Qualified Electronic Registered Delivery Service Provision Policy

Velika Gorica, December 2023

Document information

Document name	Qualified Electronic Registered Delivery Service Provision Policy
Document version	1.2
Document status	Valid
Date of adoption	15.12.2023.
OID	**1.3.6.1.4.1.54777.1.1.1**
Document type	CP
Document classification	Public
Owner	HP-Hrvatska pošta d.d., Poštanska 9, 10410 Velika Gorica PIN: 87311810356, MBS: 080266264 (Commercial Court in Zagreb)
Contact	Optimization Office, Poštanska 9, 10410 Velika Gorica ePreporuka@posta.hr
Document location	https://www.eposta.hr/info
Related CPS	Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service OID: **1.3.6.1.4.1.54777.1.1.2**

Revision history

Version	Date	Prepared by	Description of amendment
1.0	01.10.2021.	Igor Ivaštanin	Initial version
1.1.	01.01.2022.	Igor Ivaštanin	Additional clarifications made to the terms of providing the service
1.2	15.12.2023.	Marina Zečević	Change of the organization in charge of administration of the Policy

1. Introduction

The document "Qualified Electronic Registered Delivery Service Provision Policy" (hereinafter: Policy) prescribes the terms which HP – Hrvatska pošta d.d., with its registered seat of office in Velika Gorica, Poštanska 9, PIN: 87311810356, registered with the Commercial Court in Zagreb, MBS: 080266264, (hereinafter: HP d.d.) applies when providing qualified electronic registered delivery service, pursuant to the 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: the eIDAS Regulation), the Act on Implementation of eIDAS Regulation, and by-laws and standardisation documents ETSI EN 319 401, ETSI EN 319 521 and ETSI EN 319 522.

HP d.d. has implemented the infrastructure for the provision of qualified electronic registered delivery service (hereinafter: QERDS) for its customers.

Qualified electronic time stamp used by HP d.d. when providing the service is outsourced from another qualified trust service provider who is on the EU Trusted List and it indicates the date and time of sending, receiving messages and possible changes of data.

HP d.d. uses an advanced or qualified electronic seal for sealing electronic registered delivery messages when sending and receiving messages, based on an electronic certificate (at least pursuant to the NCP policy) issued by a qualified trust service provider which excludes the possibility of undetectable change of data.

Qualified electronic time stamp and at least an advanced electronic seal will ensure the integrity of the data and the authenticity of the data source.

This Policy refers to the entire HP d.d. infrastructure used to provide QERDS. The provisions of the Policy apply to all participants in the system for the provision of QERDS, including inter alia, HP d.d. as the service provider, customers, and relying parties.

The structure of this document follows the standardisation document ETSI EN 319 411-1 V1.2.2. (2021-05), to the extent applicable to the provision of QERDS.

A more detailed elaboration of the provisions of the Policy and the appropriate procedures for their application are prescribed in the document "Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service" (hereinafter: Rules of Procedure).

The policy will be published on website of HP d.d. at: https://www.eposta.hr/info

1.1. Reference documentation

Basic regulations

- 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

- Act on Implementation of the 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 (OG 62/2017)
- 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)
- Act on Implementation of the General Data Protection Regulation (OG 42/18)

Subordinate Regulations

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22 (5) of Regulation (EU) no. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) no. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27 (5) and 37 (5) of Regulation (EU) no. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- Regulation on the Provision and Use of Trust Services (OG 60/2019)

Standardisation documents

- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management
- ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management
- ETSI EN 319 102-1 V1.1.1. (2016-05) – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 401 V2.2.1. (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2. (2021-05) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2. (2021-05) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU Qualified Certificates

- ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

1.2. Identification data and OID code

Document name: Qualified Electronic Registered Delivery Service Provision Policy
Version: 1.2
Date: 15-12-2023
Document link: https://www.eposta.hr/info

Unique OID (Object Identifier) **1.3.6.1.4.1.54777** is assigned to HP d.d. Based on it, HP d.d. assigns **1.3.6.1.4.1.54777.1.1.1** for this Policy.

