APPROVED

PMO GOVERNANCE

DORU VIJIIANU ZIPPER SERVICES SRL Digitally signed by ZIPPER SERVICES SRL Date: 2025.10.14 18:30:39 +03'00'

JUDIT FEKETE FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2025.10.14 18:34:18 +03'00'

MIRELA OJOG Mirela Ojog Digitally signed by Mirela Ojog Date: 2025.10.14 15:25:52 +03'00'

-Zipper Services Authority-
Qualified Electronic Archiving Services
Policy and Code of Practice and Procedures

.

History of the edition			
Edition	**Date and description of the change**	**Ready**	**Approved**
1	28.02.2019 – First Edition	Mirela Ojog	Judit Fekete
2	06.02.2021 – Edition 2	Mirela Ojog	Judit Fekete
3	06.02.2021 – Edition 3	Mirela Ojog	Judit Fekete
4	10.05.2025 – Edition 4	Mirela Ojog	Judit Fekete
5	30.09.2025 - Edition 5 – Corelation with Preservation Service and CEN/TS 18170	Judit Fekete	Mirela Ojog

ZIPPER

Annex A. Contents

1. Introduction

This document constitutes the Policy and Code of Practice and Procedures of the Zipper Services authority (hereinafter referred to as Zipper). The purpose of the document is to describe the rules and operational procedures adopted by ZIPPER for the provision of electronic archiving services, in the Zipper Services data center, in accordance with Law no. 135 of 15 May 2007 on the archiving of documents in electronic form and the methodological norms for authorizing data centers.

This document is made available to the public at https://ezipper.ro/servicii/arhivare-conform-legii

The technical and security requirements (according to art. 5 of the Technical Norms regarding the accreditation procedure of electronic archive administrators and the approval procedure of electronic archiving systems, integral part of Order 20717/2024) that the electronic archiving system meets are described in the Security Plan specific to the electronic archiving system, considered an annex to this document.

The data center meets all the conditions required by the legislation in force in order to carry out electronic archiving operations.

Management may make exceptions to this document on a case-by-case basis to mitigate the significant, imminent impact on customers, partners, reliance parties and/or other persons in the absence of practical solutions. Any such handling exceptions are documented, tracked and reported as part of the audit process.

2. Policy administration

The electronic archiving service is offered by Zipper Services in the infrastructure of the Zipper Services Data Center, authorized by the ADR for electronic archiving services under the conditions of Law 135/2007 (Decision no. 253 of 23.05.2024).

The organization administering this document:
ZIPPER SERVICES SRL
Str. Rene Jeannel, nr. 8, Imobil Novis Plaza, corp A, et. 2, 400285, Cluj-Napoca, RO
Cluj-Napoca, 400285, Romania

Work point:
1 Decembrie 1918 Blvd. no. 1G,
Sector 3, Bucharest, 032451, Romania

Work point:
Nikola Tesla Street, no. 2, cod 400221, jud. Cluj
Cluj-Napoca, 400285, Romania
https://ezipper.ro/
Email: office@ezipper.ro

Phone +40 21.340.4638 / +40 31.101.1020
Fax: +40 21.340.4636 / +40 31.101.1022
(Monday-Friday 09.00. – 18:00 Eastern European Time)
Contact: pki@ezipper.ro Policy Management Team

3. Approval procedure

The approval of this document and subsequent amendments are made by Zipper's dedicated persons. These individuals make up the policy management team. PMG Governance members approves new versions of this document. The amended versions supersede any conflicting provisions of previous versions of this document.

4. References

Applicable national legislation:

1. Law no. 135 of 15 May 2007 on the archiving of documents in electronic form
2. ORDER no. 20.717 of May 9, 2024 for the approval of the Technical Norms regarding the procedure for the accreditation of electronic archive administrators and the procedure for the approval of electronic archiving systems and for the repeal of the Order of the Minister of Communications and Information Society no. 493/2009 on the technical and methodological norms for the application of Law no. 135/2007 on the archiving of documents in electronic form
3. MCSI Minister's Order no. 489/15.06.2009 regarding the methodological norms for authorizing data centers
4. Order no. 585 of 9 May 2011 for the completion of the Order of the Minister of Communications and Information Society no. 489/2009 regarding the methodological norms for authorizing data centers
5. Order no. 1167 of 25 November 2011 for the amendment of Annex no. 3 to the Order of the Minister of Communications and Information Society no. 489/2009 on the methodological norms for authorizing data centers.
6. Law no. 455/2001 on the electronic signature, republished, with amendments and completions
7. The National Archives Law no. 16/1996, republished, with subsequent amendments and completions;
8. Law no. 182/2002 on the protection of classified information, with subsequent amendments and completions;
9. Government Decision no. 89/2020 on the organization and functioning of the Authority for the Digitization of Romania, with subsequent amendments and completions;
10. The technical norms regarding the procedure for the accreditation of the administrators of the electronic archive and the procedure for the approval of the electronic archiving systems, approved by the Order of the Minister of Research, Innovation and Digitalization no. 20.717/2024;

The following references contain provisions that are relevant to the ZIPPER data center policy and the electronic archiving service:

11. Law no. 190/2018 on measures for the implementation of 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), as amended.

12. 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 [1];

13. CEN/TS 18170:2025 – Functional requirements for the electronic archiving services

14. 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)

15. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); general policy requirements for trust service providers;

16. ETSI SR 019 510 Electronic Signatures and Infrastructures (ESI); Delineation study and framework for standardization of long-term data preservation services, including retention/with digital signatures;

17. ETSI TR 119 001 Electronic Signatures and Infrastructures (ESI); Signature standardization framework; Definitions and abbreviations;

18. ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); cryptographic suites; Directive 1999/93/EC.

19. IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)"

5. NAME AND IDENTIFIER OF THE DOCUMENT

The full name of this document is "Qualified archiving service (QAS) “Policy, Code of Practice and Procedures (PCPP)" and object identifier (OID):

Name of the document	Object Identifier (OID)
Qualified archiving (QAS) - Policy, Code of Practice and Procedures (PCPP)	**1.3.6.1.4.1.57570.4.4.2** 4=> service classification node 4 => archiving services (subtree of preservation-related policies) 2=> **qualified** archiving variant

6. Definitions and abbreviations

6.1 General Terms and definitions

a) **data center** - a secure space, equipped with computing technology and communication equipment through which data in electronic form is received, stored and transmitted;
b) **beneficiary - holder of the right to dispose of the document** according to art. 3 letter h) of Law no. 135/2007 on the archiving of documents in electronic form, republished, which deposits for preservation the documents in electronic format in an electronic archive;
c) **accreditation** - the ascertainment by the A.D.R. of the fulfillment of the legal conditions for acquiring the quality of administrator of the electronic archive;
d) **electronic archiving system** - according to art. 3 letter g) of Law no. 135/2007 on archiving documents in electronic form, republished;
e) **IT audit** - the activity of collecting and evaluating evidence to determine whether the system IT complies with the performance and work parameters according to the design requirements, if it ensures the functionalities necessary for business requirements and compliance with the legislation in the field, if it is secure, if it maintains the integrity of the processed and stored

data, if it allows the achievement of the entity's strategic objectives and the efficient use of information resources;

f) **IT auditor** - the authorized natural person who holds an IT auditor certificate or the legal person with certified personnel who carries out an audit activity of information systems, according to
regulations and good practices in the field;

g) **IT audit report** - the tool through which the purpose of the audit is communicated, the objectives pursued,
the norms/standards applied, the period covered, the nature, procedures, findings and conclusions of the audit, as well as any reservations that the IT auditor has regarding the audited information system;

h) **qualified trust service provider** - according to art. 3 point 20 of 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;

