APROBAT

GUVERNANȚA PMO
DORU VIJIIANU
JUDIT FEKETE
MIRELA OJOG

VIJIIANU DORU-IOAN Digitally signed by VIJIIANU DORU-IOAN Date: 2026.10.09 13:26:06 +03'00'

FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2026.10.09 17:40:53 +03'00'

MIRELA OJOG
09/10/2026 13:37:09 UTC+0300

Signed with NamirialSign

-Autoritatea Zipper Services-
Servicii calificate de arhivare electronică
Politică și cod de practică și proceduri

POLITICA ESTE PROPRIETATEA ZIPPER SERVICES S.R.L.
COPIEREA NEAUTORIZATĂ NU ESTE PERMISĂ

.

Istoricul edițiilor			
Ediție	**Data și descrierea modificării**	**Pregătit**	**Aprobat**
1	28.02.2019 – Prima ediție	Mirela Ojog	Judit Fekete
2	06.02.2021 – Ediția 2	Mirela Ojog	Judit Fekete
3	06.02.2021 – Ediția 3	Mirela Ojog	Judit Fekete
4	10.05.2025 – Ediția 4	Mirela Ojog	Judit Fekete
5	30.09.2025 - Ediția 5 – Corelația cu Serviciul de Conservare și CEN/TS 18170	Judit Fekete	Mirela Ojog
6	10.06.2026 – Editia 6 – actualizare conform Decizie nr. 162/2026	Judit Fekete	Mirela Ojog
7	03.09.2026 – Editia 7 - actualizarea normelor legale aplicabile in Romania	Mirela Ojog	Judit Fekete
8	01.10.2026 – Editia 8 - actualizare cadru legal aplicabil	Mirela Ojog	Judit Fekete

ZIPPER

Cuprins

1. INTRODUCERE 4
2. ADMINISTRAREA POLITICILOR 5
3. PROCEDURA DE APROBARE 6
4. REFERINTE 6
5. DENUMIREA ȘI IDENTIFICATORUL DOCUMENTULUI 7
6. CONCEPTE GENERALE 12
6.1 PROCESUL DE FURNIZARE A SERVICIILOR 14
6.1.1 DOVEZI DE ARHIVARE ELECTRONICA 15
6.1.1.1 DOVADA PRIMIRII 15
6.1.1.2 DOVADA DEPOZITARII 15
6.1.1.3 DOVADA RECUPERARII 16
6.1.1.4 DOVADA ȘTERGERII 16
6.1.2 INTEGRITATEA DATELOR 17
6.1.3 CONFIDENȚIALITATEA DATELOR ȘI CONTROLUL ACCESULUI 17
6.1.4 CONSERVARE PE TERMEN LUNG (DURABILITATE) 17
6.1.5 DISPONIBILITATE 17
6.1.6 AUTENTICITATE 18
6.1.7 NEREPUDIERE 18
6.1.8 PROPRIETARUL DOCUMENTULUI ÎN FORMAT ELECTRONIC 18
6.1.9 METADATE DOCUMENTE 19
6.1.9.1 PACHETE DE INFORMAȚII — FORMATUL PACHETULUI DE INFORMAȚII 20
6.1.10 DEPUNEREA TRANSFERULUI 20
6.2 AUDIT ȘI TRASABILITATE 21
6.3 MASURI DE SECURITATE 21
6.4 PROCEDURI OPERAȚIONALE 21
7. DECLARAȚIE DE PRACTICA LEGATA DE SERVICIUL DE ARHIVARE ELECTRONICA OFERIT DE ZIPPER 21
8. CENTRUL DE DATE UTILIZAT DE ARHIVA ELECTRONICA 27
CENTRELE DE DATE INDEPLINESC URMATOARELE CONDIȚII: 27
8.1 POLITICA CENTRULUI DE DATE 27
8.1.1 POLITICA DE ACCES LA DOCUMENTE 28
8.1.2 POLITICA PRIVIND DISPOZITIVELE CRIPTOGRAFICE UTILIZATE 29

8.1.3 POLITICA PRIVIND MIJLOACELE DE CONTROL ȘI SECURITATE A DOCUMENTELOR ȘI A BAZELOR DE DATE 29

9. PARTICIPANTII 30

9.1 ABONAȚI (BENEFICIAR) 30

9.2 PARTI 30

9.3 ALȚI PARTICIPANȚI 31

10. OBLIGAȚII ȘI RASPUNDERE 31

UN. OBLIGAȚII ȘI GARANȚII LTA FAȚA DE ABONAȚI 31

B. DREPTURILE ABONAȚILOR 32

C. RASPUNDEREA ZIPPER 32

11. DECLARAȚIE DE BUNE PRACTICI 33

11.1 MANAGEMENTUL ȘI OPERAREA INFRASTRUCTURII 33

EU. MANAGEMENTUL SECURITAȚII 33

II. CLASIFICAREA ȘI GESTIONAREA ACTIVELOR 33

III. SECURITATEA PERSONALULUI 33

11.2 SECURITATEA FIZICA ȘI DE MEDIU 34

11.3 MANAGEMENTUL OPERAȚIUNILOR 35

12. COMPROMITEREA SERVICIILOR LTA 35

13. ÎNCETAREA SERVICIULUI DE ARHIVARE IN CENTRUL DE DATE 36

13.1 PASTRAREA PROBELOR SERVICIULUI DE ARHIVARE ELECTRONICA 36

14. FIABILITATE ORGANIZAȚIONALA 37

1. Introducere

Acest document constituie Politica și Codul de practică și proceduri ale autorității Zipper Services (denumită în continuare Zipper). Scopul documentului este de a descrie regulile și procedurile operaționale adoptate de ZIPPER pentru furnizarea serviciilor de arhivare electronică, în centrul de date Zipper Services.

Acest document este pus la dispoziția publicului la
https://pki.ca.ezipper.ro/repository/policies.php

Cerințele tehnice și de securitate pe care le îndeplinește sistemul de arhivare electronică sunt descrise în Planul de securitate specific sistemului de arhivare electronică, considerat anexă la prezentul document.

Centrul de date îndeplinește toate condițiile cerute de legislația în vigoare pentru a efectua operațiuni de arhivare electronică.

Conducerea poate face excepții de la acest document de la caz la caz pentru a atenua impactul semnificativ și iminent asupra clienților, partenerilor, părților care se bazează și/sau altor persoane în absența unor soluții practice. Orice astfel de excepții de gestionare sunt documentate, urmărite și raportate ca parte a procesului de audit.

În aplicarea prezentei Politici, Zipper Services se conformează cerințelor privind arhivarea electronică calificată prevăzute de Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (eIDAS 2.0, art. 45j), de Regulamentul de punere în aplicare (UE) 2025/2532 privind standardele de referință și specificațiile pentru serviciile calificate de arhivare electronică si Regulamentul de punere in aplicare (UE) 2025/2530 al Comisiei din 16 decembrie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European si al Consiliului in ceea ce priveste cerintele aplicabile prestatorilor de servicii de incredere calificati care presteaza servicii de incredere calificate..

În acest sens, Zipper Services respectă obligațiile referitoare la documentația de notificare și raportul de evaluare a conformității, menținerea și operarea registrului electronic al arhivei, implementarea mecanismelor de conservare pe termen lung (LTP) pentru menținerea valorii probatorii și verificabilității semnăturilor și sigiliilor electronice pe întreaga durată de păstrare, precum și toate măsurile de securitate, trasabilitate și păstrare stabilite de Regulamentul (UE) nr. 910/2014 astfel cum a fost modificat prin Regulamentul (UE) 2024/1183, de Regulamentul de punere în aplicare (UE) 2025/2532 privind standardele de referință și specificațiile pentru serviciile calificate de arhivare electronică si Regulamentul de punere in aplicare (UE) 2025/2530 al Comisiei din 16 decembrie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European si al Consiliului in ceea ce priveste cerintele aplicabile prestatorilor de servicii de incredere calificati care presteaza servicii de incredere calificate.Sistemul de arhivare electronică utilizat de Zipper Services pentru prestarea serviciului de arhivare electronică calificată este avizat tehnic de Autoritatea pentru Digitalizarea României (ADR).

Serviciul de arhivare electronică calificată este proiectat și operat astfel încât să asigure conservarea pe termen lung (LTP) a documentelor electronice, prin implementarea de măsuri tehnice și

organizatorice care garantează, pe întreaga durată legală sau contractuală de păstrare:

a) menținerea verificabilității semnăturilor electronice și a sigiliilor electronice aplicate documentelor arhivate;

b) păstrarea valorii probatorii a documentelor, inclusiv prin menținerea integrității și autenticității acestora;

c) protecția împotriva degradării tehnologice a formatelor, algoritmilor criptografici și certificatelor utilizate.

Sistemul de arhivare electronică implementat de Zipper Services permite validarea continuă a semnăturilor electronice și a sigiliilor electronice asociate documentelor arhivate, inclusiv după expirarea sau revocarea certificatelor aferente, prin utilizarea de mecanisme de revalidare, conservare pe termen lung și marcare temporală calificată, în conformitate cu Regulamentul (UE) nr. 910/2014 astfel cum a fost modificat de Regulamentul (UE) 2024/1183 și cu normele de punere în aplicare incidente.

Zipper Services asigură, în condițiile legii, accesul autorităților competente, inclusiv al ADR, la sistemul de arhivare electronică, în vederea efectuării de audituri, verificări tehnice, testări ale fluxurilor operaționale și evaluări ale controalelor de securitate, potrivit procedurilor de acreditare a administratorilor de arhivă electronică și de avizare a sistemelor electronice de arhivare prevăzute in cerintele legale aplicabile.

Sistemul de arhivare electronică respectă cerințele de securitate, integritate, trasabilitate și confidențialitate aplicabile serviciilor de încredere calificate, inclusiv prin:

a) păstrarea și protejarea jurnalelor de audit și a evidențelor privind accesul, operațiunile efectuate asupra documentelor și modificările permise;

b) implementarea de mecanisme de control al accesului, autentificare, autorizare și segregare a rolurilor;

c) asigurarea integrității și disponibilității datelor arhivate;.

Serviciul de arhivare electronică calificată furnizat de Zipper Services face parte integrantă din categoria serviciilor de încredere reglementate de Regulamentul (UE) nr. 910/2014 (eIDAS) astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 și este supus regimului de supraveghere, avizare, suspendare și retragere exercitat de ADR..

2. Administrarea politicilor

Serviciul de arhivare electronică este oferit de Zipper Services în infrastructura Centrului de Date

Organizația care administrează acest document:
ZIPPER SERVICES SRL
Str. Rene Jeannel, nr. 8, Imobil Novis Plaza, corp A, et. 2, 400285, Cluj-Napoca, RO
Cluj-Napoca, 400285, România

Punct de lucru:
Bd. 1 Decembrie 1918 nr. 1G,
Sector 3, București, 032451, România

Punct de lucru:
Strada Nikola Tesla, nr. 2, cod 400221, jud. Cluj
Cluj-Napoca, 400285, România
https://ezipper.ro/
E-mail: office@ezipper.ro

Telefon +40 21.340.4638 / +40 31.101.1020
Fax: +40 21.340.4636 / +40 31.101.1022
(Luni-Vineri 09.00. – 18:00 ora Europei de Est)
Contact: pki@ezipper.ro Echipa de Management al Politicilor

3. Procedura de aprobare

Aprobarea acestui document și modificările ulterioare sunt făcute de persoanele dedicate Zipper. Aceste persoane alcătuiesc echipa de management al politicilor. Membrii PMG Governance aprobă noi versiuni ale acestui document. Versiunile modificate înlocuiesc orice prevederi contradictorii ale versiunilor anterioare ale prezentului document.

