Terms and Conditions of Providing the Qualified Electronic Registered Delivery Service

Velika Gorica, November 2025.

Change history

Version	Date	Made by	Change description:
1.0	01.10.2021.	Igor Ivaštanin	Initial version
1.1	01.01.2022.	Igor Ivaštanin	Added additional clarifications on service provision
1.2	15.12.2023.	Marina Zečević	Change of the head office
1.3	11.11.2025.	Marina Zečević	Change of organization responsible

1. General provisions

These Terms and Conditions of Providing the Qualified Electronic Registered Delivery Service (hereinafter referred to as the Terms and Conditions of Service Provision or these Terms and Conditions) define the relationships between HP - Hrvatska pošta d.d. (hereinafter referred to as HP d.d.), having its registered office at Poštanska 9, Velika Gorica, VAT No.: 87311810356, registered in the Registry of the Commercial Court in Zagreb under Reg. No. (MBS): 080266264, as the service provider, on the one hand (hereinafter referred to as the Service Provider), and a natural or legal person using the trust service, as the user, on the other hand (hereinafter referred to as the User).

These Terms and Conditions supplement the General Terms and Conditions of Using the ePost Service and apply to the provision of the Qualified Electronic Registered Delivery Service (hereinafter referred to as the QERDS).

Details of the QERDS are available in the Qualified Electronic Registered Delivery Service Provision Policy and the Rules of Conduct for the Provision of the Qualified Electronic Registered Delivery Service (hereinafter referred to as the Policy and Rules of Conduct), as well as other documents publicly available at https://www.eposta.hr/info.

2. Contact details

Information about the provision of the service is available at ePreporuka@posta.hr or:

HP - Hrvatska pošta d.d.
Product Management
Poštanska 9
10410 Velika Gorica

3. Service Provider's obligations

The Service Provider is a qualified trust service provider providing the service in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("electronic IDentification, Authentication and trust Services", hereinafter referred to as the eIDAS Regulation), the applicable eIDAS Regulation Implementing Act, as well as the relevant subordinate legislation and normative documents.

The Service Provider shall ensure that each item (including user content and metadata) remains available, integral and confidential at all times while providing the QERDS, by:

- proper identification of the user at the time of arranging the service;
- reliable authentication of the sender and the recipient when accessing the QERDS;
- proper personal data protection;
- conducting internal and external conformity audits; and
- complying with all prescribed obligations.

Electronic documents are protected using an electronic signature/seal, supported by a certificate issued at least under the ETSI 319 411-1 NCP policy by a qualified trust service provider and generated in a way that makes it impossible to alter data undetectably.

Key lengths and algorithms used in the QERDS provision system:

- HP QERDS – key length = 2048 bits, algorithm=sha256WithRSA

The validity period of HP QERDS certificates for the advanced or qualified electronic seal and the key pair is 2 years.

The QERDS provider uses cryptographic devices defined in FIPS PUB 140-2, level 3 and/or CC EAL 4+, to store private keys.

In providing QERDS service HP d.d. uses services from another qualified trust service provider listed in Appendix I of Practice Statement for Qualified Electronic Registered Delivery Service available on https://www.eposta.hr/info.

4. Proof of service

The Service Provider collects proof of all critical events in the course of using the QERDS. Users may access such QERDS proof by using the QERDS app based on their role (sender/recipient) and the type of item being sent.

Critical events:

- submission – proof is stored after the Service Provider accepts an item submitted to it;
- consignment – proof is stored after the Service Provider delivers the item to the recipient's mailbox;
- handover – proof is stored after reliable authentication of the recipient and after the item is handed over or rejected via the QERDS app by the recipient.

The recipient shall be notified of each item via the selected notification channel. Such notification must indicate the message availability time.

If the User accesses the QERDS app within the time allowed and the item is handed over to the User, a "Successful Handover" event will be created. Depending on the type of item, it is possible to specifically reject handover and this event will be identified as "Handover Rejected".

If the User does not access the QERDS app or does not accept/reject handover, a "Handover Time Expired" event will be created.

Archived QERDS proof must be retained for 10 years and after that they are not available.