i) **backup** - the activity of copying files or databases in order to preserve and recover them in case of damage or other unforeseen event;

j) **Data container:** a data object containing a set of data objects and additional information describing the data objects contained and, optionally, the content and relationships between them (digital signatures/seals, timestamps, evidence records, validation data, etc.);

k) **Qualified EU Timestamping Authority**: a qualified trust service provider issuing qualified electronic timestamps as provided for in Regulation (EU) No 910/2014;

l) **evidence recording**: data that can be used to prove the existence of an archived data object or a group of archived data objects at a particular point in time;

m) **Nomenclator (based on Romanian archiving legislation Ordinul de zi nr. 217 din 23 mai 1996)**
The nomenclature is drawn up in the form of a table in which the categories of documents grouped by issues and retention periods are entered, by work compartments.
The fourth box of the nomenclature indicates the **retention period**. Its establishment is made taking into account the laws in force (accounting, GDPR, ohers), the practical importance for the activity of the creator of documents and, in particular, the scientific importance of the information that the documents contain. The word "permanent" is used next to groups of documents that are kept permanently, and for those that are kept temporarily, the Arabic numeral representing the number of years/month that they are kept. Art. 12. - The file nomenclature is not changed annually, but only when changes occur in the structure of the document creator. If new work departments or subdivisions are established, the nomenclature

is completed with their name and the newly created files. In the case of work departments or their subdivisions that develop their activity by creating other groups of documents than those initially provided for, the nomenclature is completed with the new files.

Art. 14. - The nomenclature is approved by the management of the document-creating unit and is confirmed, at the central level, by the [Romanian] ***National Archives*** and, at the local level, by the county directorates of the National Archives.

n) **long-term**: a long period of time during which technological changes, such as the moral wear and tear of cryptographic technology, cryptographic algorithms, key sizes or hash functions, essential compromises or the ability to check the validity status of certificates may be a cause for concern;

o) **long-term preservation**: long-term preservation (with or without storage), in which the prolongation of the validity of a digital signature and/or the provision of evidence of the existence of data over a long period of time does not depend on the moral wear and tear of cryptographic technology, cryptographic algorithms, key sizes or hash functions, key compromises or the ability to verify the validity status of certificates;

p) **preservation object container:** a file container for preserving data objects, for example, ASiC-S, ASiC-E

q) **'retention object identifier' means** a unique identifier of a retain/archive object;

r) **qualified electronic signature** - according to Article 3(12) of 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

s) **extended electronic signature** - according to art. 4 item 4 of Law no. 455/2001 on electronic signature, republished, with subsequent amendments and completions;

t) **qualified time stamp** – qualified electronic time stamp in accordance with Article 3(3) of 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;

u) **archival nomenclature** - a working tool used in the archival field, which is developed by each creator for the organization and management of his own documents, in accordance with the provisions of the National Archives Law no. 16/1996, republished, with subsequent amendments and completions;

v) **electronic archiving trust service -** service ensuring the receipt storage, retrieval and deletion

of electronic data and electronic documents in order to ensure their durability and legibility, as to preserve their integrity, confidentiality', and proof of origin throughout the preservation period

w) **qualified electronic archiving trust service** - electronic archiving trust service provided by a qualified, electronic archiving trust service provider to fulfil additional requirements and subject to periodical independent third-party conformity assessment by accredited conformity assessment bodies

x) **electronic archiving trust service provider** - natural or legal person providing electronic archiving trust service

y) **qualified long-term preservation** - qualified service for the preservation of qualified electronic signatures according to art. 34 para. (1) of 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;

z) **qualified certificate** – qualified certificate for electronic signature according to Article 3(15) of 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;

aa) **audit log** - a register in which all actions taken on data and/or documents in electronic form or on the system itself are recorded, including information such as the date and time of the action, the user involved, the type of action (creation, modification, deletion, etc.), as well as any other relevant details;

bb) **Access policy for an electronic archive** - a formal set of rules and procedures established to control and manage access to information and documents stored in electronic format within an archive. This policy is intended to ensure that only authorized persons have access to the data and documents stored in the archive and that their security and integrity are adequately protected;

cc) **security policy for an electronic archive** - specifying the security measures necessary to protect the information stored in the archive against unauthorized access, alteration or destruction (may include data encryption, implementation of strict password management policies, access monitoring, etc.);

dd) **Electronic Document Retention Policy** – establishing rules and procedures for long-term archive retention and management, including defining document retention and disposal periods in accordance with the archive administrator's regulations and policies

6.2 Terms related to digital objects

a) **digital object:** object composed of a set of bit sequences, Electronic data and electronic documents are digital objects [SOURCE ISO 14721]

b) **information package -** container of digital objects and additional information to make both the objects and the package understandable and usable. Additional information include: packaging information, representation information and preservation descriptor information. Information package is machine-readable.

c) **packaging in formation -** information that describes how the components of an information package are logically or physically bound together and how to identify and extract the components

d) **preservation description information -** information necessary for adequate preservation of the digital object (Context Information, Reference Information, Fixity Information, and Access Control Information)

e) **submission information package -** information package that is delivered by the subscriber to the electronic archiving trust service for the creation or update of one or more archival information packages

f) **archival information package -** information package which is archived within an electronic archiving trust service

g) **dissemination information package** - information package, derived from one or more archival information packages, and sent in response to a request

6.3 Terms related to electronic archiving

a) **electronic archiving -** processes carried out for keeping digital objects available, readable, interpretable and reliable for as long as needed. Digital objects are usually stored in information packages. The range of processes applies from the initial acquisition of digital objects to the end of their preservation period.

b) **Preservation -** act of maintaining overtime information, independently understandable by a designated community, and with evidence supporting its authenticity. In the context of preservation of electronic signatures seals, timestamps, or certificates ETSI EN 119 511 defines preservation service as service capable of extending the validity status of a digital signature over long periods of time and/or providing proof of existence of data over long periods of time.

c) **preservation period -** defined period during which an electronic archiving trust service ensures the archiving of digital objects

d) **transfer -** technical and organizational process for giving back the archived digital objects to the subscriber or to another Entity authorized by the subscriber

e) **format conversion -** process of changing the files included in a digital object from one format to another

f) **media migration -** transferring information from one mediate another without changing the bits sequence

6.4 Abbreviations

Abbreviated terms	terms
IP	Information Package
SIP	Submission Information Package
AJP	Archival Information Package
DIP	Dissemination Information Package
PDI	Preservation Description Information

OAIS	Open Archival Information System
EATS	Electronic Archiving Trust S ervice
EATSP	Electronic Archiving Trust Service Provider
EAQTSP	Archiving Qualified Trust Service Provider
TSP	Trust Service Provider
RepoZip LTA	Zipper Archiving application, registered in the Romanian Register of electronic archiving systems https://www.adr.gov.ro/arhivare-electronica/
Collibri	Zipper Operational Document Management system

6. General concepts

'Electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.

This document describes the functionality of the electronic archiving service, and is applied to electronic data and electronic documents created in electronic form as well as paper documents that have been scanned and digitised.

Based on **eIDAS 2.0 Article 45j** the qualified archive services shall meet the following requirements:

(a) they are provided by qualified trust service providers;

(b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin;

(c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration*, except for changes concerning their medium or electronic format;*

(d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval. The report shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.

The LTA service is intended for users who need long-term retention of their electronic documents signed with advanced/qualified electronic signature. The registration of documents in electronic form by the electronic archiving system certifies the official existence of those documents. The registration number uniquely identifies the document within the system. Once registered, the document cannot undergo any changes in content. At the same time as the registration, the electronic file of the

document shall be completed, under the conditions of art. 8 para. (2) and (3) of Law no. 135/2007, republished.