4. Referinţe

Legislația națională aplicabilă:

1. Ordinul nr. 102/2026 privind aprobarea Procedurii de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificate, a Procedurii de înregistrare și radiere a prestatorilor de servicii de încredere necalificate în Registrul prestatorilor de servicii de încredere necalificate, a Procedurii de înregistrare și radiere a prestatorilor de servicii de încredere necalificate din domeniul apărării, ordinii publice și siguranței naționale în Registrul prestatorilor de servicii de încredere necalificate, a Procedurii de supraveghere, control și sancționare a prestatorilor de servicii de încredere, precum și a Normelor de aprobare a mecanismelor de validare.

Următoarele referințe conțin prevederi care sunt relevante pentru politica centrelor de date ZIPPER și serviciul de arhivare electronică:

2. REGULAMENTUL (UE) nr. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE [1];

3. Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală.

4. Regulamentul de punere în aplicare (UE) 2025/2532 al Comisiei din 16 decembrie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește standardele de referință și specificațiile privind serviciile calificate de arhivare electronică

5. Regulamentul de punere in aplicare (UE) 2025/2530 al Comisiei din 16 decembrie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European si al Consiliului in ceea ce priveste cerintele aplicabile prestatorilor de servicii de incredere calificati care presteaza servicii de incredere calificate

6. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

8. ETSI EN 319 401 Semnături electronice și infrastructuri (ESI); cerințe generale de politică pentru furnizorii de servicii de încredere;

9. ISO 14641:2018 – Managementul documentelor electronice – Proiectarea si operarea unui sistem informatic pentru pastrarea documentelor electronice – Specificatii.

10.ISO 14721:2025 – Practici privind sistemele de date spatiale – Model de referinta pentru un sistem deschis de arhivare a informatiilor (OAIS).

11.CEN/TS 18170:2025 – Cerinte functionale pentru serviciile de arhivare electronica.

12.ETSI EN 301 549 – Cerinte de accesibilitate pentru produsele si serviciile TIC.

13.ETSI TS 119 511 – Semnaturi electronice si infrastructuri de incredere (ESI) – Cerinte de politica si de securitate pentru prestatorii de servicii de incredere care furnizeaza servicii de pastrare pe termen lung a semnaturilor digitale sau a datelor generale utilizand tehnici de semnatura digitala.

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

5. DENUMIREA ȘI IDENTIFICATORUL DOCUMENTULUI

Numele complet al acestui document este "Serviciu de arhivare calificat (QAS) "Politică, cod de practică și proceduri (PCPP)" și identificator de obiect (OID):

Denumirea documentului	Identificator de obiect (OID)
Arhivare calificată (QAS) - Politică, cod de practică și proceduri (PCPP)	**1.3.6.1.4.1.57570.4.4.2** 4=> nod de clasificare a serviciului 4 => servicii de arhivare (subarbore al politicilor legate de conservare) 2=> **variantă de arhivare** calificată

6. Definiții și abrevieri

6.1 Termeni generali și definiții

a) **centru de date** - un spațiu securizat, dotat cu tehnologie de calcul și echipamente de comunicații prin care sunt recepționate, stocate și transmise datele în formă electronică;

b) **beneficiar - titular al dreptului de a dispune de document** care depozitează spre păstrare documentele în format electronic într-o arhivă electronică;

c) **acreditare** - constatarea de către A.D.R. a îndeplinirii condițiilor legale pentru dobândirea calității de administrator al arhivei electronice;

d) **Audit IT** - activitatea de colectare și evaluare a probelor pentru a determina dacă sistemul IT respectă parametrii de performanță și de lucru conform cerințelor de proiectare, dacă asigură funcționalitățile necesare cerințelor de business și respectării legislației în domeniu, dacă este securizat, dacă menține integritatea datelor prelucrate și stocate, dacă permite atingerea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;

e) **Auditor IT** - persoana fizică autorizată care deține un certificat de auditor IT sau persoana juridică cu personal certificat care desfășoară o activitate de audit al sistemelor informatice, conform reglementări și bune practici în domeniu;

f) **Raport de audit IT** - instrumentul prin care se comunică scopul auditului, obiectivele urmărite, normele/standardele aplicate, perioada parcursă, natura, procedurile, constatările și concluziile auditului, precum și orice rezerve pe care auditorul IT le are cu privire la sistemul informatic auditat;

g) **prestator de servicii de asigurare a increderii calificat** - conform art. 3 pct. 20 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat de Regulamentul (UE) 2024/1183;

h) **backup** - activitatea de copiere a fișierelor sau bazelor de date în vederea păstrării și recuperării acestora în caz de deteriorare sau alt eveniment neprevăzut;

i) **Container de date:** un obiect de date care conține un set de obiecte de date și informații suplimentare care descriu obiectele de date conținute și, opțional, conținutul și relațiile dintre acestea (semnături/sigilii digitale, marcaje temporale, înregistrări de dovezi, date de validare etc.);

j) **Autoritate UE calificată de marcare temporală**: un furnizor de servicii de asigurare a încrederii calificat care emite marcaje temporale electronice calificate, astfel cum se prevede în Regulamentul (UE) nr. 910/2014 astfel cum a fost modificat de Regulamentul (UE) 2024/1183;

k) **înregistrarea dovezilor**: date care pot fi utilizate pentru a dovedi existența unui obiect de date arhivat sau a unui grup de obiecte de date arhivate la un moment dat;

l) **Nomenclator (bazat pe legislația română de arhivare Ordinul de zi nr. 217 din 23 mai 1996)**

Nomenclatura se întocmește sub forma unui tabel în care sunt înscrise categoriile de documente grupate pe numere și perioade de păstrare, pe compartimente de lucru.

A patra casetă a nomenclatorului indică perioada de **păstrare**. Înființarea acestuia se face ținând cont de legile în vigoare (contabilitate, GDPR, altele), de importanța practică pentru activitatea creatorului documentelor și, în special, de importanța științifică a informațiilor pe

care le conțin documentele. Cuvântul "permanent" este folosit lângă grupurile de documente care sunt păstrate permanent, iar pentru cele care sunt păstrate temporar, cifra arabă reprezentând numărul de ani/lună în care sunt păstrate. Articolul 12. - Nomenclatura fișierelor nu este modificată anual, ci numai atunci când apar modificări în structura creatorului documentului. În cazul în care se înființează noi departamente de lucru sau subdiviziuni, nomenclatorul este completat cu numele acestora și cu fișierele nou create. În cazul departamentelor de lucru sau al subdiviziunilor acestora care își desfășoară activitatea prin crearea altor grupuri de documente decât cele prevăzute inițial, nomenclatorul se completează cu noile dosare.

14. - Nomenclatorul este aprobat de conducerea unității de creare documentară și este confirmat, la nivel central, de ***Arhivele Naționale*** și, la nivel local, de direcțiile județene ale Arhivelor Naționale.

m) **pe termen lung**: o perioadă lungă de timp în care schimbările tehnologice, cum ar fi uzura morală a tehnologiei criptografice, a algoritmilor criptografici, a dimensiunilor cheilor sau a funcțiilor hash, compromisurile esențiale sau capacitatea de a verifica starea de valabilitate a certificatelor pot fi un motiv de îngrijorare;

n) **conservarea pe termen lung**: conservarea pe termen lung (cu sau fără stocare), în care prelungirea valabilității unei semnături digitale și/sau furnizarea de dovezi ale existenței datelor pe o perioadă lungă de timp nu depinde de uzura morală a tehnologiei criptografice, a algoritmilor criptografici, a dimensiunilor cheilor sau a funcțiilor hash, de compromiterea cheilor sau de capacitatea de a verifica starea de valabilitate a certificatelor;

o) **container de obiecte de conservare:** un container de fișiere pentru păstrarea obiectelor de date, de exemplu, ASiC-S, ASiC-E

p) **"identificator al obiectului de păstrare" înseamnă** un identificator unic al unui obiect de reținere/arhivare;

q) **semnătură electronică calificată** - în conformitate cu articolul 3 alineatul (12) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat de Regulamentul (UE) 2024/1183

r) **semnătură electronică avansată –** semnătură electronică ce îndeplineşte cerinţele prevăzute la art. 26 din Regulamentul (UE) nr. 910/2014 astfel cum a fost modificat de Regulamentul (UE) 2024/1183

s) **marcaj temporal calificat** – marcaj temporal electronic calificat în conformitate cu articolul 3 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat de Regulamentul (UE) 2024/1183;

t) **nomenclatorul arhivistic** - instrument de lucru utilizat în domeniul arhivistic, care este elaborat de fiecare creator pentru organizarea și gestionarea documentelor proprii, în conformitate cu prevederile Legii Arhivelor Naționale nr. 16/1996, republicată, cu modificările și completările ulterioare;

u) **Serviciul de încredere de arhivare electronică -** serviciu care asigură primirea, stocarea, extragerea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, astfel încât să se păstreze integritatea, confidențialitatea și dovada originii acestora pe toată perioada de păstrare

v) **Serviciu de încredere de arhivare electronică calificat** - Serviciu de încredere de arhivare electronică furnizat de un furnizor de servicii de încredere de arhivare electronică calificat pentru a îndeplini cerințe suplimentare și care face obiectul unei evaluări periodice independente a conformității de către organisme acreditate de evaluare a conformității

w) **furnizor de servicii de asigurare a încrederii pentru arhivare electronică** - persoană fizică sau juridică care furnizează servicii de asigurare a încrederii pentru arhivare electronică

x) **păstrarea calificată pe termen lung** - serviciu calificat pentru păstrarea semnăturilor electronice calificate conform art. 34 alin. (1) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat de Regulamentul (UE) 2024/1183;

y) **certificat calificat** – certificat calificat pentru semnătură electronică în conformitate cu articolul 3 alineatul (15) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, astfel cum a fost modificat de Regulamentul (UE) 2024/1183;

z) **jurnal de audit** - un registru în care sunt înregistrate toate acțiunile întreprinse asupra datelor și/sau documentelor în format electronic sau asupra sistemului propriu-zis, inclusiv informații precum data și ora acțiunii, utilizatorul implicat, tipul de acțiune (creare, modificare, ștergere etc.), precum și orice alte detalii relevante;

aa) **Politica de acces pentru o arhivă electronică** - un set formal de reguli și proceduri stabilite pentru a controla și gestiona accesul la informațiile și documentele stocate în format electronic într-o arhivă. Această politică are scopul de a se asigura că numai persoanele autorizate au acces la datele și documentele stocate în arhivă și că securitatea și integritatea acestora sunt protejate în mod adecvat;

bb) **politica de securitate pentru o arhivă electronică** - specificarea măsurilor de securitate necesare pentru a proteja informațiile stocate în arhivă împotriva accesului, alterării sau distrugerii neautorizate (poate include criptarea datelor, implementarea unor politici stricte de gestionare a parolelor, monitorizarea accesului etc.);

cc) **Politica de păstrare a documentelor electronice** – stabilirea regulilor și procedurilor pentru păstrarea și gestionarea pe termen lung a arhivelor, inclusiv definirea perioadelor de păstrare și eliminare a documentelor în conformitate cu reglementările și politicile administratorului arhivei