5. User's obligations

The User(s) shall:

- provide accurate and complete particulars in the service request;
- accept the Terms and Conditions of Providing the Service and other related documents;
- protect the authentication elements against loss, theft, corruption or unauthorized use;
- report to the Service Provider any event that compromises the security of authentication elements or any suspicion of such event;
- refrain from taking advantage of any security defects or irregularities in the operation of Service Provider's system and report them to the Service Provider immediately upon becoming aware of them;
- refrain from delegating its qualified electronic registered delivery service responsibilities to third parties; and
- use the service in a lawful manner, in accordance with its permitted purpose and in compliance with applicable regulations.

6. Relying parties' obligations

Reasonable reliance on the QERDS for a relying party shall be deemed achieved if such relying party, at the time of its use:

- takes the necessary preventive security measures;
- verifies Service Provider's advanced or qualified electronic seal and qualified electronic time stamp by using authentic systems; and
- uses reliable applications in a secure IT environment.
-

Where a relying party acts in violation of these requirements, such relying party shall bear the risk of relying on Service Provider's advanced or qualified electronic seal and qualified electronic time stamp.

All changes that may affect provision of QERDS service, relying party is obliged to inform HP d.d.

7. Limitation of service providing

Limitations of providing QERDS service are:
a) as the QERDS service is part of ePošta service, prior to register the use of QERDS service, user is obliged to register to ePošta service in accordance to ePošta Terms and Conditions. By registering to ePošta service, the user will receive a username and password with which he accesses the service, which is a prerequisite for access to the QERDS service.
b) the user may register the use of QERDS service by remote electronic registration in the manner prescribed in item 3.1. of Certificate Policy for Qualified Electronic Registered Delivery Service, using a digital signature supported by a personal certificate issued by the Agencija za komercijalnu djelatnost proizvodno, uslužno i trgovačko d.o.o, OIB: 58843087891.

In addition to remote electronic registration, the QERDS user can register to service at any post office.

8. Limitation of liability

The Service Provider has sufficient funds available and carries appropriate liability insurance necessary to provide the QERDS.

The Service Provider shall not be liable for any damage, including indirect damages, loss of revenue, loss of data or any other damages associated with qualified trust services, resulting from the use of QERDS provided by other service providers or the use of Service Provider's QERDS in violation of the Certificate Policy and Practice Statement.

Details of Limitation of Liability are available in the Certificate Policy and Practice Statement at https://www.eposta.hr/info

9. Policy and other relevant documents

All documents relevant to the provision of qualified trust services are available in the Service Provider's public repository at https://www.eposta.hr/info

10. Personal data protection

The Service Provider has adopted personal data protection measures in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

The Service Provider is responsible for protecting personal data processed in the course of providing qualified trust services as defined in the General Terms and Conditions of Using the ePost Service.

11. Service availability

QERDS service is, in general, available 24 hours each day in a year. Service Provider cannot guaranty availability if the system outage or infrastructure malfunction is out of the Service provider´s control or jurisdiction or if circumstances have arisen that can be described as *force majeure*.

Service Provider has the right to announce the unavailability of the QERDS service in the event of regular system maintenance.

12. Price of service

The use of the QERDS is subject to the rates defined in Service Provider's applicable pricelist.

13. Complaints

The User may submit to the Service Provider a complaint about the provision of the QERDS and the Service Provider shall respond to such complaint within 15 days. Such complaints are submitted and

the relevant procedure is conducted as defined in the General Terms and Conditions of Using the ePost Service.

The resolution of any dispute shall be governed by the applicable legislation of the Republic of Croatia. The Service Provider and the User shall endeavor to amicably resolve any such dispute and shall otherwise submit to the jurisdiction of the competent court in Zagreb.

14. Trust designations for the Service Provider

The central public administration authority of the Republic of Croatia responsible for economic affairs supervises the implementation of the eIDAS Regulation with regard to its provisions for trust services. Compliance with the eIDAS Regulation is audited and verified by an independent accredited conformity assessment body.

Audits with regard to the processing, use and protection of personal data may also be conducted by further public and other authorities defined in the relevant personal data protection laws and regulations.

As a qualified trust service provider, the Service Provider appears on the EU Trusted List, which demonstrates its compliance with the applicable legislation and standards.

15. Effective date; Applicability

These Terms and Conditions shall enter into force on the day of its adoption and shall apply as of November 11. 2025.

Class: 025-02/25-06/20
No.: HP-03-02-25-5

HP-Hrvatska pošta d.d. (Croatian Post)
Chairman of the Bord

Ivan Čulo