The following aspects are also dealt with within the archiving service:

1) Long-term preservation using electronic signature techniques, the ability to validate an electronic signature, and the ability to generate evidence of the existence of the data associated with the signature, at the time of entering a document into the archive, even if the signature key is subsequently compromised, the validity of the certificate expires or there is a cryptographic attack of the signature algorithm or hash algorithm used in the signature;

2) Providing evidence of the existence of digital objects, using electronic signature techniques (electronic signatures, time stamps, records of evidence, etc.)

3) Preservation of digital signatures (PDS) for long periods of time to maintain their validity

All these objectives require:

- Proof of the integrity of an electronic document or a signature/seal;
- Proof of the existence of an electronic document or a signature/seal at a given time/in the past;
- Maintaining the validity of electronic signatures/seals applied by the archivist for long periods of time;
- Data availability.

The integrity of the data is verified during the retention period by means of a proof of integrity (hash, signature/seal).

The proof of existence indicates that the digital object existed at a certain time and is implemented by combining a proof of integrity and a time indication of confidence (qualified time stamp).

In order to maintain the validity status of the electronic signature/seal, all the elements necessary to verify the validity and whose availability cannot be guaranteed in the future must also be preserved. This can include certificates, revocation information (CRLs, OCSP responses), trust lists, etc.

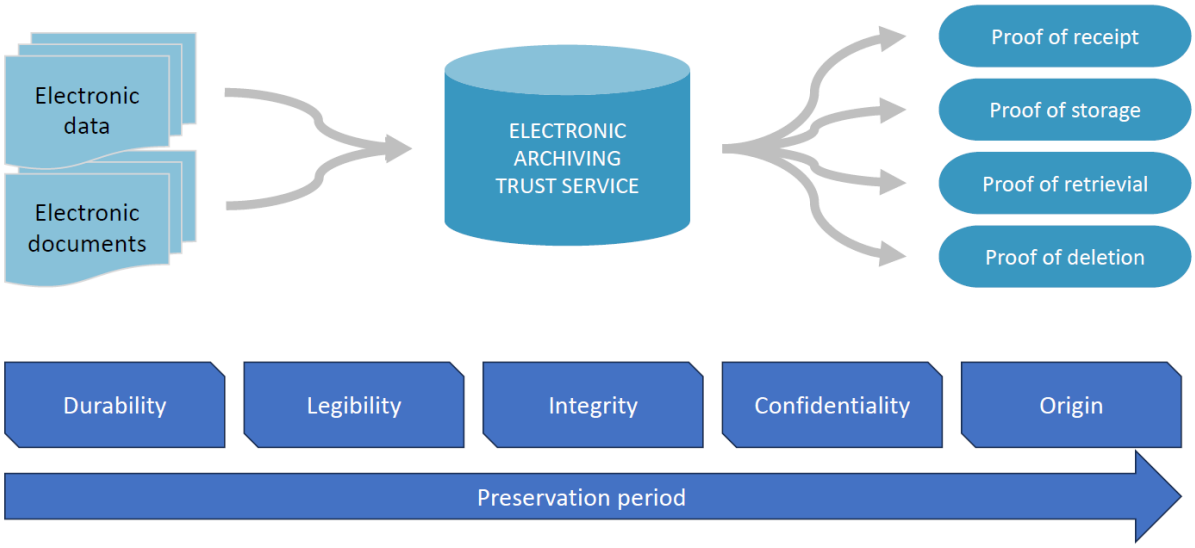
Qualified timestamping services using the RFC 3161 timestamping protocol over HTTP transport are used in the archiving process. Qualified timestamping services ensure the use of a reliable time source and the correct management of all system components. Qualified signature/seal validation services are also used.

6.1 Service Provision Process

The qualified archiving service (QAS) RepoZip LTA provided by Zipper QTSP use procedures and technologies to ensure the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin and are preserved in such a way that they are safeguarded against loss and alteration*, except for changes concerning their medium or electronic format.*

RepoZip LTA is the archiving application responsible to provide techical support for the archiving flow. The document to be archived is packaged in a digital container together with the signed validation

proof that the signature/seal was validated, as well as other metadata detailing the archiving process, as required by the Romanian law. In the next step, the container is encrypted to safeguard integrity. The encryption happens by applying a Long-Term Archival signature (also called an LTA-level signature) with Zipper qualified time stamp provider. Zipper's way of creating and encrypting containers is based on Associated Signature Container (ASiC) baseline profile for the container and the CMS Advanced Electronic Signature (CAdES) for the encryption.



6.1.1 Proofs of Electronic Archiving

6.1.1.1 Proof of Receipt

Receipt of data in our archiving system is confirmed through multiple technical and procedural measures:

- The document's import triggers the creation of a unique hash which is permanently linked to the document, serving as proof of receipt.
- Qualified electronic seal is applied (level B-LTA) on preservation object content (imported document, metadata and signed validation report) and stored in accordance with the specified **preservation profiles**
- The system generates a **validation report** that certifies that the document was correctly received regarding the signatures/seals
- An audit log records the exact date and time of import, the operator performing the action, and the uniqueID of the object container (ASIC-E), providing an unalterable record of receipt
- The **qualified timestamp** provided by Zipper TSA (Time-Stamping Authority) further affirms the moment of receipt, creating a trusted proof that the document existed in the system at a specific point in time.

6.1.1.2 Proof of storage

Our archiving service guarantees data integrity, confidentiality, and long-term availability through a combination of advanced technical measures and infrastructure. Specifically, we utilize Dell Elastic Storage (ECS) with geo-replication, which ensures that data is stored redundantly across geographically separated locations. This setup provides:

- Data durability: copies stored at different site to prevent data loss
- High availability: Continuous access and retrieval of data, even in case of hardware failure or disaster
- Compliance: Meets regulatory requirements for data retention and security, as the data remains unaltered and securely stored

This infrastructure, combined with digital signatures, hash functions, audit logs, and qualified validation services, ensures a comprehensive proof of storage, with data being both tamper-evident and reliably recoverable at any time.

All operations on documents, such as import, or access are logged with detailed audit trails.

6.1.1.3 Proof of Retrieval

The system guarantees the authenticity and integrity of data during retrieval through:

- **Secure, authenticated access controls** ensuring only authorized users can retrieve documents.
- The retrieval process is logged, including the user identity, time, and accessed document details.
- The retrieved documents are accompanied by their respective signatures, seals, and hash values, which users can verify using the validation service
- Metadata and audit logs maintain a detailed record of the retrieval event, fulfilling legal and compliance requirements for proof of access.

In accordance with the National Archives Law no. 16/1996 updated in 2025 and the regulations on document management, digital data destruction is carried out only after the legal retention period has been completed and in the presence of strictly controlled and audited processes. When a document reaches the retention period, our system:

6.1.1.4 Proof of Deletion

Proof of deletion need to be adapted to legal compliance (e.g., GDPR, Romanian National Archives Law no. 16/1996 updated in 2025) and internal auditing procedures.

In accordance with the National Law and the regulations on document management, digital data destruction is carried out only after **the legal retention period has been completed** and in the presence of strictly controlled and audited processes.

When a document reaches the retention period, our system:

- Records a possible deletion request in the audit log, mentioning the date, time, operator and reason for deletion
- Performs a final check of the list of documents before deletion, and needs operator approval
- Keeps all deletion records in logs, so that they are available for audit and legal verification, according to the Romanian and European legal framework

- If there is a requirement to extend the preservation of a document, it must be documented and approved by Romanian National Archives.

This procedure ensures compliance with national legislation, transparency of the process and the possibility of demonstrating, at any time, that the documents have been deleted legally and securely.