6.2 Termeni referitori la obiectele digitale

a) **obiect digital:** obiect compus dintr-un set de secvențe de biți, Datele electronice și documentele electronice sunt obiecte digitale [SURSA ISO 14721]

b) **pachet de informații -** container de obiecte digitale și informații suplimentare pentru a face atât obiectele, cât și pachetul ușor de înțeles și utilizabil. Informațiile suplimentare includ: informații despre ambalaj, informații despre reprezentare și informații despre descriptorul de conservare. Pachetul de informații poate fi citit automat.

c) **informații privind structurarea și împachetarea datelor -** informații care descriu modul în care componentele unui pachet de informații sunt legate logic sau fizic între ele și cum să identifice și să extragă componentele

d) **informații de descriere a conservării -** informații necesare pentru conservarea adecvată a obiectului digital (informații de context, informații de referință, informații de fixitate și informații de control al accesului)

e) **Pachet de informații de depunere -** Pachet de informații care este livrat de abonat Serviciului de încredere de arhivare electronică pentru crearea sau actualizarea unuia sau mai multor pachete de informații de arhivare

f) **pachet de informații de arhivare -** pachet de informații care este arhivat în cadrul unui serviciu de încredere de arhivare electronică

g) **Pachet de informații privind diseminarea** - Pachet informativ, derivat din unul sau mai multe pachete de informații de arhivă și trimis ca răspuns la o solicitare

6.3 Termeni referitori la arhivarea electronică

a) **arhivare electronică -** procese efectuate pentru păstrarea obiectelor digitale disponibile, lizibile, interpretabile și fiabile atât timp cât este necesar. Obiectele digitale sunt de obicei stocate în pachete de informații. Gama de procese se aplică de la achiziția inițială a obiectelor digitale până la sfârșitul perioadei de conservare a acestora.

b) **Conservare -** act de păstrare a informațiilor privind orele suplimentare, ușor de înțeles independent de o comunitate desemnată și cu dovezi care să susțină autenticitatea acestora. În contextul păstrării semnăturilor electronice, a sigiliilor, a marcajelor temporale sau a certificatelor, ETSI EN 119 511 definește serviciul de păstrare ca fiind un serviciu capabil să

prelungească starea de valabilitate a unei semnături digitale pe perioade lungi de timp și/sau să furnizeze dovada existenței datelor pe perioade lungi de timp.

c) **perioada de conservare -** perioadă definită în care un serviciu de încredere de arhivare electronică asigură arhivarea obiectelor digitale
d) **transfer -** proces tehnic și organizatoric de returnare a obiectelor digitale arhivate către abonat sau către o altă entitate autorizată de abonat
e) **conversia formatului -** procesul de schimbare a fișierelor incluse într-un obiect digital dintr-un format în altul
f) **Migrare media -** transferul de informații de la o medie la alta fără a schimba secvența de biți

6.4 Abrevieri

Termeni prescurtați	Termeni
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
Collibri RepoZIP LTA	Aplicația Zipper Archiving, înregistrată în Registrul Român al sistemelor de arhivare electronică https://www.adr.gov.ro/arhivare-electronica/
Collibri	Sistem de management operațional al documentelor apartinand Zipper

6. Concepte generale

"Arhivare electronică" înseamnă un serviciu care asigură primirea, stocarea, extragerea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a le păstra integritatea, confidențialitatea și dovada originii pe toată perioada de păstrare.

Acest document descrie funcționalitatea serviciului de arhivare electronică și se aplică datelor electronice și documentelor electronice create în formă electronică, precum și documentelor pe suport de hârtie care au fost scanate și digitalizate.

Pe baza **articolului 45j din eIDAS 2.0** , serviciile de arhivare calificate trebuie să îndeplinească următoarele cerințe:

(a) sunt furnizate de prestatori de servicii de asigurare a încrederii calificați;

(b) utilizează proceduri și tehnologii capabile să asigure durabilitatea și lizibilitatea

datele și documentele electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținând în același timp integritatea și acuratețea originii lor;

(c) se asigură că aceste date electronice și documente electronice respective sunt păstrate astfel încât să fie protejate împotriva pierderii și *modificării, cu excepția modificărilor privind suportul sau formatul lor electronic;*

(d) permit părților autorizate care se bazează să primească în mod automat un raport care confirmă

că datele electronice și documentele electronice extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate a datelor de la începutul perioadei de păstrare până la momentul recuperării. Raportul este furnizat într-un mod fiabil și eficient și poartă semnătura electronică calificată sau sigiliul electronic calificat al furnizorului serviciului de arhivare electronică calificat.

Serviciul LTA este destinat utilizatorilor care au nevoie de păstrarea pe termen lung a documentelor lor electronice semnate cu semnătură electronică avansată/calificată. Înregistrarea documentelor în formă electronică de către sistemul de arhivare electronică atestă existența oficială a acestor documente. Numărul de înregistrare identifică în mod unic documentul din sistem. Odată înregistrat, documentul nu poate suferi modificări ale conținutului. Odată cu înregistrarea, dosarul electronic al documentului se completează.

Următoarele aspecte sunt, de asemenea, tratate în cadrul serviciului de arhivare:

1) Păstrarea pe termen lung folosind tehnici de semnătură electronică, capacitatea de a valida o semnătură electronică și capacitatea de a genera dovezi ale existenței datelor asociate semnăturii, în momentul introducerii unui document în arhivă, chiar dacă cheia de semnătură este compromisă ulterior, valabilitatea certificatului expiră sau există un atac criptografic al algoritmului de semnătură sau al algoritmului hash utilizat în semnătură;

2) Furnizarea de dovezi ale existenței obiectelor digitale, folosind tehnici de semnătură electronică (semnături electronice, marcaje temporale, înregistrări de probe etc.)

3) Păstrarea semnăturilor digitale (PDS) pentru perioade lungi de timp pentru a le menține valabilitatea

Toate aceste obiective necesită:

- Dovada integrității unui document electronic sau a unei semnături/sigilii;
- Dovada existenței unui document electronic sau a unei semnături/sigiliu la un moment dat/în trecut;
- Menținerea valabilității semnăturilor/sigiliilor electronice aplicate de arhivist pentru perioade lungi de timp;
- Disponibilitatea datelor.

Integritatea datelor este verificată în perioada de păstrare prin intermediul unei dovezi de integritate (hash, semnătură/sigiliu).

Dovada existenței indică faptul că obiectul digital a existat la un moment dat și este implementată prin

combinarea unei dovezi de integritate și a unei indicații de încredere a timpului (marcaj temporal calificat).

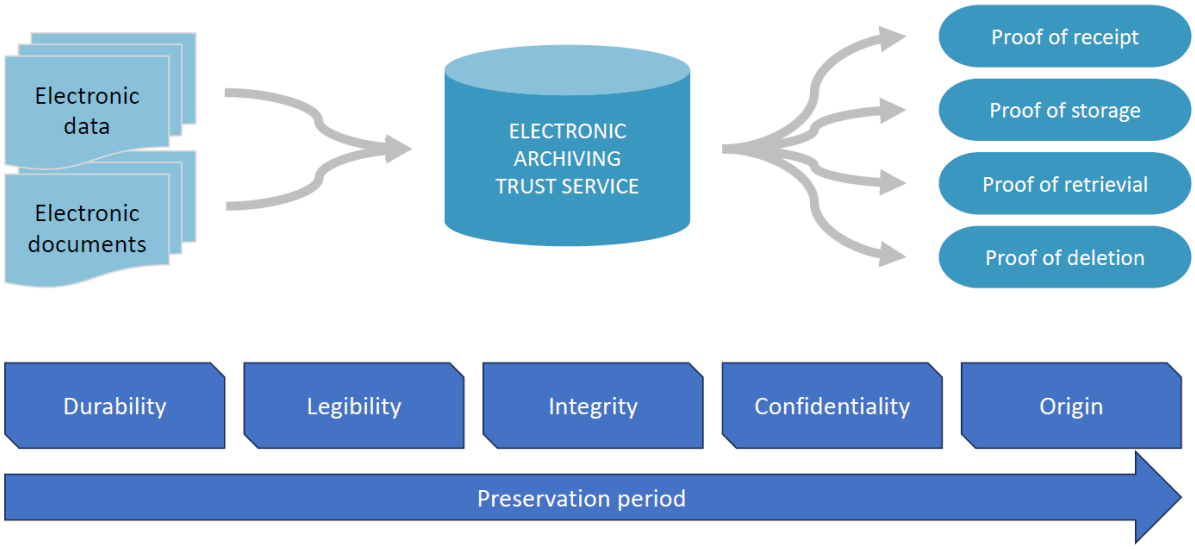
Pentru a menține starea de valabilitate a semnăturii/sigiliului electronic, trebuie păstrate și toate elementele necesare verificării valabilității și a căror disponibilitate nu poate fi garantată în viitor. Acestea pot include certificate, informații de revocare (CRL-uri, răspunsuri OCSP), liste de încredere etc.

În procesul de arhivare sunt utilizate servicii de marcare temporală calificate care utilizează protocolul de marcare temporală RFC 3161 prin transport HTTP. Serviciile calificate de marcare temporală asigură utilizarea unei surse de timp fiabile și gestionarea corectă a tuturor componentelor sistemului. De asemenea, sunt utilizate servicii calificate de validare a semnăturii/sigiliului.

6.1 Procesul de furnizare a serviciilor

Serviciul de arhivare calificat (QAS) Collibri RepoZIP LTA furnizat de Zipper QTSP utilizează proceduri și tehnologii pentru a asigura durabilitatea și lizibilitatea datelor electronice și a documentelor electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținând în același timp integritatea și acuratețea originii lor și sunt păstrate în așa fel încât să fie protejate împotriva pierderii și modificării*, cu excepția modificărilor privind suportul sau formatul electronic.*

Collibri RepoZIP LTA este aplicația de arhivare responsabilă pentru a oferi suport tehnic pentru fluxul de arhivare. Documentul care urmează să fie arhivat este ambalat într-un container digital împreună cu dovada de validare semnată că semnătura/sigiliul a fost validat, precum și alte metadate care detaliază procesul de arhivare, conform legislației românești. În pasul următor, containerul este criptat pentru a proteja integritatea. Criptarea are loc prin aplicarea unei semnături de arhivare pe termen lung (numită și semnătură la nivel LTA) cu furnizorul de marcaj temporal calificat Zipper. Modul Zipper de a crea și cripta containere se bazează pe profilul de bază ASiC (Associated Signature Container) pentru container și CMS Advanced Electronic Signature (CAdES) pentru criptare.