Method of assigning the OID and clarification of digits after the unique OID:

- first digit: 1 – documentation,
- second digit: 1 – umbrella documentation,
- third digit: 1-CP, 2-CPS.

1.3. Subjects and scope of provision of service

Qualified electronic registered delivery service provider
HP d.d. provides QERDS using the qualified time stamp and advanced/qualified electronic seal to protect the integrity of user content and QERDS evidence and to link them with the correct time.

Users
QERDS users are natural and legal persons who, when contracting QERDS, accept the Terms of Qualified Electronic Registered Delivery Service and other related documents relevant for the performance of the service. QERDS users can be recipients and senders of user content.

Relying parties
Relying parties in QERDS are external service providers, business entities in a business relationship with HP d.d. who accept QERDS evidence but are not users. Relying parties must check the advanced/qualified electronic seal, qualified electronic time stamp and certificates as well as the corresponding list of revoked certificates, or use the OCSP service to verify the certificates used by HP d.d. before accepting the information contained in the QERDS evidence.

Other participants
Other participants of the system for the provision of QERDS are legal persons which do not provide and do not use qualified trust services, but participate in parts of the process related to the provision of qualified trust services. This group of system participants includes manufacturers and distributors of hardware and software used in the QERDS system, manufacturers and distributors of HSMs and other cryptographic devices, independent evaluators, etc.

1.4. Administration of the Policy

1.4.1. Organization in charge of the administration of the Policy

Organization competent for administration of the Qualified Electronic Registered Delivery Service Provision Policy:

HP-Hrvatska pošta d.d.
Optimization Office
Poštanska 9
10410 Velika Gorica
Republic of Croatia
email: ePreporuka@posta.hr

1.4.2. Policy Adoption Procedure

Each version of the Policy is in force until the new version of the Policy enters into force.

The initiative for adoption and the initiative for amendments to the Policy is given by the Office for Strategy and Development, whereas the announcement of the amendments and the amended Policy will be available in the public repository of HP d.d.

The responsible persons of HP d.d. are competent for the adoption of the Policy and amendments to the said Policy.

1.5. Definitions and abbreviations

1.5.1. Definitions

Electronic Registered Delivery Service App	A system consisting of hardware and/or software, which allows the sender and recipient to participate in data exchange with the electronic registered delivery service provider
Evidence of electronic registered delivery service	Data generated within the electronic registered delivery system, proving that a specific event in the system occurred at a specific time
Consignment	The electronic registered delivery service provider has delivered user content within the recipient's eBox QERDS defined by the General Terms of Use of the ePost Service.
Public key	A cryptographic key of a user which is publicly available, and which together with a private key enables digital signature verification or data encryption
Coordinated Universal Time (UTC)	Second-based time scale as defined by ITU-R Recommendation TF.460-5. For most practical applications, UTC is equivalent to the mean solar time at the zero meridian (0°). More accurately, UTC is a trade-off between very stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular rotation

	of the Earth (relative to the agreed Greenwich Mean Sidereal Time - GMST).
User Content	Original data produced by the sender, to be delivered to the recipient.
User	User as defined in the General Terms of Use of the ePost Service, that uses trust services.
Qualified Electronic Signature Certificate	A certificate for electronic signatures issued by a qualified trust service provider that meets the requirements set out in Annex I of the eIDAS Regulation.
Qualified Electronic Time Stamp	An electronic time stamp that meets the following requirements: (a) it connects 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 an equivalent method.
Qualified Trust Service Provider	A trust service provider that provides one or more qualified trust services and has granted the qualified status by the supervisory body.
Qualified Electronic Registered Delivery Service Provider	Trust service provider providing qualified electronic registered delivery service.
Qualified Electronic Registered Delivery Service	Electronic registered delivery service that meets the requirements set out in Article 44 of the eIDAS Regulation
Cryptographic module	An element of the certification system that has the function of generating and/or storing keys during cryptographic operations (*Hardware Security Module*).
List of qualified service providers	Trusted List of certification service providers supervised/accredited by EU Member States
List of revoked certificates	List of revoked or suspended certificates, whose availability must be ensured to relying parties or other persons or systems (*Certificate Revocation List*).
Advanced Electronic Signature	Electronic signature which reliably guarantees the identity of the user and which: ▪ is uniquely linked to the user; ▪ unequivocally identifies the user; ▪ is created using data that the user can solely control and that is exclusively under the supervision of the user;