6.1.2 Data Integrity

- The archiving solution implements mechanisms (such as digital signatures and hash functions) to ensure that archived data remains unaltered by making the imprint of the documents and signing with the qualified electronic seal issued to Zipper Services (the archivist)
- Fingerprint generation (hash): Each document is associated with a unique hash (e.g. SHA-256) calculated before import
- Audit trail and logging: Any operation on the document is recorded in a log
- Provide verification processes enabling users to confirm data integrity and authenticity at any time over Qualified validation service (validation report)

6.1.3 Data Confidentiality and Access Control

- access control ensures that only authorized personnel can access archived data, RepoZip developed access policies to govern who can access the collections and under what conditions. These policies often balance the need for public access with the protection of sensitive or copyrighted materials.
- ensuring access to documents (associated metadata) through a secure channel, only by authenticating the person, in accordance with the permissions resulting from the group and role setting (based on the Nomenclature in force sent to the Zipper archiver EATSP). The solution allows:
    - RepoZip LTA implements different type of authentication mechanisms, such as login credentials and IP restrictions,2FA, SSO to ensure that only authorized users can access restricted materials. They may also employ encryption to protect sensitive data.
    - Granular access control: Permissions are dynamically managed based on the groups and roles defined in the Archival Nomenclature. Access can be restricted at the level of allowed action (e.g. read, download).
    - End-to-end encryption: The communication channels between the user and the archive are encrypted with TLS 1.3 protocols, and the archived objects are stored encrypted (AES-256).

6.1.4 Long-term Preservation (durability)

- Support data preservation over extended periods, considering technological obsolescence.

- The archiving service offered by Zipper QTSP is based on **preservation profiles specified in QPS-QPSA-ZS_Qualified Preservation Services_v1 PCPP:**

- use a Qualified TimeStamp provided by Zipper Time-Stamping Authority (TSA)
- use a Qualified Validation Service (ValS) (see ETSI TS 119 441 and ETSI TS 119 442) to collect certification path information and revocation information or directly collect certification path information and gather certificate status information issued by a Certificate Status

Authority (CSA).

6.1.5 Availability

The RepoZip LTA application ensures the necessary conditions for easy retrieval and use, whenever needed, in strict compliance with the conditions of confidentiality and integrity of documents (associated metadata):

- Redundancy and replication: The archive is stored in two geographical locations (geo-redundancy) to prevent data loss
- Periodic and automatic backup: Performed daily, with strict restore policies
- Quick Retrieval Interface: Provides search functionality based on associated metadata

6.1.6 Authenticity

The RepoZip LTA application ensures the possibility of verifying the identity of the person/entity, who signed/sealed the document with a qualified certificate, as the holder with the right to dispose of the document. This verification is done through the qualified signature/seal validation service (Zipper Services accreditation):

- eIDAS qualified certificates: Only signatures/seals based on qualified certificates, issued by accredited suppliers, are accepted and the verification report, signature
- Automatic validation: The system integrates validation services (OCSP, CRL) provided by Zipper Services to verify the validity of the signatures and seals of the holders of the right of disposal.
- Marking of the identity of the signatory: Metadata with the data of the signatory and the issuing authority of the certificate is preserved

6.1.7 Non-repudiation

It is ensured that after importing into RepoZip LTA that document existed at that time of time. This proof is provided by the procedurally applied measures, the archivist also applying a qualified time stamp to subsequently demonstrate its existence.

- Registered import with qualified timestamp: At the time of import, a timestamp according to the eIDAS Regulation is applied to the archived object, certified by the QTSP supplier Zipper
- Chain of trust: Each archived object is accompanied by a qualified seal of the Archiver (Zipper EATSP) and a timestamp embedded in the signature, forming a cryptographic chain that can be verified in court

6.1.8 THE OWNER OF THE DOCUMENT IN ELECTRONIC FORM

The owner of the document in electronic form is defined at the application level under the name of Client and will define the types of documents, metadata, groups and users belonging to this Client.

The holder of the right to dispose of the document is the owner or, as the case may be, the issuer of the document, who has the right to establish and modify the regime of access to the document,

according to the legislation in force.

The receipt of a document in electronic form in the electronic archive is conditioned by the fulfillment of the following requirements:

a) signing the documents in electronic form with the extended electronic signature of the holder of the right to dispose of the document, hereinafter referred to as the electronic signature.
b) the validity of the electronic signature of the holder of the right to dispose of the document at the time of its introduction in the archive;

The beneficiary of the electronic archiving service must:
a) to possess a qualified digital certificate for the electronic signature;
b) the qualified digital certificate must be valid;
c) to communicate to the administrator the information necessary to verify the validity of the certificate used for the electronic signature of the documents stored in the electronic archive.

6.1.9 DOCUMENT METADATA

Within the application, descriptive preservation information is created for the archived information, respectively keywords necessary to identify the document in electronic form.

Keywords, hereinafter referred to as metadata, will allow user groups to discover and identify the document of interest.

Required metadata will include creator information, data formats, cryptographic details and metadat required by nation archiving law and will contain at least the following information:

a) the owner of the electronic document;

b) the issuer of the electronic document;

c) the holder of the right to dispose of the document;

d) history of the electronic document;

e) type of electronic document;

f) classification level of the electronic document;

g) the digital format in which the electronic document is archived;

h) the keywords necessary to identify the electronic document;

i) the elements of locating the physical medium (if the electronic document was generated by transferring information from analog to digital media)

j) the unique identifier of the electronic document, within the electronic archive;

k) the date of issue of the document;

l) the date of archiving;

m) the term of retention of the document.

If the electronic document was generated by transferring information from analog to digital media, the record shall additionally contain the following information:

a) references to the owner of the original and the location where the original is located;

b) the transfer method used;

c) the hardware device used;

d) the computer program used.

6.1.9.1 Information packages — Information Package Format

The Information Package is defined in a formal data definition language (XML), and is sent to the Subscriber, based on metadata list defined by the Romanian law.

The IP differentiate between mandatory and optional data elements in the definition and description of the data structure.

Optional elements in the format maybe defined as mandatory due to conditional logic (e.g. an element is optional, but if it exists the otherwise following optional requirement is mandatory).

Retention period is defined in the Subscriber`s Nomenclator (in month), but calculation of date could be relative to date of issue of the document or other date (defined in another metadata – e.g. document closing date)

6.1.10 Transfer submission

Zipper QTSP is responsible for the integrity and confidentiality of the transfer of the submission provided by the Subscriber and will verify if the the procedures and protocols for the transfer has been followed by the subscriber.

The exchange of information between the Subscriber and Zipper QTSP is carried out based on a signed agreement (contract), which includes the means, requirements and responsibilities related to information security. Each agreement will contain a documented procedure for handling transfer between Zipper QTSP and Subscriber and also, the possible failures between the subscriber and Zipper EATSP.

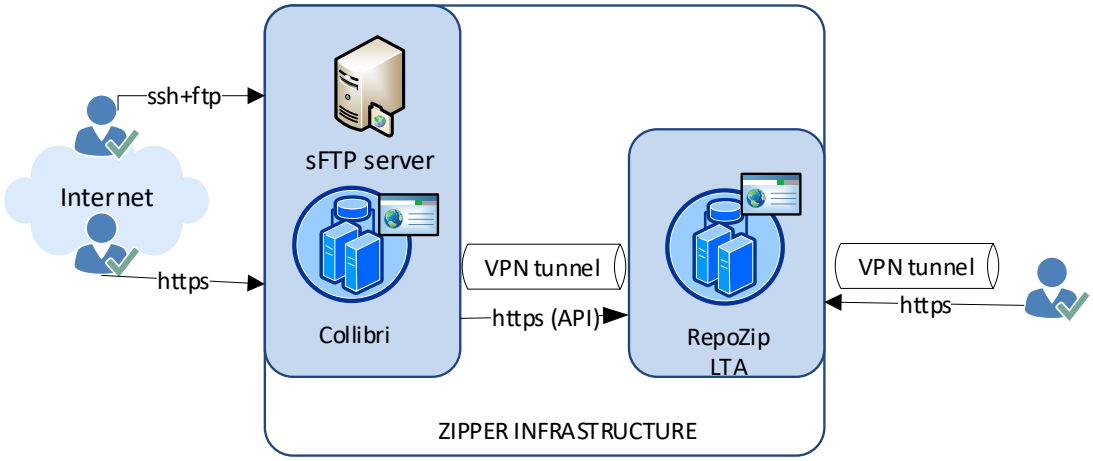
Different communication security protocols can be applied (at data link, network, transport and application level) such as: tunneling protocols (IPSec/SSL VPN), sFTP, FTPs, HTTPS, which will be established in the signed agreement.