6.1.1 Dovezi de arhivare electronică

6.1.1.1 Dovada primirii

Primirea datelor în sistemul nostru de arhivare este confirmată prin mai multe măsuri tehnice și procedurale:

- Importul documentului declanșează crearea unui hash unic care este legat permanent de document, servind drept dovadă de primire.
- Sigiliul electronic calificat (nivel B-LTA) este aplicat pe conținutul obiectului de conservare (document importat, metadate și raport de validare semnat) și stocat în conformitate cu profilurile de **conservare specificate**
- Sistemul generează un **raport de validare** care certifică că documentul a fost primit corect în ceea ce privește semnăturile/sigiliile
- Un jurnal de audit înregistrează data și ora exactă a importului, operatorul care efectuează acțiunea și ID-ul unic al containerului de obiecte (ASIC-E), oferind o înregistrare inalterabilă a primirii
- Marcajul **temporal calificat** furnizat de Zipper TSA (Time-Stamping Authority) afirmă în continuare momentul primirii, creând o dovadă de încredere că documentul a existat în sistem la un moment dat în timp.

6.1.1.2 Dovada depozitării

Serviciul nostru de arhivare garantează integritatea datelor, confidențialitatea și disponibilitatea pe termen lung printr-o combinație de măsuri tehnice avansate și infrastructură. Mai exact, utilizăm Dell Elastic Storage (ECS) cu replicare geografică, care asigură stocarea redundantă a datelor în locații separate geografic. Această configurare oferă:

- Durabilitatea datelor: copii stocate în diferite locații pentru a preveni pierderea datelor
- Disponibilitate ridicată: Acces continuu și preluare a datelor, chiar și în caz de defecțiune

hardware sau dezastru
- Conformitate: Îndeplinește cerințele de reglementare pentru păstrarea și securitatea datelor, deoarece datele rămân nemodificate și stocate în siguranță

Această infrastructură, combinată cu semnături digitale, funcții hash, jurnale de audit și servicii de validare calificate, asigură o dovadă cuprinzătoare a stocării, datele fiind atât protejate împotriva modificărilor neautorizate, cât și recuperabile în mod fiabil în orice moment.

Toate operațiunile asupra documentelor, cum ar fi importul sau accesul, sunt înregistrate cu piste de audit detaliate.

6.1.1.3 Dovada recuperării

Sistemul garantează autenticitatea și integritatea datelor în timpul extragerii prin:

- **Controale de acces securizate, autentificate,** asigurându-se că numai utilizatorii autorizați pot prelua documente.
- Procesul de recuperare este înregistrat, inclusiv identitatea utilizatorului, ora și detaliile documentului accesat.
- Documentele recuperate sunt însoțite de semnăturile, sigiliile și valorile hash respective, pe care utilizatorii le pot verifica folosind serviciul de validare
- Metadatele și jurnalele de audit păstrează o evidență detaliată a evenimentului de recuperare, îndeplinind cerințele legale și de conformitate pentru dovada accesului.

În conformitate cu Legea Arhivelor Naționale nr. 16/1996 actualizată în 2025 și cu reglementările privind gestionarea documentelor, distrugerea datelor digitale se realizează numai după finalizarea perioadei legale de păstrare și în prezența unor procese strict controlate și auditate. Când un document ajunge la perioada de păstrare, sistemul nostru:

6.1.1.4 Dovada ștergerii

Dovada ștergerii trebuie adaptată conformității legale (de exemplu, GDPR, Legea Arhivelor Naționale nr. 16/1996 actualizată în 2025) și procedurilor de audit intern.

În conformitate cu Legea Națională și reglementările privind gestionarea documentelor, distrugerea datelor digitale se realizează numai după **finalizarea perioadei legale de păstrare** și în prezența unor procese strict controlate și auditate.

Când un document ajunge la perioada de păstrare, sistemul nostru:

- Înregistrează o posibilă solicitare de ștergere în jurnalul de audit, menționând data, ora, operatorul și motivul ștergerii
- Efectuează o verificare finală a listei de documente înainte de ștergere și necesită aprobarea operatorului
- Păstrează toate înregistrările de ștergere în jurnale, astfel încât acestea să fie disponibile pentru audit și verificare legală, conform cadrului legal românesc și european
- Dacă există o cerință de prelungire a păstrării unui document, acesta trebuie să fie documentat și aprobat de Arhivele Naționale ale României.

Această procedură asigură respectarea legislației naționale, transparența procesului și posibilitatea de a demonstra, în orice moment, că documentele au fost șterse în mod legal și securizat.

6.1.2 Integritatea datelor

- Soluția de arhivare implementează mecanisme (cum ar fi semnături digitale și funcții hash) pentru a se asigura că datele arhivate rămân nemodificate prin punerea amprentei documentelor și semnarea cu sigiliul electronic calificat emis către Zipper Services (arhivistul)
- Generarea amprentei digitale (hash): Fiecare document este asociat cu un hash unic (de exemplu, SHA-256) calculat înainte de import
- Pistă de audit și înregistrare: Orice operațiune pe document este înregistrată într-un jurnal
- Furnizarea de procese de verificare care permit utilizatorilor să confirme integritatea și autenticitatea datelor în orice moment prin intermediul serviciului de validare calificat (raport de validare)

6.1.3 Confidențialitatea datelor și controlul accesului

- controlul accesului asigură că numai personalul autorizat poate accesa datele arhivate, RepoZip a dezvoltat politici de acces pentru a guverna cine poate accesa colecțiile și în ce condiții. Aceste politici echilibrează adesea nevoia de acces public cu protecția materialelor sensibile sau protejate prin drepturi de autor.
- asigurarea accesului la documente (metadate asociate) printr-un canal securizat, doar prin autentificarea persoanei, in conformitate cu permisiunile rezultate din setarea grupului si rolului (pe baza Nomenclatorului in vigoare transmis arhivatorului Zipper EATSP). Soluția permite:
    - Collibri RepoZIP LTA implementează diferite tipuri de mecanisme de autentificare, cum ar fi acreditări de conectare și restricții IP, 2FA, SSO pentru a se asigura că numai utilizatorii autorizați pot accesa materiale restricționate. De asemenea, pot folosi criptarea pentru a proteja datele sensibile.
    - Control granular al accesului: Permisiunile sunt gestionate dinamic pe baza grupurilor și rolurilor definite în Nomenclatura arhivistică. Accesul poate fi restricționat la nivelul acțiunii permise (de exemplu, citire, descărcare).
    - Criptare end-to-end: Canalele de comunicare dintre utilizator și arhivă sunt criptate cu protocoale TLS 1.3, iar obiectele arhivate sunt stocate criptate (AES-256).

6.1.4 Conservare pe termen lung (durabilitate)

- Susține conservarea datelor pe perioade lungi de timp, având în vedere obsolescența tehnologică.

- Serviciul de arhivare oferit de Zipper QTSP se bazează pe **profilurile de conservare specificate în QPS-QPSA-ZS_Qualified Preservation Services_v1 PCPP:**

- utilizeaza o marca temporala calificata furnizat de Zipper Time-Stamping Authority (TSA)
- utilizeaza un serviciu de validare calificat (ValS) (a se vedea ETSI TS 119 441 și ETSI TS 119 442) pentru a colecta informații despre calea de certificare și informații despre revocare sau pentru a colecta direct informații despre calea de certificare și pentru a colecta informații despre starea certificatului emise de o autoritate de stare a certificatului (CSA).

6.1.5 Disponibilitate

Aplicatia Collibri RepoZIP LTA asigura conditiile necesare pentru preluarea si utilizarea usoara, ori de

cate ori este necesara, cu respectarea stricta a conditiilor de confidentialitate si integritate a documentelor (metadate asociate):

- Redundanță și replicare: Arhiva este stocată în două locații geografice (geo-redundanță) pentru a preveni pierderea datelor
- Backup periodic și automat: Efectuat zilnic, cu politici stricte de restaurare
- Interfață de recuperare rapidă: Oferă funcționalitate de căutare bazată pe metadatele asociate

6.1.6 Autenticitate

Aplicația Collibri RepoZIP LTA asigură posibilitatea verificării identității persoanei/entității, care a semnat/sigilat documentul cu un certificat calificat, în calitate de titular cu drept de a dispune de document. Această verificare se face prin serviciul de validare a semnăturii/sigiliului calificat (acreditare Zipper Services):

- Certificate calificate eIDAS: Sunt acceptate doar semnăturile/sigiliile bazate pe certificate calificate, emise de furnizori acreditați, iar raportul de verificare, semnătura
- Validare automată: Sistemul integrează serviciile de validare (OCSP, CRL) furnizate de Zipper Services pentru a verifica valabilitatea semnăturilor și sigiliilor titularilor dreptului de dispoziție.
- Marcarea identității semnatarului: Se păstrează metadatele cu datele semnatarului și ale autorității emitente a certificatului

6.1.7 Nerepudiere

Se asigură că, după importul în Collibri RepoZIP LTA, acel document exista la acel moment. Această dovadă este asigurată de măsurile aplicate procedural, arhivistul aplicând și o marcă temporală calificată pentru a demonstra ulterior existența acesteia.

- Import înregistrat cu marcaj temporal calificat: La momentul importului, obiectului arhivat i se aplică o marcă temporală conform Regulamentului eIDAS, certificată de furnizorul QTSP Zipper
- Lanț de încredere: Fiecare obiect arhivat este însoțit de un sigiliu calificat al Arhivatorului (Zipper EATSP) și de o marcă temporală încorporată în semnătură, formând un lanț criptografic care poate fi verificat în instanță

6.1.8 PROPRIETARUL DOCUMENTULUI ÎN FORMAT ELECTRONIC

Proprietarul documentului în formă electronică este definit la nivel de aplicație sub numele de Client și va defini tipurile de documente, metadate, grupuri și utilizatori aparținând acestui Client.

Titularul dreptului de a dispune de document este proprietarul sau, după caz, emitentul documentului, care are dreptul de a stabili și modifica regimul de acces la document, conform legislației în vigoare.

Primirea unui document în formă electronică în arhiva electronică este condiționată de îndeplinirea următoarelor cerințe:

a) semnarea documentelor în format electronic cu semnătura electronică extinsă a titularului dreptului

de a dispune de document, denumită în continuare semnătură electronică.
b) valabilitatea semnăturii electronice a titularului dreptului de a dispune de document la momentul introducerii acestuia în arhivă;

Beneficiarul serviciului de arhivare electronică trebuie:
a) să dețină un certificat digital calificat pentru semnătura electronică;
b) certificatul digital calificat trebuie să fie valabil;
c) să comunice administratorului informațiile necesare verificării valabilității certificatului utilizat pentru semnătura electronică a documentelor stocate în arhiva electronică.

6.1.9 METADATE DOCUMENTE

În cadrul aplicației se creează informații descriptive de conservare pentru informațiile arhivate, respectiv cuvinte-cheie necesare identificării documentului în formă electronică.

Cuvintele cheie, denumite în continuare metadate, vor permite grupurilor de utilizatori să descopere și să identifice documentul de interes.