	▪ contains a direct link to the data to which it relates in a way that unequivocally allows review of any modification of the original data.
Certificate revocation	Procedure for suspending the validity of certificates before their regular expiration.
Relying Party	A natural or legal person relying on electronic identification or a trust service.
Trusted roles	Roles that are assigned to employees and on which the safety of certification service provider's work depends. Trusted roles and related responsibilities must be clearly defined and described in the employee's job description
Shipment	Structured data in electronic form prepared by the sender and intended for electronic registered delivery, consisting of user content and metadata (name of the recipient, address of the recipient, etc.).
Sender	A user sending the user content.
Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service	Rules of procedure for the provision of electronic registered delivery services in accordance with the requirements of the eIDAS Regulation.
Recipient	A natural or legal person to whom the user content is addressed.
Private key	A cryptographic key of a user that is known only to the user, and together with the public key enables the creation of a digital signature or decryption of data.
Electronic Registered Delivery Service Provider	HP d.d. or another trust service provider, which provides an electronic registered delivery service
Conformity assessment body	A body authorised by applicable regulation as competent to carry out the conformity assessment of a qualified trust service provider and the qualified trust services provided by such provider.
Handover	After the trusted authentication of the recipient, the user content is downloaded or rejected by the recipient through the QERDS application, or the scheduled deadline for delivery has expired regardless of the authentication of the recipient.
Signature validation	The process of verification and confirmation that the electronic signature is valid.
Signature verification	The process of verifying the cryptographic value of a signature using signature verification data.
Electronic Registered Delivery Service	An electronic service, which allows the transmission of data/shipment between the sender and the recipient, while securing evidence of sending and receiving of data and protection measures to reduce the risk of loss, theft, destruction or unauthorized change of data.

1.6.2. Abbreviations

ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
NCP	Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID.	Object Identifier
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature Creation Device
TLS	Transport Layer Security
TSP	Trust Service Provider

2. Responsibility for disclosure of information and repositories

The QERDS Provision System Repository is maintained by HP d.d. as a qualified trust service provider who is responsible for the documents and information therein. The repository is publicly available and contains:

- public key and certificate, which HP d.d. uses for advanced/qualified electronic seal of the user content and QERDS evidence and
- documents for QERDS.

The repository is available at: https://www.eposta.hr/info

3. Identification and verification of identity

3.1. User identification and authentication

Identification of a natural person when contracting QERDS delivery will be performed in the following ways:

1) personally, with the operator at the post office by presenting the identity card or passport.
2) by remote electronic registration with digital signature supported by a personal certificate accepted by HP, issued pursuant to the policies ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-n or QCP-n-qscd.

Citizens of the Republic of Croatia are identified by an identity card, while foreign persons are identified exclusively by a passport.

Identification of a legal person or a natural person who is the registered business operator when contracting QERDS will be performed in the following ways:

1) Personally by the authorized representative of the legal person or by the natural person who is the registered business operator, with the sales representative, by presenting the identity card

and by collecting and verifying data on the legal person or the registered business (full name and legal status, proof of existence and proof of the authorized representative, e.g. from the competent register (by bringing an extract or printout of an electronic record from the register and/or online inquiry into the register). In case an attorney contracts a service for a legal person or for a registered business operator, it is also necessary to obtain power of attorney, which is enclosed to the contract itself and on which the signature of the authorized representative of the legal person must be notarized.

2) By remote electronic registration, using digital signature supported by a business certificate issued pursuant to the policies ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-l or QCP-l-qscd.