Zipper EATSP provides transfer of the documents over the internet (with tunneling protocols) using common network protocols:

- sFTP/ FTPS
- REST API
- Manual upload over UI

Example of transfer:

REST API



possible failure responses:

answerId	***answerMessaje***	***'additionalText'***
1	*FILEUPLOADEDSUCCESSFULLY*	*POCId:12345* Other elements (Receive submission defined at Subsciber level)
-1	*TEMPLATEERROR*	*Null*
-2	FILEERROR	Null
-3	FILETYPEERROR	Null
-4	REQUIREDDATAMISSED	Null
-5	SYSTEMVARIABLEERROR	Null
-6	METAVARIABLEERROR	null
-7	FILESAVEERROR	null
-8	SUBTEMPLATEERROR	null
-9	FILESIGNATUREERROR	null
-10	FILESIGNINGERROR, LOGIN FAILED	null
-12	FILEUPLOADNOTSUCCESFUL	null

6.2 Audit and Traceability

Zipper maintains detailed logs of all actions on archived data, including creation, access, modifications, and retrieval and can enable traceability for audit purposes and legal compliance.

6.3 Security Measures

The application is stored in a secure infrastructure in Zipper datacenter and applies physical and logical security controls to protect against data loss, tampering, theft, and unauthorized access.

6.4 Operational Procedures

The Subscriber agreement define clear operational procedures for data ingestion, validation, storage, and retrieval.

Zipper implemented disaster recovery and backup processes to minimize data loss risks.

7. Practice Statement related to eArchiving service offered by Zipper

The archiving flow consists of:

1. **Transfer submission**: Downloading the document and associated metadata from the operational archive to the RepoZip LTa aplication in the agreed way (FTP hot folder, API). Ex. the operational archive application will call, through webservice, the request to upload a document and the associated metadata in the archive.

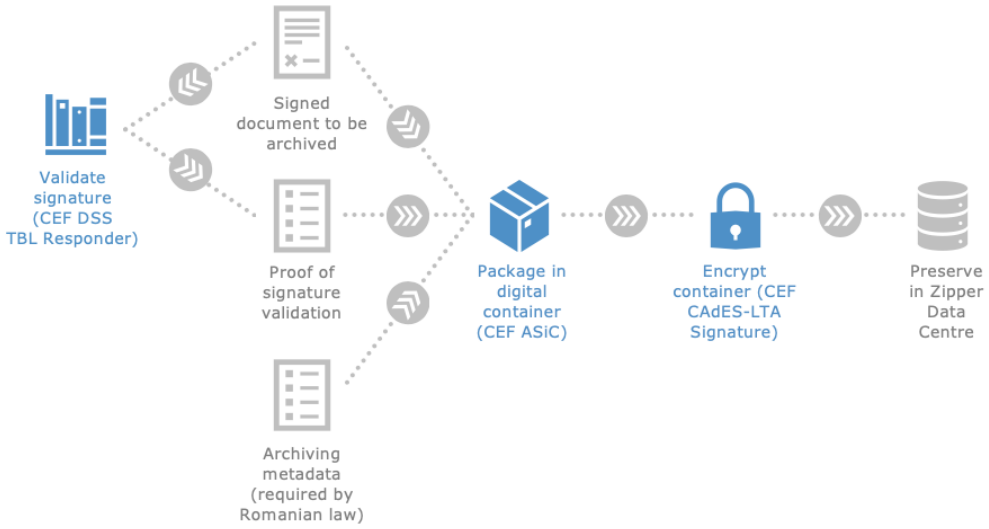
2. **Verify Information Package**: Based on document type, RepoZip make the association to the archival nomenclature of the user company and completing the mandatory metadata (based on Romanian law).

POST parameter or XML metadata	Required
UniqueIdentifier	Receive submission element
_Owner	Yes
_Issuer	Yes
_DispHolder	Yes
_Type	Yes
_Classification	Yes
_IssueDate	Yes
_ArchivingDate	Yes
_ArchivingPeriod	Yes
AdditionalMetavar1, AdditionalMetavar2,…. AdditionalMetavar10	Optional

If auxiliary table `Nomenclator` is provided by the Subscriber, there will be a clear correlation between NomenclatorId and the archived document, in this case _ArchivingPeriod (preservation period) and other required metadata will be completed automatically by the archiving application.

3. **Preservation of Object Container based on Qualified Preservation Service, Preservation scheme with signature/seal augmentation and with storage (F3 – comply with ETSI ES 119 512 Appendix F)**

- The application verify automatically the electronic signature of the document. The signature/seal of the official issuer of the document need to valid and made with a qualified certificate
- Generate a validation report based on ETSI EN 319 102-1, using Zipper `qualified validation service` QVS (checks certificate status, revocation, signature profile, algorithms, etc.). Validation report is signed with a qualified electronic seal (issued for Zipper) and embedded qualified TS.
- QVS returns a Validation Report (VR), digitally signed/sealed by the QVS, asserting the result at that point in time.
- The validation will result a TOTAL_PASSED, INDETERMINATE OT TOTAL_FAILED status, based on Zipper constrain rules.
- Only the TOTAL_PASSED and INDETERMINATE (NO-POE) electronic document will be accepted in the archive to be preserve. An ASIC-E container is created and is countersigned/sealed by the archive administrator (Zipper) using a qualified electronic certificate. The signature applied on ASIC will provide Long Term Availability and Integrity of Validation Material (ER). **Receive submission** is provided.
- **Augmentation of POC**: The RepoLTA archiving application will mentain the preservation of the validity status of the digital signature (LTA-level signature) applied on ASIC file. This operation will be done for ASIC files, before the qualified timestamp applied will expire or there are cryptographic security issues.



In case of a successful IMPORT in the electronic archive:

1. The electronic document will receive a unique ID (IDDoc/POID) for identification within the archive.

2. The document container `Associated signature container' is created, stored in a ZIP format (extension .asic), according to ETSI TS 102 918 V1.3.1. The container will contain the original pdf received, the received metadata, the validation report, according to ETSI EN 319 102-1

3. It is countersigned with the electronic signature of the administrator of the electronic archive;

4. The qualified time stamp is applied

5. The automatically created metadata is generated

The „electronic file'' attached to each archived document will contain at least the following information:

Received from the Beneficiary:

a) the owner of the document in electronic form.

a) the issuer of the document in electronic form.

b) the holder of the right to dispose of the document.

c) date of issue of the document.

d) type of document in electronic form.

e) the classification level of the document in electronic form.

f) keywords necessary to identify the document in electronic form.

g) the document retention period (can be calculated relative to a metadata/keyword).

h) elements for locating the physical support; - if it's necessary.