Metadatele necesare vor include informații despre creator, formate de date, detalii criptografice și metadate cerute de legea națională privind arhivarea și vor conține cel puțin următoarele informații:

a) proprietarul documentului electronic;

b) emitentul documentului electronic;

c) titularul dreptului de a dispune de document;

d) istoricul documentului electronic;

e) tipul documentului electronic;

f) nivelul de clasificare a documentului electronic;

g) formatul digital în care este arhivat documentul electronic;

h) cuvintele cheie necesare identificării documentului electronic;

i) elementele de localizare a suportului fizic (dacă documentul electronic a fost generat prin transferul de informații de pe suporturi analogice în suporturi digitale)

j) identificatorul unic al documentului electronic, din arhiva electronică;

k) data emiterii documentului;

l) data arhivării;

m) termenul de păstrare a documentului.

În cazul în care documentul electronic a fost generat prin transferul de informații de pe suporturi analogice în suporturi digitale, înregistrarea trebuie să conțină în plus următoarele informații:

a) referințe la proprietarul originalului și la locația în care se află originalul;

b) metoda de transfer utilizată;

c) dispozitivul hardware utilizat;

d) programul de calculator utilizat.

6.1.9.1 Pachete de informații — Formatul pachetului de informații

Pachetul de informații este definit într-un limbaj formal de definire a datelor (XML) și este trimis Abonatului, pe baza listei de metadate definite de legea română.

IP face diferența între elementele de date obligatorii și opționale în definirea și descrierea structurii de date.

Elementele opționale în format pot fi definite ca obligatorii din cauza logicii condiționate (de exemplu, un element este opțional, dar dacă există, următoarea cerință opțională este obligatorie).

Perioada de păstrare este definită în Nomenclatorul Abonatului (în lună), dar calculul datei ar putea fi relativ la data emiterii documentului sau la altă dată (definită într-alte metadate – de exemplu, data închiderii documentului)

6.1.10 Depunerea transferului

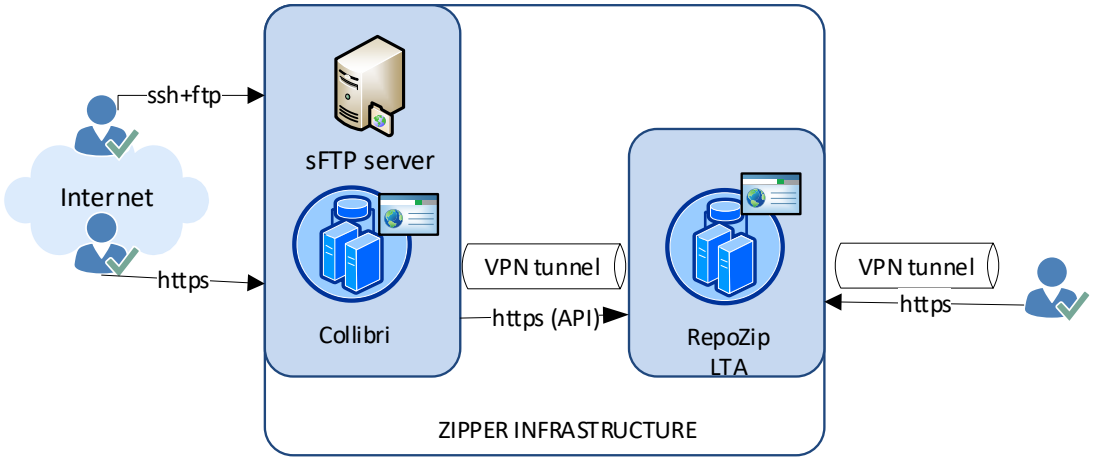
Zipper QTSP este responsabil pentru integritatea și confidențialitatea transferului trimiterii furnizate de Abonat și va verifica dacă procedurile și protocoalele pentru transfer au fost urmate de abonat.

Schimbul de informații între Abonat și Zipper QTSP se realizează în baza unui acord (contract) semnat, care include mijloacele, cerințele și responsabilitățile legate de securitatea informațiilor. Fiecare acord va conține o procedură documentată pentru gestionarea transferului între Zipper QTSP și Abonat și, de asemenea, posibilele eșecuri între abonat și Zipper EATSP.

Pot fi aplicate diferite protocoale de securitate a comunicațiilor (la nivel de legătură de date, rețea, transport și aplicație) cum ar fi: protocoale de tunelare (IPSec/SSL VPN), sFTP, FTP, HTTPS, care vor fi stabilite în acordul semnat.

Zipper EATSP asigură transferul documentelor pe internet (cu protocoale de tunelare) folosind protocoale de rețea comune:

- sFTP/ FTPS
- API-ul REST
- Încărcare manuală prin interfață



Exemplu de transfer:

Răspunsuri la posibile eșecuri API REST:

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 și trasabilitate

Zipper menține jurnale detaliate ale tuturor acțiunilor asupra datelor arhivate, inclusiv crearea, accesul, modificările și recuperarea și poate permite trasabilitatea în scopuri de audit și conformitate legală.

6.3 Măsuri de securitate

Aplicația este stocată într-o infrastructură securizată în centrul de date Zipper și aplică controale de securitate fizice și logice pentru a proteja împotriva pierderii datelor, manipulării, furtului și accesului neautorizat.

6.4 Proceduri operaționale

Acordul de abonat definește proceduri operaționale clare pentru ingestia, validarea, stocarea și recuperarea datelor.

Zipper a implementat procese de recuperare în caz de dezastru și backup pentru a minimiza riscurile de pierdere a datelor.

7. Declarație de practică legată de serviciul de arhivare electronică oferit de Zipper

Fluxul de arhivare constă în:

1. **Depunerea transferului**: Descărcarea documentului și a metadatelor asociate din arhiva operațională în aplicația Collibri RepoZIP LTA în modul convenit (hot folder FTP, API). Ex. aplicația de arhivă operațională va apela, prin webservice, solicitarea de încărcare a unui document și a metadatelor asociate în arhivă.

2. **Verificarea pachetului de informații**: Pe baza tipului de document, RepoZip face asocierea la nomenclatorul arhivistic al companiei utilizatore si completarea metadatelor obligatorii (in baza legislatiei romane).

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

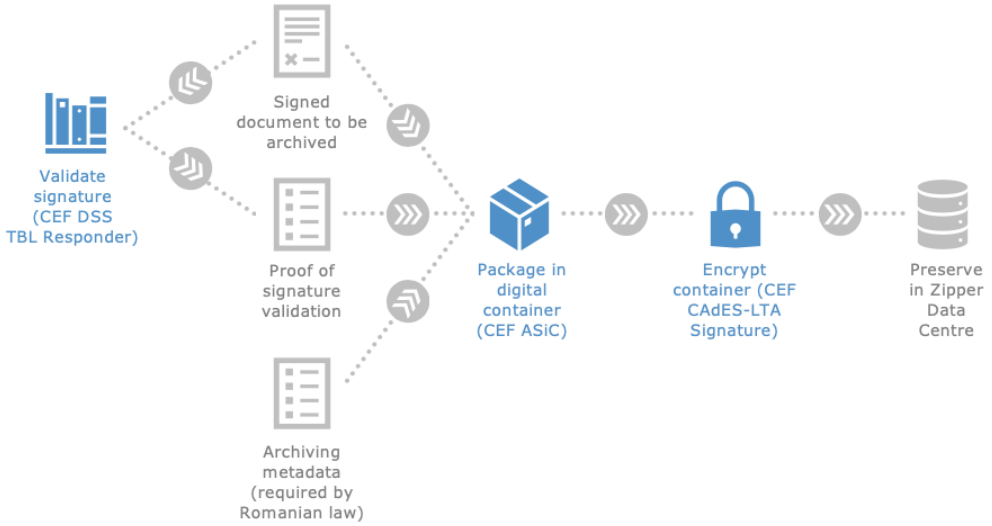
Dacă tabelul auxiliar "Nomenclator" este furnizat de către Abonat, va exista o corelație clară între NomenclatorId și documentul arhivat, în acest caz _ArchivingPeriod (perioada de păstrare) și alte metadate necesare vor fi completate automat de aplicația de arhivare.

3. **Conservarea containerului de obiecte pe baza serviciului de conservare calificat, schema de conservare cu augmentarea semnăturii/sigiliului și cu depozitare (F3 – conform ETSI TS 119 512 Anexa F)**

- Aplicația verifică automat semnătura electronică a documentului. Semnătura/sigiliul emitentului oficial al documentului trebuie să fie valabil și întocmit cu un certificat calificat
- Se generează un raport de validare bazat pe ETSI EN 319 102-1, folosind QVS Zipper 'qualified validation service' (verifică starea certificatului, revocarea, profilul de semnătură, algoritmii etc.). Raportul de validare este semnat cu un sigiliu electronic calificat (emis pentru Zipper) și TS calificat încorporat.
- QVS returnează un raport de validare (VR), semnat/sigilat digital de QVS, afirmând

rezultatul în acel moment.

- Validarea va avea ca rezultat o stare TOTAL_PASSED, NEDETERMINATĂ sau TOTAL_FAILED, pe baza regulilor de constrângere Zipper.
- Doar documentul electronic TOTAL_PASSED și NEDETERMINAT (NO-POE) va fi acceptat în arhivă pentru a fi păstrat. Un container ASIC-E este creat și este contrasemnat/sigilat de către administratorul arhivei (Zipper) folosind un certificat electronic calificat. Semnătura aplicată pe ASIC va asigura disponibilitatea și integritatea pe termen lung a materialului de validare (ER). **Se furnizează** confirmarea primirii.
- **Augmentarea POC**: Aplicația de arhivare RepoLTA va menține păstrarea stării de valabilitate a semnăturii digitale (semnătură la nivel LTA) aplicată pe fișierul ASIC. Această operațiune se va face pentru fișierele ASIC, înainte ca marcajul de timp calificat aplicat să expire sau să existe probleme de securitate criptografică.



În cazul unui IMPORT reușit în arhiva electronică:

1. Documentul electronic va primi un ID unic (IDDoc/POID) pentru identificare în arhivă.

2. Containerul de documente "Container de semnături asociat" este creat, stocat într-un format ZIP (extensie .asic), conform ETSI TS 102 918 V1.3.1. Containerul va conține pdf-ul original primit, metadatele primite, raportul de validare, conform ETSI EN 319 102-1

3. Se contrasemnează cu semnătura electronică a administratorului arhivei electronice;

4. Se aplică marca temporală calificată

5. Metadatele create automat sunt generate

"Dosarul electronic" atașat fiecărui document arhivat va conține cel puțin următoarele informații:

Primit de la beneficiar:

a) proprietarul documentului în format electronic.

a) emitentul documentului în format electronic.

b) titularul dreptului de a dispune de document.

c) data emiterii documentului.

d) tipul de document în format electronic.

e) nivelul de clasificare a documentului în format electronic.

f) cuvinte-cheie necesare identificării documentului în format electronic.

g) perioada de păstrare a documentului (poate fi calculată în raport cu un metadat/cuvânt cheie).

h) elemente de amplasare a suportului fizic; - dacă este necesar.

Generat automat în aplicația de arhivare (după momentul arhivării electronice):

Generat de arhivator (Zipper EATSP):

i) identificatorul unic al documentului în format electronic, în cadrul arhivei electronice.

j) data arhivării (data introducerii în arhivă).

k) formatul digital în care documentul este arhivat în format electronic.

l) istoricul documentului în format electronic.

m) dimensiunea documentului arhivat

Dacă un document nu îndeplinește criteriile de integritate, acesta este marcat automat și nu poate fi arhivat. După corectare, va trebui reintrodus în sistem și, dacă trece cu succes validările, va fi arhivat.