After successful identification, the collected data is used to register users for QERDS. By registration, the user is assigned with a secure electronic mailbox address (eBox QERDS). Upon completion of the registration, the user can use a qualified electronic registered delivery service.

A registered user cannot open an additional user account that would contain his personal data and will be warned about it by the system or the operator at the post office.
The described methods of user identification are also carried out in case of loss, damage or suspicion of compromise of authentication elements.
The authentication of a natural person and/or a legal person when logging into the system for a qualified service is carried out by two-factor authentication (username, password and OTP one-time password submitted via the ePost mobile application or via SMS).

Trusted authentication must be used when using the mobile application to access the qualified electronic registered delivery service. The users log into it with their PIN numbers, which in addition to possessing a mobile device, which is proven by the ePost mobile application that is securely connected to the mobile device, constitutes a 2-factor authentication.

4. Operational management of the service

HP d.d., as a qualified trust service provider, provides the service in accordance with the eIDAS Regulation, the Act on Implementation of the eIDAS Regulation, and standardisation documents, and ensures availability, integrity and confidentiality of user content and metadata, during transmission and storage.
Electronic documents are protected by an electronic signature/seal, supported certificate issued pursuant at least ETSI 319 411-1 NCP policy by a qualified trust service provider (QTSP), generated in such a way as to prevent undetectable change of data.

HP d.d. checks the correctness of the electronic seal and time stamp and the qualification of the QTSP (EU Trust List) by periodically reviewing whether the service provider of qualified certification and issuance of time stamps is on the EU Trust List. This qualification check is carried out by inquiry on the EU Trust List. Reviews of the electronic signature and seal as well as of the qualified electronic time stamp are carried out in accordance with ETSI EN 319 102.
QERDS supports the signing of shipments in two ways:

a) delegated scenario – signature is executed by the service provider,
b) additional security scenario – signature executed by the sender.

The system provides QERDS evidence of submission of the shipment, and of consignment and handover of the shipment. QERDS evidence is protected by an advanced/qualified electronic seal, supported by a certificate issued under at least ETSI 319 411-1 NCP policy and a qualified electronic time stamp (PAdES Baseline level LT or LTA) generated by a qualified trust service provider (QTSP) and is kept for 10 (ten) years.

5. Equipment and premises protection measures, organizational security measures and supervision of employees' work

Protection measures implemented by HP d.d. are:

- defining and assigning trust roles for QERDS,
- supervision of employees' work,
- asset management,
- access control,
- cryptographic controls,
- physical protection of equipment and premises,
- operations protection,
- online safety,
- incident management,
- collection of audit records,
- business continuity management and
- defined actions in the event of termination of the service.

Equipment and premises protection measures, organizational security measures and supervision of employees' work are described in detail in the Rules of Procedure.

6. Technical security measures of the QERDS provision system

A pair of keys for the electronic seal is generated in the protected zone on the cryptographic device, with at least double control by authorized persons.

The key lengths and algorithms used in the QERDS provision system are:

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

The validity period of the HP QERDS advanced/qualified electronic seal and key pair certificate is two (2) years.
Cryptographic devices in accordance with FIPS PUB 140-2, level 3 and/or CC EAL 4+ are used to store private keys.

The private keys for advanced/qualified electronic seal stored on the cryptographic module are activated after the ePost application system is launched on HP d.d. servers. Reliable authentication regarding cryptographic modules is required for activation. The private keys for advanced/qualified electronic seal are deactivated by stopping the operation of the ePost system.

The qualified electronic time stamp used by HP d.d. when providing the service is outsourced from another qualified trust service provider (on the EU Trusted List).
Other technical security measures of the QERDS provision system are described in detail in the Rules of Procedure.

7. Certificate profiles and revoked certificate lists

The qualified electronic seal of HP d.d. used when providing QERDS, is supported by a qualified certificate in accordance with ETSI 319 411-2 QCP-l-qscd policy issued by a qualified trust service provider (QTSP) and prevents undetectable change of data.

The field "Subject" within the certificate contains the full name of the QERDS provider – HP d.d.