Generated automatically in the archiving app (after the moment of electronic archiving):

Generated by Archiver (Zipper EATSP):

i) the unique identifier of the document in electronic form, within the electronic archive.

j) date of archiving (date of entry into the archive).

k) the digital format in which the document is archived in electronic form.

l) the history of the document in electronic form.

m) the size of the archived document

If a document does not meet the integrity criteria, it is automatically marked and cannot be archived. After correction, it will have to be re-entered into the system and, if it passes the validations successfully, it will be archived.

All operations performed on the electronic archive are logged, the audit records containing the date and time of the event, the type of event, the result (success or failure) of the event.

Access to the RepoZip electronic archiving system is achieved through secure communication lines between the Beneficiary and the Provider (Zipper Services). Access to archived documents is restricted, a user can retrieve an archived document only if he is part of the access group established by the participant to access the document and has the appropriate security level to be able to view the document.

The archiver verification and signature module uses eSignature DSS to first validate the electronic signature of the received document, before the document is approved for archiving.

- Check if the signature is qualified and what type of certificate was used. The beneficiary will be responsible for signing the documents using a qualified certificate provided by a QTSP (qualified trust service provider). If signing is outsourced, it must be done by a QTSP, which offers QTS (qualified trust services) signing. AdES digital certificates are accepted (according to ETSI TR 119 112 V1.1.1 (2019-04) and ETSI EN 391 102-1 [i.6]) of the type:

-> Basic Signature (Ex. CAdES-B, PAdES-B, etc.)

-> Signature with Time (e.g. CAdES-T, PAdES-B-T, etc.)

-> Signatures with Long-Term Validation Material. Ex. CAdES-X, PAdES-B-LT

-> Signatures providing Long Term Availability and Integrity of Validation Material (Ex. CAdES-X-L, PAdES-B-LTA, PADES-E-LTV, etc.)

The verification steps are:

A) the X.509 certificate for the electronic signature applied to the document by the holder of the right of disposition is checked by:

-> hash comparison for document integrity;

-> Public Key Certificates (PKC) used

-> Revocation status information for each Certificate Revocation List (CRL) or Certificate Status (OCSP)

-> `Time assertion' applied to the signature (if any)

- The document to be archived is then packed in a digital container together with proof that the signature has been validated, as well as other metadata detailing the archiving process, according to Romanian law.

- In the next step, the container is encrypted to protect the integrity. Encryption occurs by applying a long-term archiving signature (also called an LTA-level signature) with a qualified timestamp provider.

- The Data Container Creation and Encryption (ASIC) module is also based on the eSignature DSS specifications: the Associated Signature Container (ASiC) base profile for the container and the CMS Advanced Electronic Signature (CAdES) for encryption.

- ASIC: `Associated signature container' according to ETSI TS 102 918 V1.3.1. The container will contain the original pdf received, the verification PDF (point b), the received metadata, signature identification data.

Zipper eArchiving service archive Preservation Object Containers as is described in Zipper eArchiving Policy.

The POC contains:

- Preservation Objects (POs) — the data to be preserved. These could be only signed data
- Evidence, validation and revocation / status data — data needed to validate signatures, time-

stamps, certificate revocation / validity paths, and possibly validation reports. These are essential to ensure that in future the validity status (or invalidity) of signatures can be reconstructed.

- Metadata about the POC itself: identifiers (e.g. owner of the document), timestamps, hash values, checksums, etc. This supports integrity, traceability, ability to verify that the container hasn't been tampered with, and helps reconstruct evidences.

Zipper POC container has the following specifications:

- **Format**: ASiC-E container
- **Contents**: Signed documents + signatures + validation report (signed XML) + evidence records
- **Signature level**: B-LTA (Baseline with Long-Term validation and Archival timestamps)
- **Signing certificate**: Qualified certificate for electronic seal issued by a QTSP [Provider] from TL, issued to *Zipper Services*
- **Timestamping**: Qualified timestamp (QTS) provided by Zipper QTS (see https://pki.ca.ezipper.ro/repository/certs.php)
- **Validation data included**: Certificates, revocation information (CRLs/OCSP) by a Validation report issued by Zipper QVS.
- **Purpose**: Preservation service ensures the signature and associated objects are verifiable over the long term, compliant with ETSI TS 119-511 and eIDAS requirements.

Zipper will preserve the POC by extending it over time:

[**Client**] → *Zipper Creates initial POC* (ASiC-E, B-LTA level) → [**Preservation Service** PDS+PGD+WST] *-> Validate via SVS → Collect validation data-> Generate Preservation Evidence-> Store extended POC (+ evidence) with =>* [**Preservation Service-AUG**] **(A-E, B-LTA level)**

↓

RetrievePO / Audit / Verify

8. Data center used by the electronic archive

The Zipper data center used by the electronic archive administrator Zipper Services has the necessary technical equipment and applies the necessary management and security policies and procedures to meet the conditions provided for in <>art. 17 para. (1) of Law no. 135/2007 and the requirements of

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 Eidas 2.0 related to archiving services.

The electronic archive resulting from the electronic archiving service (LTA Service), is stored in the data center subject to prior Romanian authorization, in compliance with the rules on ensuring:

a) the integrity and security of documents in electronic form;

b) the security and integrity of the space occupied by the equipment hosting the electronic archives;

c) recovery of information following natural disasters, according to the regulations in force.

Data centers meet the following conditions:

(a)ensure the security and integrity of the data, at the level of physical security and access through computer means;
b) the availability of the electronic archiving service and the backup of the stored information.

Data availability is ensured by using dedicated storage devices in two different locations in a high-availability configuration, using a clustered backend that provides mirrored copies of all documents and associated metadata.

8.1 Data Center Policy

This document contains specific details on the operating environment, organisational structure, operating procedures, facilities and infrastructure of ZIPPER. It describes only the general rules for managing the data center. Detailed descriptions of the infrastructure and related operational procedures are described in additional documents that are not publicly available. These additional documents are only available to ZIPPER authorised staff and, on a need-to-know basis, to the conformity assessment body auditing the timestamping services.

This section sets out the general rules regarding ZIPPER's technical, organisational and procedural requirements. Zipper Services SRL has a data center, consisting of 2 containers, on a redundant architecture, high performance and availability of services, in a distributed structure.

The following are described the policies and procedures for ensuring the confidentiality of the data, the integrity and the availability of the documents archived in electronic form, throughout the legal period of their retention.

8.1.1 DOCUMENT ACCESS POLICY

The solution has appropriate mechanisms in place to detect data corruption or loss. There is an internal procedure for reporting all incidents of corruption or loss of data and the steps taken to restore or remove corrupted or lost data.

The solution has appropriate mechanisms in place to ensure the integrity of the archived documents. Integrity is defined as the absence of unintentional changes to the content of the archive, the necessary descriptive metadata remaining properly associated, the verification of the number of copies, the synchronization of the copies, the verification of the completeness of the archiving agreements, the validation of the audit traces for all accesses.

The solution has appropriate mechanisms in place to ensure the confidentiality and privacy of the stored information. All stored information will be obtained, stored and processed in accordance with the laws in force, in particular with the Romanian Law on the protection of personal data. There is a statement of Personal Data Protection Policy, which will be annexed to this document.

Access to the data will be consistent with the classification of the data, the group and the user's role. The regime of access to a document in electronic form, the modification and the term of its retention shall be established exclusively by the holder of the right to dispose of the documents.

The rights of each user are set at the customer, group and role level (access level), thus ensuring user access only to the documents and data of the customer to which the group belongs has access.

All users' passwords are kept encrypted in the RepoZip LTA system. A user account that has not been used for a period of 1 year is deactivated, requiring a reactivation request from the Beneficiary.

The Beneficiary is obliged to take all possible actions in order to protect the identification name and password necessary for the use of the services provided. The Beneficiary is responsible for any event or facts that occurred through the use of its identification name and access password, unless the event or action occurred for reasons that can be attributed to the Archivist.