Sunt înregistrate toate operațiunile efectuate pe arhiva electronică, înregistrările de audit care conțin data și ora evenimentului, tipul evenimentului, rezultatul (succes sau eșec) al evenimentului.

Accesul la sistemul de arhivare electronică RepoZip se realizează prin linii de comunicare securizate între Beneficiar și Furnizor (Zipper Services). Accesul la documentele arhivate este restricționat, un

utilizator poate prelua un document arhivat doar dacă face parte din grupul de acces stabilit de participant pentru a accesa documentul și are nivelul de securitate adecvat pentru a putea vizualiza documentul.

Modulul de verificare și semnătură a arhivatorului utilizează eSignature DSS pentru a valida mai întâi semnătura electronică a documentului primit, înainte ca documentul să fie aprobat pentru arhivare.

- Verificați dacă semnătura este calificată și ce tip de certificat a fost utilizat. Beneficiarul va fi responsabil pentru semnarea documentelor folosind un certificat calificat furnizat de un QTSP (furnizor de servicii de încredere calificat). Dacă semnarea este externalizată, aceasta trebuie făcută de un QTSP, care oferă semnare QTS (servicii de încredere calificate). Certificatele digitale AdES sunt acceptate (conform ETSI TR 119 112 V1.1.1 (2019-04) și ETSI EN 391 102-1 [i.6]) de tipul:

-> semnătură de bază (ex. CAdES-B, PAdES-B etc.)

-> Semnătură cu timp (de exemplu, CAdES-T, PAdES-B-T etc.)

-> semnături cu material de validare pe termen lung. Ex. CAdES-X, PAdES-B-LT

-> Semnături care asigură disponibilitatea și integritatea pe termen lung a materialului de validare (ex. CAdES-X-L, PAdES-B-LTA, PADES-E-LTV etc.)

Pașii de verificare sunt:

A) certificatul X.509 pentru semnătura electronică aplicată documentului de către titularul dreptului de dispunere este verificat prin:

-> comparație hash pentru integritatea documentelor;

-> certificate de cheie publică (PKC) utilizate

-> Informații despre starea revocării pentru fiecare listă de revocare a certificatelor (CRL) sau stare a certificatului (OCSP)

-> "Afirmație de timp" aplicată semnăturii (dacă există)

- Documentul care urmează să fie arhivat este apoi ambalat într-un container digital împreună cu dovada validării semnăturii, precum și alte metadate care detaliază procesul de arhivare, conform legislației române.

- În pasul următor, containerul este criptat pentru a proteja integritatea. Criptarea are loc prin aplicarea unei semnături de arhivare pe termen lung (numită și semnătură la nivel LTA) cu un furnizor de marcaj

temporal calificat.

- Modulul Data Container Creation and Encryption (ASIC) se bazează, de asemenea, pe specificațiile eSignature DSS: profilul de bază ASiC (Associated Signature Container) pentru container și CMS Advanced Electronic Signature (CAdES) pentru criptare.

- ASIC: "Container de semnătură asociat" în conformitate cu ETSI TS 102 918 V1.3.1. Containerul va conține pdf-ul original primit, PDF-ul de verificare (punctul b), metadatele primite, datele de identificare a semnăturii.

Serviciul Zipper eArchiving arhivează containerele de obiecte de conservare, așa cum este descris în Politica de arhivare electronică Zipper.

POC conține:

- Obiecte de conservare (PO) — datele care trebuie păstrate. Acestea pot fi doar date semnate
- Date de probă, validare și revocare / stare - date necesare pentru validarea semnăturilor, marcajelor temporale, căilor de revocare / valabilitate a certificatelor și, eventual, rapoarte de validare. Acestea sunt esențiale pentru a se asigura că, în viitor, starea de valabilitate (sau invaliditatea) semnăturilor poate fi reconstruită.
- Metadate despre POC în sine: identificatori (de exemplu, proprietarul documentului), marcaje temporale, valori hash, sume de control etc. Acest lucru susține integritatea, trasabilitatea, capacitatea de a verifica dacă containerul nu a fost modificat și ajută la reconstruirea dovezilor.

Containerul POC Zipper are următoarele specificații:

- **Format**: Container ASiCE
- **Conținut: Documente** semnate + semnături + raport de validare (XML semnat) + înregistrări de dovezi (evidence records)
- **Nivel de semnătură**: BLTA (Baseline cu validare pe termen lung și marcaje temporale de arhivare)
- **Certificat de semnare**: Certificat calificat pentru sigiliu electronic emis de un QTSP [Furnizor] de la TL, emis către *Zipper Services*
- **Marcaj temporal**: Marcaj temporal calificat (QTS) furnizat de Zipper QTS (vezi https://pki.ca.ezipper.ro/repository/certs.php)
- **Date de validare incluse:** Certificate, informații de revocare (CRL-uri/OCSP) printr-un raport de

validare emis de Zipper QVS.

- **Scop:** Serviciul de conservare asigură că semnătura și obiectele asociate sunt verificabile pe termen lung, în conformitate cu cerințele ETSI TS 119511 și eIDAS.

Zipper va păstra POC-ul extinzându-l în timp:

[**Client**] → *Zipper Creează POC inițial* (nivel ASiC-E, B-LTA) → [**Serviciu de conservare** PDS+PGD+WST] -> *Validare prin SVS* → *Colectarea datelor de validare* → *Generarea dovezilor de conservare* → *Stocarea POC extins (+ dovezi) cu =>* [**Serviciu de conservare-AUG] (nivel A-E, B-LTA)**

↓

Recuperare PO / Audit / Verificare

8. Centrul de date utilizat de arhiva electronică

Centrul de date Zipper utilizat de administratorul arhivei electronice Zipper Services dispune de echipamentele tehnice necesare și aplică politicile și procedurile de management și securitate necesare pentru îndeplinirea condițiilor prevăzute de cerințele Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice în piața internă, astfel cum a fost modificat de Regulamentul (UE) 2024/1183 (eIDAS 2.0), legate de serviciile de arhivare.

Arhiva electronică rezultată din serviciul de arhivare electronică (Serviciul LTA), este stocată în centrul de date sub rezerva autorizării prealabile a României, cu respectarea normelor privind asigurarea:

a) integritatea și securitatea documentelor în format electronic;

b) securitatea și integritatea spațiului ocupat de echipamentele care adăpostesc arhivele electronice;

c) recuperarea informațiilor în urma dezastrelor naturale, conform reglementărilor în vigoare.

Centrele de date îndeplinesc următoarele condiții:

(a)asigură securitatea și integritatea datelor, la nivelul securității fizice și al accesului prin mijloace informatice;
b) disponibilitatea serviciului de arhivare electronică și copierea de rezervă a informațiilor stocate.

Disponibilitatea datelor este asigurată prin utilizarea dispozitivelor de stocare dedicate în două locații diferite într-o configurație de înaltă disponibilitate, folosind un backend clusterizat care oferă copii în oglindă ale tuturor documentelor și metadatelor asociate.

8.1 Politica centrului de date

Acest document conține detalii specifice despre mediul de operare, structura organizațională, procedurile de operare, facilitățile și infrastructura ZIPPER. Descrie doar regulile generale de

gestionare a centrului de date. Descrierile detaliate ale infrastructurii și ale procedurilor operaționale aferente sunt descrise în documente suplimentare care nu sunt disponibile publicului. Aceste documente suplimentare sunt disponibile numai personalului autorizat ZIPPER și, pe baza necesității de a cunoaște, organismului de evaluare a conformității care auditează serviciile de marcare temporală.

Această secțiune stabilește regulile generale privind cerințele tehnice, organizatorice și procedurale ale ZIPPER. Zipper Services SRL dispune de un centru de date, format din 2 containere, pe o arhitectură redundantă, performanță ridicată și disponibilitate a serviciilor, într-o structură distribuită.

Mai jos sunt descrise politicile și procedurile de asigurare a confidențialității datelor, integritatea și disponibilitatea documentelor arhivate în formă electronică, pe toată perioada legală de păstrare a acestora.

8.1.1 POLITICA DE ACCES LA DOCUMENTE

Soluția are mecanisme adecvate pentru a detecta coruperea sau pierderea datelor. Există o procedură internă de raportare a tuturor incidentelor de corupție sau pierdere de date și a pașilor întreprinși pentru a restaura sau elimina datele corupte sau pierdute.

Soluția dispune de mecanisme adecvate pentru a asigura integritatea documentelor arhivate. Integritatea este definită ca absența modificărilor neintenționate ale conținutului arhivei, a metadatelor descriptive necesare rămânând asociate corespunzător, verificarea numărului de copii, sincronizarea copiilor, verificarea completitudinii acordurilor de arhivare, validarea urmelor de audit pentru toate accesările.

Soluția are mecanisme adecvate pentru a asigura confidențialitatea și protecția vieții private informațiilor stocate. Toate informațiile stocate vor fi obținute, stocate și prelucrate în conformitate cu legile în vigoare, în special cu Legea română privind protecția datelor cu caracter personal. Există o declarație de politică privind protecția datelor cu caracter personal, care va fi anexată la acest document.

Accesul la date va fi în concordanță cu clasificarea datelor, grupul și rolul utilizatorului. Regimul de acces la un document în format electronic, modificarea și termenul de păstrare a acestuia se stabilesc exclusiv de titularul dreptului de a dispune de documente.

Drepturile fiecărui utilizator sunt stabilite la nivel de client, grup și rol (nivel de acces), asigurând astfel accesul utilizatorului doar la documentele și datele clientului căruia îi aparține grupul.

Parolele tuturor utilizatorilor sunt păstrate criptate în sistemul Collibri RepoZIP LTA. Un cont de utilizator care nu a fost utilizat pentru o perioadă de 1 an este dezactivat, necesitând o cerere de reactivare din partea Beneficiarului.

Beneficiarul este obligat să întreprindă toate acțiunile posibile pentru a proteja numele de identificare și parola necesare utilizării serviciilor furnizate. Beneficiarul este responsabil pentru orice eveniment sau fapte care au avut loc prin utilizarea numelui său de identificare și a parolei de acces, cu excepția cazului în care evenimentul sau acțiunea a avut loc din motive care pot fi atribuite

Arhivistului.

