

APROBAT

GUVERNANȚA PMO

DORU VIJIANU

JUDIT FEKETE

MIRELA OJOG

**-Autoritatea Zipper Services-
Serviciul calificat de păstrare (QPS)
pentru semnături/sigilii electronice calificate (QES)
Disclosure Statement**

**ACEST DOCUMENT ESTE PROPRIETATEA ZIPPER SERVICES S.R.L.
COPIEREA NEAUTORIZATĂ NU ESTE PERMISĂ**

Istoric ediții			
Ediție	Data și descrierea modificării	Gata	Aprobat
1	18.09.2025 – Prima ediție	Judit Fekete	Mirela Ojog

Annex A. Conținut

1. INTRODUCERE	3
2. ADMINISTRAREA DOCUMENTELOR	3
3. PROCEDURA DE APROBARE	4
4. DENUMIREA ȘI IDENTIFICATORUL DOCUMENTULUI	4
6. CLASE ȘI NIVELURI DE SEMNATURI/SIGILII.....	5
7. MODEL, MECANISM ȘI SCHEMA	7
7.1 MODEL.....	7
7.2 MECANISM	7
7.3 SCHEMA.....	8
7.4 VALIDARE.....	8
7.5 ARHIVA/STOCARE	9
7.6 SCOPURI DE CONSERVARE PE TERMEN LUNG	9
7.7 DOVEZI PRIVIND SCOPURILE DE CONSERVARE PE TERMEN LUNG	9
7.8 ADMINISTRAREA DECLARAȚIILOR DE POLITICA ȘI PRACTICA	9
8. SERVICIU DE CONSERVARE PE TERMEN LUNG	10
PROCEDURI DE BAZA.....	10
8.1 ÎNCARCARE/PASTRARE	10
8.2 DESCARCA.....	11
8.3 AFIȘAREA UNUI DOCUMENT PASTRAT	11
8.4 ȘTERGEREA UNUI DOCUMENT ELECTRONIC PASTRAT	12
9. REZILIEREA CONTRACTULUI DE SERVICII	12
10. APLICABILITATE	12
11. DREPTURILE ȘI OBLIGAȚIILE UTILIZATORILOR ȘI ALE PARȚILOR DE INCREDERE	12
12. RESPONSABILITATEA UTILIZATORULUI	12
13. OBLIGAȚIILE UTILIZATORULUI	12
14. DREPTURILE UTILIZATORULUI	12
15. RESPONSABILITATEA PARȚII DE INCREDERE.....	13
16. GARANȚIE LIMITATA ȘI DECLINAREA RASPUNDERII/LIMITAREA RASPUNDERII IN FURNIZAREA SERVICIULUI	13
17. ACORDURI APLICABILE, CPS, CP	13
18. POLITICA/DECLARAȚIE DE CONFIDENȚIALITATE	14
19. POLITICA DE RAMBURSARE	14
20. LEGEA APLICABILĂ, RECLAMAȚII ȘI SOLUȚIONAREA LITIGIILOR	14
21. EVALUARI ALE CONFORMITAȚII, MARCI DE INCREDERE/LOGO-URI ȘI AUDIT	15

1. Introducere

Zipper Services (denumit în continuare Zipper) oferă utilizatorilor săi serviciul de păstrare calificată a semnăturilor/sigiliilor electronice calificate în conformitate cu art. 34 și art. 40 din Regulamentul (EU) nr. 910/2014 și Regulamentul (UE) 2024/1183 (eIDAS 2.0) și este înregistrat în lista de încredere a furnizorilor europeni de servicii de încredere, precum și în registrul furnizorilor români de servicii de încredere ținut de Autoritatea pentru Digitalizarea României (ADR).

Acest document este declarația **de dezvăluire** a furnizorului de servicii de încredere calificat (QTSP) Zipper privind păstrarea calificată a semnăturilor/sigiliilor electronice calificate. Declarația de dezvăluire se bazează pe structura definită în Anexa A la documentul ETSI TS 319-411-1 și are scop informativ pentru utilizatorii SERVICIULUI. Acest document nu înlocuiește și nu înlocuiește Politica, Codul de Practică și Proceduri (PCPP) pentru SERVICIU, conform căruia se asigură păstrarea calificată pe termen lung a semnăturilor și sigiliilor electronice calificate.