The archiving app offers:
• proof of the existence of a document received, based on time
• Ensures data authentication/integrity
• Provides long-term archiving (so it must be able to ensure the validity of archived data and documents for the required archiving period, i.e. exceeding certificate expiration/revocation, timestamp expiration, and technological exceeding due to key and hash length or signing algorithms

8.1.2 POLICY ON CRYPTOGRAPHIC DEVICES USED

The holder of a cryptographic device must perform his duties and obligations responsibly in every possible situation.
The following elements are taken into account when developing the policy on cryptographic controls:
- how management approaches the use of cryptographic controls, including the general principles underlying the protection of business information;
- Key management approach, including methods for recovering encrypted information in case of loss, compromise or destruction of keys;
- roles and responsibilities for:
- implementation of the policy;
- key management;

A cryptographic device holder must notify its issuer in the event of theft, loss, unauthorized disclosure, or security compromise immediately after the incident.
A cryptographic device holder is not responsible for the failure to perform his/her duties/obligations due to reasons that are impossible for him to control.
The cryptographic device holder is responsible for neglecting its obligations to notify the issuer of the disclosure or breach of security as a result of its mistakes, negligence or irresponsibility.

8.1.3 POLICY ON MEANS OF CONTROL AND SECURITY OF DOCUMENTS AND DATABASE

The RepoZip LTA application ensures the control and security of access to the application by limiting access to:

- internal mesh Zipper
- the Beneficiary's network/IPs

Control and security of access to documents:
-It is secured, by indicating a username and password.
- The regime of access to a document in electronic form, the modification and the term of its retention are established exclusively by the holder of the right to dispose of the documents. The provider is obliged to comply with the regime of access to electronic documents.
-The rights of each user are set at the customer, group and role level (access level), thus ensuring user access only to the documents and data of the customer to which the group belongs has access.
- All users' passwords are kept encrypted in the RepoZip LTA system.
- A user account not used for a period of 1 year is deactivated, requiring a reactivation request from the Beneficiary.
- The Beneficiary is obliged to take all possible actions in order to protect the identification name and password necessary for the use of the services provided. The Beneficiary is responsible for any event or facts that occurred through the use of its identification name and access password, unless the event or action occurred for reasons that can be attributed to the Provider.

Control and security of access to the database
-At the request of the Beneficiary, there is also the possibility of using a separate virtual server exclusively for the client's application (a clone of the application and a database containing exclusively the client's data are used) for an increased level of security.
- Any access to the Beneficiary's database is recorded in an access file (called a log to automatic processing). Information regarding the addition, modification or deletion of the Beneficiary's business data is saved

User authentication
Any activity that can lead to actions on sensitive business data (e.g. download)
The log of a Log event will contain the following data: user id, timestamp and Operation type
The log will be available for consultation by users with rights in this regard.

9. Participants

9.1 Subscribers (beneficiary)

The subscriber/beneficiary is the applicant, the natural or legal person who requests the electronic archiving service and who enters into a contractual relationship with ZIPPER. The subscriber will be held directly liable if his obligations are not fulfilled correctly.

9.2 Parties

One party is the Subscriber, a natural or legal person who transmits a digital document to the electronic archive and the other party is the accredited archivist, who takes over the document and the metadata, according to the legislation in force.

The electronic archiving of documents is governed by the same rules as in the case of paper documents and is subject to the provisions of the archival legislation in force, with the following specifications:

a) the registration of documents in electronic form by the electronic archiving system certifies the official existence of those documents. The registration number uniquely identifies the document within the system. Once registered, the document cannot undergo any changes in content. At the same time as the registration, the electronic file of the document shall be completed, under the conditions of art. 8 para. (2) and (3) of Law no. 135/2007;
c) the electronic document management system automatically generates an audit record, in which all decisions and actions that occur on a document from the moment of registration until its destruction are recorded, without the possibility of being modified;
d) the documents and files archived in electronic form will be included in the Subscriber's archival nomenclature, specifying in the "Observations" section: "in electronic form".

9.3 Other participants

Not applicable.

10. Obligations and liability

This chapter includes all obligations, liabilities, warranties and liabilities of ZIPPER LTA, its subscribers and users (subscribers and relied parties). These obligations and responsibilities are governed by agreements accepted by all parties.

ZIPPER assumes responsibility for implementing the requirements of the "LTA Practices" section of this document, as well as the provisions of national law.

ZIPPER's agreements with subscribers and the parties they rely on describe each other's obligations and responsibilities, including financial responsibilities. The ZIPPER Policy and Practice Statement (this document) forms an integral part of these agreements.

a. LTA obligations and warranties towards subscribers

ZIPPER guarantees the availability of 99.5% of the 24/7 electronic archiving infrastructure and application, with the exception of scheduled technical breaks, in terms of equipment and system maintenance.

ZIPPER assumes the following obligations towards Subscribers:

- Operate in accordance with this ZIPPER LTA Policy and Practice Statement (this document) and other relevant operational policies and procedures;
- Ensure that the TSO maintains a minimum UTC time accuracy of ± 1 second;

- Maintaining a competent and experienced team that can ensure the continuity of the Infrastructure Services;
- Permanently ensuring the physical and logical security, as well as the integrity of the servers, software and databases necessary for the proper functioning of the electronic archiving services
- Monitors the entire LTA infrastructure to prevent or limit any disruption or unavailability of services
- Undergoes internal and external reviews/audits to ensure compliance with relevant legislation and ZIPPER's internal policies and procedures;
- Provides high-availability access to ZIPPER LTA systems, except for planned technical outages and loss of time synchronization.

b. Subscribers' rights

The beneficiary subscribers have the following rights:
a) establishing the regime of access to the archived document, as well as its modification, under the conditions of art. 14 of Law no. 135/2007;
b) the attestation of the original or copy value of the archived document;
c) online access to the electronic register of the electronic archive;
d) online access to the electronic file attached to each document entered into the electronic archive, according to the established access regime;
e) Online access to archived documents that do not have public access and to their electronic files is considered ensured when the persons who have the right of access to documents and to
Their electronic files can be consulted through a private network (which is not connected to the Internet). The written consent of the beneficiary regarding the use of that network is required.

Subscribers should verify the data package archived by ZIPPER LTA.

This check includes:

- Check that the data package contains the original archived document, the electronic record of the document and the signature validation report, countersigned by the archivist
- Verification of the archivist's certificate:
    - Verification of the trust path up to the trusted root certificate and for each of the certificates in the chain (including the certificate with which it is signed)
    - Verify that the certificate is not expired at the time of signing
    - Check that the certificate has not been revoked at the time of signing

Other obligations of the Subscriber may also be defined in the ZIPPER Terms and Conditions for Electronic Archiving Services.

c. Zipper's liability

The liability of ZIPPER acting as administrator of the archive for its subscribers is specified in the agreement between the parties or is that provided for in applicable law.

ZIPPER is liable for any damages caused directly, intentionally or negligently, to any person or entity, as a result of the failure to comply with the obligations set forth herein.

ZIPPER's terms and conditions for electronic archiving services limit ZIPPER's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include a liability ceiling on ZIPPER's combined aggregate liability to any and all persons in respect of electronic archiving services, which is limited to an amount not exceeding that of that contract for the timestamping service and a total maximum of €300,000, regardless of the nature and type of liability, the value or extent of any damage suffered.

ZIPPER LTA is in no way responsible for the fraudulent use of the service.