The path to the list of revoked certificates and the OCSP services for reviewing the status of the certificate of a qualified trust service provider who has issued a certificate for HP d.d., is located within the certificates in the fields "CRL Distribution Points" and "Authority Information Access".

8. Compliance audit and other reviews

Supervision of the provision of qualified trust services within the scope of these Rules of Procedure is carried out by the competent national authority (Ministry of Economy and Sustainable Development) in accordance with provisions of the eIDAS Regulation, implementing acts adopted on the basis thereof and the Act on Implementation of the eIDAS Regulation. External compliance reviews shall be carried out at least every 2 (two) years in accordance with the eIDAS Regulation. Regular monitoring of the information security management system to verify compliance with ISO/IEC 27001 shall be carried out at least every 12 (twelve) months.
Internal compliance reviews are carried out periodically at least once a year, before the provision of new qualified trust services, and after significant changes in the system for the provision of QERDS.

The compliance assessment includes evaluation of the following areas of providing qualified trust services:

- completeness and accuracy of documentation;
- implementation of requirements for qualified trust services;
- organizational processes and procedures;
- technical processes and procedures;
- implemented information security measures;
- trustworthy systems;
- physical security of the sites in question.

The description of the said evaluation of the compliance is defined in the compliance evaluation plan.

9. Other financial and legal matters

9.1. Service fee

The use of QERDS is charged in accordance with the applicable price list of HP d.d.

9.2. Liability insurance

With regards to the risk of liability for damages in accordance with Article 13 of the eIDAS Regulation, HP d.d. has appropriate liability insurance. HP d.d. has sufficient resources and financial stability to provide qualified trust services.

9.3. Confidentiality of information

All employees of HP d.d. participating in the operation of the QERDS provision system shall maintain the confidentiality of information/data defined in this clause. The obligation to maintain confidentiality of the information/data also applies to employees of external service providers, which must be regulated in a business cooperation agreement between HP d.d. and external service providers. All information/data from the system for the provision of QERDS which is not marked as public is considered confidential information/data, including all information/data necessary for the provision of qualified trust services, classified data and such information/data whose disclosure would cause damage to the participants in the process.

9.4 Personal data protection

HP d.d. 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). HP d.d. is responsible for the protection of personal data processed during the provision of qualified trust services.

In the process of user registration and thereafter, HP d.d. is authorized to collect personal data necessary for the valid identification of users and other data necessary for valid provision of qualified trust services. Personal data collected by HP d.d., which is not visible in public records and/or registers which must be duly kept for the purpose of providing qualified trust services, is confidential personal data that HP d.d. adequately protects.

HP d.d. is authorized, except for the purpose of fulfilling legal obligations, i.e. obligations under the Contract, to use personal data and publish them only on basis of a written consent of the user, which can be given in the request for contracting the service or later.

Personal data may be disclosed to third parties only under the conditions provided by law.

9.5. Protection of Intellectual Property

All data and documentation published in the public repository of the system for the provision of QERDS represent the intellectual property of HP d.d.

The object identifier numbers (OIDs) used are the property of HP d.d. and are registered with the competent authority.

HP d.d. does not claim intellectual property rights to the software used in the system for the provision of QERDS, which is owned by third parties.

9.6. Obligations and responsibilities

9.6.1. Obligations of the service provider

HP d.d., as a qualified trust service provider, is responsible for:

- correct identification of users when contracting the service,
- trusted authentication of senders and recipients,
- providing the service in a secure manner while ensuring the authenticity, confidentiality and integrity of the data,
- proper protection of personal data,
- conducting internal and external compliance reviews,
- compliance with all prescribed obligations.

In addition, HP d.d. provides QERDS in accordance with the eIDAS Regulation, the Act on Implementation of the eIDAS Regulation, and standardisation documents. HP d.d. is responsible for the use of a reliable and credible information infrastructure which is used for the implementation of the qualified electronic registered delivery service.