Aplicația de arhivare oferă:
• dovada existenței unui document primit, în funcție de timp
• Asigură autentificarea/integritatea datelor
• Oferă arhivare pe termen lung (deci trebuie să poată asigura validitatea datelor și documentelor arhivate pentru perioada de arhivare necesară, adică depășirea expirării/revocării certificatului, expirarea marcajului temporal și depășirea tehnologică din cauza lungimii cheii și hash-ului sau a algoritmilor de semnare

8.1.2 POLITICA PRIVIND DISPOZITIVELE CRIPTOGRAFICE UTILIZATE

Deținătorul unui dispozitiv criptografic trebuie să își îndeplinească sarcinile și obligațiile în mod responsabil în orice situație posibilă.
Următoarele elemente sunt luate în considerare la elaborarea politicii privind controalele criptografice:
- modul în care conducerea abordează utilizarea controalelor criptografice, inclusiv principiile generale care stau la baza protecției informațiilor comerciale;
- Abordarea de gestionare a cheilor, inclusiv metode de recuperare a informațiilor criptate în caz de pierdere, compromitere sau distrugere a cheilor;
- roluri și responsabilități pentru:
  - punerea în aplicare a politicii;
  - managementul cheilor;

Un deținător de dispozitiv criptografic trebuie să-și notifice emitentul în caz de furt, pierdere, dezvăluire neautorizată sau compromitere a securității imediat după incident.
Un deținător de dispozitiv criptografic nu este responsabil pentru neîndeplinirea sarcinilor/obligațiilor sale din motive imposibil de controlat pentru el.
Deținătorul dispozitivului criptografic este responsabil pentru neglijarea obligațiilor sale de a notifica emitentul cu privire la dezvăluirea sau încălcarea securității ca urmare a greșelilor, neglijenței sau iresponsabilității sale.

8.1.3 POLITICA PRIVIND MIJLOACELE DE CONTROL ȘI SECURITATE A DOCUMENTELOR ȘI A BAZELOR DE DATE

Aplicatia Collibri RepoZIP LTA asigura controlul si securitatea accesului la aplicatie prin limitarea accesului la:
- internal mesh Zipper
- rețeaua/IP-urile beneficiarului

Controlul și securitatea accesului la documente:
-Este securizat, prin indicarea unui nume de utilizator și a unei parole.
- Regimul de acces la un document în format electronic, modificarea și termenul de păstrare a acestuia sunt stabilite exclusiv de titularul dreptului de a dispune de documente. Furnizorul este obligat să respecte regimul de acces la documentele electronice.
-Drepturile fiecarui utilizator sunt stabilite la nivel de client, grup si rol (nivel de acces), asigurand astfel accesul utilizatorului doar la documentele si datele clientului la care apartine grupul are acces.
- Parolele tuturor utilizatorilor sunt păstrate criptate în sistemul Collibri RepoZIP LTA.
- Un cont de utilizator neutilizat pentru o perioadă de 1 an este dezactivat, necesitând o cerere de

reactivare din partea Beneficiarului.
- Beneficiarul este obligat să întreprindă toate acțiunile posibile în vederea protejării numelui de identificare și a parolei necesare utilizării serviciilor furnizate. Beneficiarul este responsabil pentru orice eveniment sau fapte care au avut loc prin utilizarea numelui său de identificare și a parolei de acces, cu excepția cazului în care evenimentul sau acțiunea a avut loc din motive care pot fi atribuite Furnizorului.

Controlul și securitatea accesului la baza de date
-La cererea Beneficiarului, exista si posibilitatea utilizarii unui server virtual separat exclusiv pentru aplicatia clientului (se utilizeaza o clona a aplicatiei si o baza de date care contine exclusiv datele clientului) pentru un nivel sporit de securitate.
- Orice acces la baza de date a Beneficiarului este înregistrat într-un fișier de acces (denumit jurnal de procesare automată). Informațiile privind adăugarea, modificarea sau ștergerea datelor de afaceri ale Beneficiarului sunt salvate

Autentificarea utilizatorului
Orice activitate care poate duce la acțiuni asupra datelor sensibile ale afacerii (de exemplu, descărcare) Jurnalul unui eveniment Log va conține următoarele date: ID utilizator, marcaj temporal și tip de operațiune
Jurnalul va fi disponibil pentru consultare de către utilizatorii cu drepturi în acest sens.

9. Participanţii

9.1 Abonați (beneficiar)

Abonatul/beneficiarul este solicitantul, persoana fizică sau juridică care solicită serviciul de arhivare electronică și care intră într-o relație contractuală cu ZIPPER. Abonatul va fi tras la răspundere în mod direct dacă obligațiile sale nu sunt îndeplinite corect.

9.2 Părţi

Una dintre părți este Abonatul, persoană fizică sau juridică care transmite un document digital în arhiva electronică, iar cealaltă parte este arhivistul acreditat, care preia documentul și metadatele, conform legislației în vigoare.

Arhivarea electronică a documentelor este reglementată de aceleași reguli ca și în cazul documentelor pe suport de hârtie și se supune prevederilor legislației arhivistice în vigoare, cu următoarele specificații:

a) înregistrarea documentelor în formă electronică de către sistemul de arhivare electronică atestă existența oficială a acestor documente. Numărul de înregistrare identifică în mod unic documentul din sistem. Odată înregistrat, documentul nu poate suferi modificări ale conținutului. Odată cu înregistrarea, se completează dosarul electronic al documentului.
c) sistemul electronic de gestiune a documentelor generează automat o înregistrare de audit, în care sunt înregistrate toate deciziile și acțiunile care au loc asupra unui document din momentul înregistrării până la distrugerea acestuia, fără posibilitatea de a fi modificate;
d) documentele și dosarele arhivate în format electronic vor fi incluse în nomenclatorul arhivistic al Abonatului, precizând în secțiunea "Observații": "în formă electronică".

9.3 Alți participanți

Nu se aplică.

10. Obligații și răspundere

Acest capitol include toate obligațiile, răspunderile, garanțiile și răspunderile ZIPPER LTA, ale abonaților și utilizatorilor săi (abonați și părți care se bazează). Aceste obligații și responsabilități sunt guvernate de acorduri acceptate de toate părțile.

ZIPPER își asumă responsabilitatea pentru implementarea cerințelor secțiunii "Practici LTA" a acestui document, precum și a prevederilor legislației naționale.

Acordurile ZIPPER cu abonații și părțile pe care se bazează descriu reciproc obligațiile și responsabilitățile, inclusiv responsabilitățile financiare. Declarația de politică și practică ZIPPER (acest document) face parte integrantă din aceste acorduri.

a. Obligații și garanții LTA față de abonați

ZIPPER garanteaza disponibilitatea a 99,6% din infrastructura si aplicatia de arhivare electronica in zilele lucratoare, cu exceptia pauzelor tehnice programate, in ceea ce priveste mentenanta echipamentelor si sistemelor.

ZIPPER își asumă următoarele obligații față de Abonați:

- Să opereze în conformitate cu această declarație de politică și practică ZIPPER LTA (acest document) și cu alte politici și proceduri operaționale relevante;
- să se asigure că OTS menține o precizie minimă a orei UTC de ± 1 secundă;
- Menținerea unei echipe competente și experimentate care să asigure continuitatea serviciilor de infrastructură;
- Asigurarea permanentă a securității fizice și logice, precum și a integrității serverelor, software-ului și bazelor de date necesare bunei funcționări a serviciilor de arhivare electronică
- Monitorizează întreaga infrastructură LTA pentru a preveni sau limita orice întrerupere sau indisponibilitate a serviciilor
- Urmează revizuiri/audituri interne și externe pentru a asigura conformitatea cu legislația relevantă și cu politicile și procedurile interne ale ZIPPER;
- Oferă acces de înaltă disponibilitate la sistemele LTA ZIPPER, cu excepția întreruperilor tehnice planificate și a pierderii de sincronizare a timpului.
- Scanare de vulnerabilități cel puțin o dată pe trimestru și test de penetrare cel puțin o dată pe an
- Program de funcționare: nivelul de disponibilitate garantat de 99,6% se aplică în zilele lucrătoare, cu excepția perioadelor de mentenanță planificată.
- Mentenanță planificată: anunțată abonaților prin e-mail cu cel puțin 24 de ore înainte, programată de preferință în afara programului de lucru, de exemplu între 22:00 și 06:00 CET, și cu o durată de cel mult [12 ore] pe lună.

- Recuperare în caz de dezastru: o locație secundară poate prelua serviciul în cel mult [4 ore] (RTO), conform planului de continuitate a activității. Nu se pierde nicio dovadă de păstrare emisă și nicio înregistrare din jurnalul de audit (RPO = 0 pentru jurnalul de audit).

b. Drepturile abonaților

Abonații beneficiari au următoarele drepturi:
a) stabilirea regimului de acces la documentul arhivat, precum și modificarea acestuia;
b) atestarea valorii originale sau de copie a documentului arhivat;
c) accesul online la registrul electronic al arhivei electronice;
d) accesul online la dosarul electronic atașat fiecărui document introdus în arhiva electronică, conform regimului de acces stabilit;
e) Accesul online la documentele arhivate care nu au acces public și la dosarele electronice ale acestora este considerat asigurat atunci când persoanele care au drept de acces la documente și la Fișierele lor electronice pot fi consultate printr-o rețea privată (care nu este conectată la Internet). Este necesar consimțământul scris al beneficiarului cu privire la utilizarea rețelei respective.

Abonații trebuie să verifice pachetul de date arhivat de ZIPPER LTA.

Această verificare include:

- Verificați dacă pachetul de date conține documentul original arhivat, înregistrarea electronică a documentului și raportul de validare a semnăturii, contrasemnat de arhivist
- Verificarea certificatului de arhivist:
  - Verificarea căii de încredere până la certificatul rădăcină de încredere și pentru fiecare dintre certificatele din lanț (inclusiv certificatul cu care este semnat)
  - Verificați dacă certificatul nu a expirat în momentul semnării
  - Verificați dacă certificatul nu a fost revocat în momentul semnării

Alte obligații ale Abonatului pot fi, de asemenea, definite în Termenii și condițiile ZIPPER pentru serviciile de arhivare electronică.

c. Răspunderea Zipper

Răspunderea ZIPPER care acționează în calitate de administrator al arhivei pentru abonații săi este specificată în acordul dintre părți sau este cea prevăzută de legea aplicabilă.

ZIPPER este răspunzător pentru orice daune cauzate direct, intenționat sau din neglijență, oricărei persoane sau entități, ca urmare a nerespectării obligațiilor prevăzute aici.

Termenii și condițiile ZIPPER pentru serviciile de arhivare electronică limitează răspunderea ZIPPER. Limitările de răspundere includ excluderea daunelor indirecte, speciale, incidentale și consecutive. Acestea includ, de asemenea, un plafon de răspundere pentru răspunderea agregată combinată a ZIPPER față de toate persoanele în ceea ce privește serviciile de arhivare electronică, care este limitat la o sumă care nu depășește cea a contractului respectiv pentru serviciul de marcare temporală și la un maxim total de 500.000 EUR, indiferent de natura și tipul răspunderii, de valoarea sau amploarea oricărui prejudiciu suferit.

ZIPPER LTA nu este în niciun fel responsabil pentru utilizarea frauduloasă a serviciului.