11. Statement of good practice

11.1 Infrastructure management and operation

i. Security Management

ZIPPER ensures that appropriate administrative and management procedures are in place that correspond to recognised best practices.
ZIPPER performs all EE functions using reliable systems that meet the requirements of ZIPPER ISMS.

ii. Asset classification and management

ZIPPER maintains an inventory of all assets and assigns a classification of protection requirements to those assets in accordance with risk analysis.

iii. Staff security

ZIPPER maintains adequate personnel controls that meet the best security practices and requirements of the relevant standards.
Management and operational staff have the appropriate skills and knowledge on timestamping, digital signatures and trust services, as well as security procedures for staff with security responsibilities, information security and risk assessment.
ZIPPER implements the Trust Roles Policy for all those employees who have access to or control cryptographic operations. Trusted people and roles include, but are not limited to:

- Crypto Business Operations Staff,
- Security personnel,
- system administration staff;
- Designated engineering personnel and
- Directors who are assigned to manage the credibility of the infrastructure.

Prior to entering a trust role, ZIPPER conducts background checks which may include, as a guideline, the following:

- Identity verification
- Verification of previous employment and professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Verification that there is no criminal conviction;
- Verification of financial records.

ZIPPER requires that personnel wishing to become trusted persons provide evidence of the training, qualifications and experience necessary to competently perform their future job responsibilities as specified in the employment contract and job description, before performing any operational or security functions.
Employment contracts signed by employees include confidentiality provisions for information brought to their attention during their performance.
ZIPPER ensures that staff have achieved trust status and that departmental approval has been granted before these staff have been:

- Issued access devices and granted access to the necessary facilities;
- Issued electronic credentials to access and perform specific functions on ZIPPER LTA or other IT systems.

User accounts are created for personnel with specific roles that require access to the system in question. All users must log in with a dedicated account, and administrative commands are only available with explicit permission. File system permissions and other features available in the operating system security model are used to prevent any further use. User accounts are locked out as soon as possible when the role change dictates.

11.2 Physical and environmental security

ZIPPER implements the Physical Security Policy, which supports the security requirements of this LTA policy and practice statement.

ZIPPER LTA operations are conducted in a physically protected environment that discourages, prevents, and detects the unauthorized use, access to, or disclosure of sensitive information and systems.

ZIPPER also maintains disaster recovery facilities for its electronic archiving service operations. ZIPPER's disaster recovery facilities are protected by several levels of physical security comparable to those of the primary ZIPPER installation.

The physical security system includes layers for key management security, which serves to protect the online and offline storage of the cryptographic signing unit (OSC) and keying materials.

The areas used for the creation and storage of cryptographic materials require access control. Access to CSOs and key materials is restricted in accordance with segregation of duties requirements. The opening and closing of cabinets or containers on these levels is recorded for audit purposes.

ZIPPER's operations are protected through physical access controls, making them accessible only to duly authorized individuals. Access to secure areas of buildings requires the use of an 'access' card and/or biometrics. The use of the access card is recorded by the building's security system.

Access card logs are reviewed regularly.

Secure zipper facilities are equipped with primary and backup:

- Power supply systems to ensure continuous and uninterrupted access to electricity and
- Heating/ventilation/air conditioning systems for controlling temperature and relative humidity.

ZIPPER has taken reasonable precautions to minimize the impact of water exposure to its facilities, as well as to prevent and extinguish fires or other harmful exposures to flame or smoke.

All media containing production and data software, audit, archive or backup information is stored in zipper facilities or secure off-site storage facilities with appropriate physical and logical access controls designed to limit access by authorized personnel and protect these media from accidental damage.

ZIPPER securely stores all removable media and paper containing sensitive information related to its operations in secure containers. Sensitive documents and materials are shredded before disposal. The media used to collect or transmit sensitive information becomes unreadable before disposal. Cryptographic devices are physically destroyed before removal.

11.3 Operations management

ZIPPER LTA ensures that procedures, processes and infrastructure must comply with operational management, security procedural requirements, system access management, reliable system deployment and maintenance, business continuity management and incident management as defined in ETSI EN 319 421.

The operations management procedures for the ZIPPER LTA are incorporated into the general procedures for managing ZIPPER's internal operations.

12. Compromise of LTA services

Zipper has developed procedures to manage the continuity of its operations. In case of service interruptions, it strives to minimize these interruptions so as not to affect the activity of the client/client. Zipper has created and maintains a disaster continuity plan. In the event of a disaster, including the compromise of a private signing key, operations are resumed within the deadline set out in the continuity plan. The causes of the disaster are taken into account and reasonable measures are determined to eliminate the cause of the interruption of the process, as well as measures to prevent such disasters in the future.

The company has created, documented, implemented and maintained plans, procedures and control mechanisms in accordance with the international standard ISO 22301 to ensure the necessary level of business continuity and continuity of information security in adverse cases.

Zipper provides:

a) an appropriate management structure available to prepare, mitigate and respond to a destructive event, using staff with the necessary authorities, experience and competence;

b) developing and approving response and recovery plans and procedures that describe in detail how the company will handle a destructive event and maintain continuity of information security;

c) information security control mechanisms within procedures and systems and tools to maintain disaster continuity and recovery;

d) compensatory mechanisms for controlling information security control mechanisms that cannot be maintained in an adverse event.

The continuity plan includes the backup of critical systems. The backup is stored in the two locations, which are 300 km away geographically. The special conditions comply with the applicable standards, recommendations and regulations in the field of information security. The Company verifies any mechanisms created to control the continuity of information security at regular intervals, so that it can ensure their effect and effectiveness in unfavorable cases. Zipper regularly backs up important information and software and guarantees that all basic information and software can be recovered after a disaster or in the event of loss of archive. The recovery mechanisms are checked regularly, so that it can be guaranteed that they meet the requirements of the work continuity plan.

Storage for business recovery in the event of an incident or disaster is maintained and stored in safe and secure locations. Zipper has the obligation to inform subscribers and any third parties about incidents occurring in the service provision activity.

13. Termination of the archiving service in the data center

The LTA ends:

- with a decision of the Board of Directors of ZIPPER;
- by a decision of the authority exercising the supervision of timestamping services;
- with a court decision;
- upon the liquidation or cessation of ZIPPER operations.

ZIPPER ensures that potential disruption to subscribers and parties is minimised as a result of the termination of ZIPPER's services and, in particular, ensures that the information necessary to verify the correctness of the services is continuously maintained.

If it is necessary for ZIPPER LTA to cease operation, ZIPPER shall use commercially reasonable efforts to notify Subscribers and reliant parties of such termination prior to termination of the LTA.

13.1 Preservation of evidence of the electronic archiving service

- ✓ The retention period of the collected samples is in accordance with national legislation and is in accordance with the recommendations of ETSI TS 119 312;
- ✓ The confidentiality and integrity of current and archived records of the operation of the Service are maintained and archived in accordance with Zipper's business practice;
- ✓ The time used to record events, as required in the log log, is synchronized with UTC at least once a day;
- ✓ Events are recorded in a way that cannot be easily deleted or destroyed;
- ✓ The same preservation profile applies throughout the sample preservation period;
- ✓ The validity period of the samples is extended by using secure and reliable cryptographic algorithms;
- ✓ The evidence format in this policy complies with the requirements of IETF RFC 6283, as well as CAdES ETSI EN 319 122, XAdES ETSI EN 319 132, and PAdES ETSI EN 319 142.

If necessary, Zipper extends the validity of the evidence to the archive. During the archiving period, the archiving service checks whether the evidence can be used to achieve the appropriate preservation purpose. This can be threatened if the cryptographic algorithm can no longer be trusted or the archive

administrator's certificate is revoked. In such cases, Zipper expands the evidence before it can be used to achieve the purpose of archiving.

14. Organizational reliability

ZIPPER LTA ensures that its organization is reliable in accordance with ETSI EN 319 421. ZIPPER has the financial stability and resources to operate in accordance with this Policy and Practice Statement.