9.6.2. Obligations of the user

Users are obliged to:

- provide accurate and complete information in the request for contracting the service,
- accept the Terms of Service and other related documents,
- keep authentication elements safe from loss, theft, damage or unauthorized use,
- report to HP d.d. any event that has compromised the security of authentication elements or a suspicion that such an event has occurred,
- refrain from taking advantage of any security failures or irregularities in the operation of the HP d.d. system, and notify HP d.d. immediately upon determination of such failures, as well as
- refrain from transferring its responsibilities in dealing with the qualified electronic registered delivery service to third parties.
- use the service in a lawful manner, in accordance with its permitted purpose and in compliance with applicable regulations

9.6.3. Obligations of relying parties

Reasonable confidence in a qualified electronic registered delivery service for the relying party is achieved if, at the time of use:

- takes the necessary preventive safety measures,
- verifies advanced/qualified electronic seal and qualified electronic time stamp of HP d.d. by using trustworthy systems,
- uses reliable applications in a secure IT environment.

The relying party not acting in accordance with these Rules of Procedure and the obligations arising therefrom is solely responsible for the risks of trusting the advanced/qualified electronic seal and qualified electronic time stamp of HP d.d.
The relying party is obliged to report to HP d.d. all changes that affect the provision of QERDS service.

9.7. Limitation of Liability

HP d.d., as a qualified trust service provider, assumes no responsibility for any damage that may occur in the following cases:

- if the registration of the user was carried out on the basis of incorrect or unreliable data submitted by the applicant,
- if the QERDS service has been used improperly or maliciously,
- if adversities or losses occurred in the period between submitting the registration application and delivery of authentication elements to the applicant,
- if the user or the relying party has not acted in accordance with the provisions of this Policy and Rules of Procedure
- if there has been abuse or security breach of the computer of the user or relying party
- if the user has enabled unauthorized persons to use QERDS
- if the computer of the user or relying party was malfunctioning
- if there has been a work interruption or infrastructure malfunction that is not under the responsibility or control of the QERDS provision system or
- if circumstances that can be described as force majeure have occurred.

Apart from what HP d.d. is expressly responsible for pursuant to clause 9.6 of this Policy, HP d.d. as a provider of qualified trust services is not liable for any other obligation or liability, especially not in the event that liability of HP d.d. under the given obligations would result from a breach of obligations and liability caused by other participants listed in the said clause of the Policy.
HP d.d. is not liable for damages, including indirect damage or loss of revenue, loss of data or other damages related to qualified trust services, caused by the use of electronic registered delivery of other service providers or the use of QERDS of HP d.d. in other way than as permitted in this Policy and Rules of Procedure.

9.8. Indemnification

Each participant in the QERDS system is liable to the injured party for damage caused by non-compliance with the provisions of this Policy, Rules of Procedure and relevant applicable regulations.

9.9. Complaint-dealing mechanism and disputes

Users may submit complaints with HP d.d. regarding the provision of a qualified trust service, to which HP d.d. will respond. Complaints are submitted and the procedure is carried out as specified in the General Terms of Use of the ePost Service. Any disputes between HP d.d. and users that may arise during the use of QERDS will be resolved amicably. In other cases, disputes will be resolved before the competent court in Zagreb with the application of Croatian law. Exceptionally, if applicable, the user – a natural person, provided that the conditions prescribed by the Act on Alternative Dispute Resolution of Consumer Disputes under which the user is considered a consumer are met, has the right to initiate a consumer dispute resolution procedure before the Alternative Dispute Resolution Body at: https://ec.europa.eu/consumers/odr.

9.10. Applicable Regulations

The qualified trust service within the scope of this Policy is provided by HP d.d. in accordance with regulations set out under clause 1.1. of this Policy.

9.11. Entry into force

This Policy enters into force on the day of its adoption, and applies from 15 December 2023, whereby the Qualified Electronic Registered Delivery Service Provision Policy of 1 January 2022 shall expire.

Number: HP-19/1-038964/23

HP-Hrvatska pošta d.d.
President of the Management Board

Ivan Čulo

HP - Hrvatska pošta d.d.
01
Velika Gorica, Poštanska ulica 9