backend (server) through the built API interface, and successful delivery shall be considered the receipt of the sent electronic content in the information system of the recipient through such interface.
4. When using a web-based portal, successful sending shall be considered the receipt of the electronic message from the web browser of the Subscriber using the portal on the SecuMailer backend (server), and successful delivery shall be considered when the content sent by the sender has successfully entered the information system of the recipient.
5. When using the qualified REM service, successful sending shall be considered the time of receipt of the electronic message in the information system on the SecuMailer electronic mail server (backend), and receipt shall be considered when the content sent by the sender has successfully entered the information system of the recipient.

2.1.2 Protection

SecuMailer makes sure that the service protects the electronic content being transmitted against loss, theft, breach of integrity or unauthorized alteration and meets the requirements of Regulation (EU) № 910/2014.

2.1.3 Availability

The period of time during which the sent electronic content is available and the electronic registered mail system is making attempts to is 12 hours.

3. SecuMailer Obligations

The obligations of SecuMailer shall include:

- to carry out external audits at least every year by independent auditors in order to verify the compliance of the trust service with the requirements of Regulation (EU) № 910/2014 and the applied policy.

SecuMailer warrants that it operates by:

1. strictly observing the terms and conditions referred to in this document, the requirements of Regulation (EU) № 910/2014, REGULATION (EU) 2016/679 and the applicable law in carrying out its activities as a qualified registered Email service provider;
2. its provided services not infringing any third party copyrights and license rights;

3. using technical equipment and technologies that ensure the reliability of the systems and the technical and cryptographic security in the implementation of the processes, including a secure and protected mechanism/device for the generation of keys and for the creation of an electronic signature/seal in its infrastructure;
4. observing the established operating procedures and rules for technical and physical control, in accordance with the terms and conditions in the Practice and Policy in the provision of qualified trust services;
5. providing conditions for the precise determination of the time of issuance, cancellation, renewal and revocation of the certificates;
6. performing procedures of identification and establishment of the authenticity of the Sender/Recipient;
7. using reliable cryptographic keys storage and management systems;
8. allowing only duly authorized employees to have access for the purpose of making changes in the data, establishing the authenticity and validity of the cryptographic keys;
9. taking immediate measures in case of any technical problems related to security;
10. using and storing the collected personal and other information only for the purposes of its activity of providing trust services in accordance with the applicable law;
11. keeping available funds which enable it to carry out its activities;
12. entering into an insurance for the time of its activities;
13. maintaining trusted personnel having the necessary expertise, experience and qualifications for carrying out the activities;
14. publishing in its website other circumstances and electronic documents, according to this document and the applicable law;
15. performing external audits by independent auditors and publishing on its website the results of such audits;
16. using in its activities trusted software and hardware, as well as secure and reliable technological systems;

4. Subscriber Responsibility

The Subscriber's responsibilities shall include:

1. The Subscriber shall be responsible for fulfilling the obligations provided for in these Additional Terms and Conditions.
2. The Subscriber shall be solely responsible for the used means of identification, as well as for any use by third parties allowed by it. The Subscriber shall be solely responsible for the protection of its devices with access to SecuMailer applications or any use thereof allowed by it;
3. The Subscriber shall cooperate with an annual check if all eIDAS obligations are still compliant.

5. Amendment and Termination

5.1 Amendment of the additional terms and conditions

SecuMailer allows amendments to these Terms and Conditions in the following cases:

1. SecuMailer may unilaterally amend these Terms and Conditions, notifying the Subscriber of any amendment in accordance with the requirements of the law;
2. Where it does not agree with the amendments, the Subscriber may withdraw from the contract without stating any reason therefor and without owing any compensation or penalty. In such case, the contract shall be automatically terminated upon receipt by SecuMailer of the Subscriber's notice under item 6.1 (c), unless SecuMailer has explicitly indicated the possibility to continue using the Services under these terms and conditions applicable before the amendment. This rule shall not apply in cases where the amendment to the terms of these Terms and Conditions is due to an order or instruction of a competent authority;
3. The Subscriber may exercise its right under item 6.1 (b) by a respective statement addressed to SecuMailer within one month from the notice under item 6.1 (a). If within the said period the Subscriber does not declare that it does not agree with the amendments, it will be deemed to be bound by them.

6. Policies and practices applicable

In accordance with the requirements of Regulation (EU) № 910/2014, SecuMailer includes in its digital signature an object identifier (OID)/link (URI), through which Subscribers are able to check the SecuMailer Policies and Practices applicable to the provision of the trust service related to the issued certificate.

The Policies and Practices applicable to the trust service provided by SecuMailer are publicly accessible on the website of SecuMailer: <https://www.secumailer.nl/eidas/>. Each version of the Practice for providing a qualified trust service will be applied until the approval and publication of a new version. The Subscribers and Relying Parties shall be obliged to get acquainted in advance with and to comply only with the valid version of the Policies and Practices applicable at the time of using the SecuMailer services.

7. Accessibility. Logs. Audit/conformity assessment

7.1 Conformity Assessment

SecuMailer is audited at least once every year by a conformity assessment body accredited by the European Commission. The purpose of the audit is to confirm that SecuMailer, as a qualified trust service provider, and the qualified trust services it provides, meet the requirements set out in EU Regulation № 910/2014.

7.2 Availability

SecuMailer ensures that the availability of the service is in accordance with the terms and conditions described in its Policies and Practices and in these Terms and Conditions. SecuMailer provides uninterrupted access (24/7/365) to the service, with the exception of technical maintenance time.

7.3 Logs

SecuMailer stores in logs events that are needed as evidence. SecuMailer collects the following information:

ETSI Evidence logs: These are a set of chronological records related to security that provide documentary evidence of the sequence of activities that affected an operation, procedure or event. There logs also contain the evidence of the integrity of the e-mail send. These records are kept for at least 7 (seven) years;

SecuMailer records the exact time of events important for the activity management, such as key management, clock synchronization, events related to identification of persons, issuance of certificates and others. Events are recorded in a way that cannot be easily deleted or destroyed, unless they are reliably transferred to long-term backups within the period in which they must be kept.

8. Publication of Information

SecuMailer publishes the following information on its website: <https://www.SecuMailer.com>:

- These terms and conditions
- Policies and Practices for provided Qualified Registered Email Service.