11. Declarație de bune practici

11.1 Managementul și operarea infrastructurii

i. Managementul securității

ZIPPER asigură existența unor proceduri administrative și de gestionare adecvate care corespund celor mai bune practici recunoscute.
ZIPPER îndeplinește toate funcțiile EE folosind sisteme fiabile care îndeplinesc cerințele ZIPPER ISMS.

ii. Clasificarea și gestionarea activelor

ZIPPER menține un inventar al tuturor activelor și atribuie o clasificare a cerințelor de protecție acelor active în conformitate cu analiza de risc.

iii. Securitatea personalului

ZIPPER menține controale adecvate ale personalului care îndeplinesc cele mai bune practici de securitate și cerințele standardelor relevante.
Personalul de conducere și operațional are abilitățile și cunoștințele adecvate privind marcarea temporală, semnăturile digitale și serviciile de încredere, precum și procedurile de securitate pentru personalul cu responsabilități de securitate, securitatea informațiilor și evaluarea riscurilor.
ZIPPER implementează politica de roluri de încredere pentru toți acei angajați care au acces sau controlează operațiunile criptografice. Persoanele și rolurile de încredere includ, dar nu se limitează la:

- Personalul pentru operațiunile criptografice,
- Personalul de securitate,
- personal de administrare a sistemului;
- Personalul ingineresc desemnat și
- Directori care sunt desemnați să gestioneze fiabilitatea infrastructurii.

Înainte de a intra într-un rol de încredere, ZIPPER efectuează verificări de antecedente care pot include, ca orientare, următoarele:

- Verificarea identității
- Verificarea angajării anterioare și a referințelor profesionale;
- Confirmarea celei mai înalte sau celei mai relevante diplome de studii obținute;
- Verificarea faptului că nu există o condamnare penală;
- Verificarea înregistrărilor financiare.

ZIPPER cere ca personalul care dorește să devină persoane de încredere să furnizeze dovezi ale pregătirii, calificărilor și experienței necesare pentru a-și îndeplini în mod competent viitoarele responsabilități profesionale, așa cum sunt specificate în contractul de muncă și fișa postului, înainte de a îndeplini orice funcții operaționale sau de securitate.
Contractele de muncă semnate de angajați includ prevederi de confidențialitate pentru informațiile aduse la cunoștința acestora în timpul îndeplinirii acestora.

ZIPPER se asigură că personalul a obținut statutul de încredere și că aprobarea departamentului a fost acordată înainte ca acest personal să fie:

- Li se emit dispozitive de acces și li se acordă acces la facilitățile necesare;
- Li se emit credențiale electronice pentru a accesa și îndeplini funcții specifice pe ZIPPER LTA sau alte sisteme IT.

Conturile de utilizator sunt create pentru personalul cu roluri specifice care necesită acces la sistemul în cauză. Toți utilizatorii trebuie să se conecteze cu un cont dedicat, iar comenzile administrative sunt disponibile numai cu permisiune explicită. Permisiunile sistemului de fișiere și alte caracteristici disponibile în modelul de securitate al sistemului de operare sunt utilizate pentru a preveni orice utilizare ulterioară. Conturile de utilizator sunt blocate cât mai curând posibil atunci când schimbarea rolului dictează.

11.2 Securitatea fizică și de mediu

ZIPPER implementează Politica de securitate fizică, care susține cerințele de securitate ale acestei politici LTA și declarație de practică.

Operațiunile ZIPPER LTA se desfășoară într-un mediu protejat fizic care descurajează, previne și detectează utilizarea, accesul sau dezvăluirea neautorizată a informațiilor și sistemelor sensibile.

ZIPPER întreține, de asemenea, facilități de recuperare în caz de dezastru pentru operațiunile sale de servicii de arhivare electronică. Facilitățile de recuperare în caz de dezastru ale ZIPPER sunt protejate de mai multe niveluri de securitate fizică comparabile cu cele ale instalației principale ZIPPER.

Sistemul de securitate fizică include straturi pentru securitatea gestionării cheilor, care servește la protejarea stocării online și offline a unității de semnare criptografică (CSU) și a materialelor de chei.

Zonele utilizate pentru crearea și stocarea materialelor criptografice necesită control al accesului. Accesul la CSU-uri și la materialele cheie este restricționat în conformitate cu cerințele de separare a sarcinilor. Deschiderea și închiderea dulapurilor sau containerelor la aceste niveluri este înregistrată în scopuri de audit.

Operațiunile ZIPPER sunt protejate prin controale fizice de acces, făcându-le accesibile doar persoanelor autorizate în mod corespunzător. Accesul în zonele securizate ale clădirilor necesită utilizarea unui card de "acces" și/sau a datelor biometrice. Utilizarea cardului de acces este înregistrată de sistemul de securitate al clădirii.

Jurnalele cardului de acces sunt revizuite în mod regulat.

Spatiile securizate Zipper sunt echipate cu sisteme primare și de back-up:

- Sisteme de alimentare cu energie electrică pentru a asigura accesul continuu și neîntrerupt la energie electrică și
- Sisteme de încălzire/ventilație/aer condiționat pentru controlul temperaturii și umidității relative.

ZIPPER a luat măsuri de precauție rezonabile pentru a minimiza impactul expunerii la apă asupra instalațiilor sale, precum și pentru a preveni și stinge incendiile sau alte expuneri dăunătoare la flacără sau fum.

Toate mediile care conțin software de producție și date, informații de audit, arhivare sau backup sunt stocate în facilitățile Zipper sau în facilități de depozitare securizate în afara locației, cu controale de acces fizice și logice adecvate, concepute pentru a limita accesul la personalul autorizat și pentru a proteja aceste suporturi de daune accidentale.

ZIPPER stochează în siguranță toate suporturile amovibile și hârtia care conține informații sensibile legate de operațiunile sale în containere securizate. Documentele și materialele sensibile sunt mărunțite înainte de eliminare. Suportul utilizat pentru colectarea sau transmiterea informațiilor sensibile devine ilizibil înainte de eliminare. Dispozitivele criptografice sunt distruse fizic înainte de a fi îndepărtate.

11.3 Managementul operațiunilor

ZIPPER LTA asigură că procedurile, procesele și infrastructura trebuie să respecte managementul operațional, cerințele procedurale de securitate, managementul accesului la sistem, implementarea și întreținerea fiabilă a sistemului, managementul continuității afacerii și managementul incidentelor, așa cum sunt definite în ETSI EN 319 421.

Procedurile de management al operațiunilor pentru ZIPPER LTA sunt încorporate în procedurile generale de gestionare a operațiunilor interne ale ZIPPER.

12. Compromiterea serviciilor LTA

Zipper a dezvoltat proceduri pentru a gestiona continuitatea operațiunilor sale. În cazul întreruperilor serviciului, se străduiește să minimizeze aceste întreruperi pentru a nu afecta activitatea clientului. Zipper a creat și menține un plan de continuitate în caz de dezastru. În caz de dezastru, inclusiv compromiterea unei chei de semnare private, operațiunile sunt reluate în termenul stabilit în planul de continuitate. Cauzele dezastrului sunt luate în considerare și se stabilesc măsuri rezonabile pentru a elimina cauza întreruperii procesului, precum și măsuri de prevenire a unor astfel de dezastre în viitor.

Compania a creat, documentat, implementat și întreținut planuri, proceduri și mecanisme de control în conformitate cu standardul internațional ISO 22301 pentru a asigura nivelul necesar de continuitate a afacerii și continuitatea securității informațiilor în cazuri adverse.

Zipper oferă:

a) o structură de management adecvată disponibilă pentru a pregăti, atenua și răspunde la un eveniment distructiv, utilizând personal cu autoritățile, experiența și competența necesare;

b) dezvoltarea și aprobarea planurilor și procedurilor de răspuns și recuperare care descriu în detaliu modul în care compania va gestiona un eveniment distructiv și va menține continuitatea securității informațiilor;

c) mecanisme de control al securității informațiilor în cadrul procedurilor, sistemelor și instrumentelor pentru menținerea continuității și redresării în caz de dezastre;

d) mecanisme compensatorii pentru controlul securității informațiilor mecanisme de control care nu pot fi menținute într-un eveniment advers.

Planul de continuitate include backup-ul sistemelor critice. Backup-ul este stocat în cele două locații, care se află la 300 km distanță geografic. Condițiile speciale respectă standardele, recomandările și reglementările aplicabile în domeniul securității informațiilor. Compania verifică la intervale regulate orice mecanisme create pentru a controla continuitatea securității informațiilor, astfel încât să poată asigura efectul și eficacitatea acestora în cazuri nefavorabile. Zipper face în mod regulat copii de rezervă a informațiilor și software-ului important și garantează că toate informațiile și software-ul de bază pot fi recuperate după un dezastru sau în caz de pierdere a arhivei. Mecanismele de recuperare sunt verificate periodic, astfel încât să se poată garanta că îndeplinesc cerințele planului de continuitate a activității.

Stocarea pentru recuperarea afacerii în caz de incident sau dezastru este menținută și stocată în locații sigure și securizate. Zipper are obligația de a informa abonații și orice terțe părți despre incidentele apărute în activitatea de furnizare a serviciilor.

13. Încetarea serviciului de arhivare în centrul de date

LTA se încheie:

- cu o decizie a Consiliului de Administrație al ZIPPER;
- printr-o decizie a autorității care exercită supravegherea serviciilor de marcare temporală;
- printr-o hotărâre judecătorească;
- la lichidarea sau încetarea operațiunilor ZIPPER.

ZIPPER se asigură că potențialele perturbări pentru abonați și părți sunt reduse la minimum ca urmare a încetării serviciilor ZIPPER și, în special, asigură menținerea continuă a informațiilor necesare pentru verificarea corectitudinii serviciilor.

Dacă este necesar ca ZIPPER LTA să înceteze să funcționeze, ZIPPER va depune eforturi rezonabile din punct de vedere comercial pentru a notifica abonații și părțile care se bazează cu privire la o astfel de încetare înainte de încetarea LTA.

13.1 Păstrarea probelor serviciului de arhivare electronică

- ✓ Perioada de păstrare a dovezilor colectate este în conformitate cu legislația națională și este în conformitate cu recomandările ETSI TS 119 312;
- ✓ Confidențialitatea și integritatea înregistrărilor curente și arhivate ale funcționării Serviciului sunt păstrate și arhivate în conformitate cu practica comercială a Zipper;
- ✓ Timpul utilizat pentru înregistrarea evenimentelor, așa cum este necesar în jurnalul de evenimente, este sincronizat cu UTC cel puțin o dată pe zi;
- ✓ Evenimentele sunt înregistrate într-un mod care nu poate fi șters sau distrus cu ușurință;
- ✓ Același profil de conservare se aplică pe toată perioada de conservare a dovezii;
- ✓ Perioada de valabilitate a dovezilor este prelungită prin utilizarea unor algoritmi criptografici siguri și fiabili;
- ✓ Formatul de dovezi din această politică respectă cerințele IETF RFC 6283, precum și CAdES ETSI EN 319 122, XAdES ETSI EN 319 132 și PAdES ETSI EN 319 142.

Dacă este necesar, Zipper extinde valabilitatea dovezilor la arhivă. În timpul perioadei de arhivare,

serviciul de arhivare verifică dacă dovezile pot fi utilizate pentru a atinge scopul corespunzător de conservare. Acest lucru poate fi amenințat dacă algoritmul criptografic nu mai poate fi de încredere sau certificatul administratorului arhivei este revocat. În astfel de cazuri, Zipper extinde dovezile înainte ca acestea să poată fi folosite pentru a atinge scopul arhivării.

14. Fiabilitate organizațională

ZIPPER LTA se asigură că organizația sa este fiabilă în conformitate cu ETSI EN 319 421. ZIPPER are stabilitatea financiară și resursele necesare pentru a funcționa în conformitate cu această declarație de politică și practică.