Acest document este pus la dispoziția publicului la <https://pki.ca.ezipper/policies>

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

2. Administrarea documentelor

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

3. Procedura de aprobare

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

Abonații care nu acceptă termenii noi, modificați ai declarației de dezvăluire trebuie să facă o declarație adecvată în termen de 15 zile de la data publicării noii versiuni a PCPP. Acest lucru va duce la rezilierea contractului aferent serviciilor QPS furnizate.

4. DENUMIREA ȘI IDENTIFICATORUL DOCUMENTULUI

Numele complet al acestui document este "Serviciul de conservare calificat pentru semnături/sigilii electronice calificate (QPSES) (Qualified preservation service) Policy, Code of Practice and Procedures (PCPP)" și identificator de obiect (OID):

Denumirea documentului	Identificator de obiect (OID)
Serviciul de conservare calificat (QPS) pentru semnăturile/sigiliile electronice calificate (QES) - Politică, Cod de practică și proceduri (PCPP)	1.3.6.1.4.1.57570.4.3.2 4=> nod de clasificare a serviciului 3 => servicii de conservare (subarbore pentru politicile legate de conservare) 2=> variantă de conservare calificată

Serviciul Zipper QPS este aplicabil numai pentru documentele electronice, pe baza profilurilor de certificat pentru semnături electronice în conformitate cu eIDAS (Regulamentul (UE) nr. 910/2014).

0.4.0.19511.1.2 este un identificator de obiect (OID) ETSI care se referă la un certificat calificat (QC) în conformitate cu Regulamentul UE eIDAS, definit în ETSI EN 319 412-1.

5. Acronime

AUG Obiectiv de augmentare
CA Autoritatea de certificare
CARL Lista de revocare a autorității de certificare
LCR Lista de revocare a certificatelor
DN Nume distins
EUMS Stat membru al Uniunii Europene
OCSP Protocol de stare a certificatului on-line
QTSP - Furnizor de servicii de încredere calificat;
CSA (Certificate Status Authority) - Autoritate de încredere pentru verificarea stării (OCSP)
ER - Înregistrarea probelor
PCPP - Politică, cod de practică și proceduri
PO - Obiect de conservare
PDO - Obiect de date de conservare
PDS - Păstrarea semnăturilor digitale
PGD - Păstrarea datelor generale
POC - Container de obiecte de conservare
PRP - Protocolul serviciului de conservare
PRS - Serviciu de conservare
PSP - Furnizor de servicii de conservare
QC - Certificat calificat
QES - Semnătură electronică calificată sau sigiliu electronic calificat
QPS – Serviciu de conservare calificat
QVS – Serviciu de validare calificat
SubDO - Obiect de date de trimitere
SigS - Serviciu de creare de semnături digitale
TS - Serviciu de încredere
TL - Lista de încredere
TSA - Autoritatea de marcare temporală
TSP - Furnizor de servicii de încredere
UTC - Timp universal coordonat
ValS - Serviciu de validare
Zipper Services SRL - Zipper
WST - serviciu de conservare cu depozitare
WTS - servicii de conservare cu depozitare temporară

6. Clase și niveluri de semnături/sigilii

DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1506 A COMISIEI A DEFINIT SPECIFICAȚIILE TEHNICE ȘI STANDARDELE REFERITOARE LA CLASELE ȘI NIVELURILE DE SEMNĂTURI ELECTRONICE/SIGILII ELECTRONICE CALIFICATE ȘI AVANSATE, PE CARE FIECARE STAT MEMBRU AL Uniunii ar trebui să le sprijine și care sunt acceptate de autoritățile publice ale statelor membre având în vedere interoperabilitatea lor transfrontalieră și nivelul de securitate necesar în scopuri comerciale specifice:

Tip	Standard curent	Cea mai recentă versiune	Titlu
Profil de referință XAdES	ETSI EN 319 132-1	V1.3.1 (2024-07)	<i>semnături electronice și infrastructuri (ESI); Semnături digitale XAdES; Partea</i>
Cod: QPS-DS-ZS		Editia: 1	Clasa : Public
		Pagina 5 din 15	

The user should ensure that the present copy is the most recent revision.

Tip	Standard curent	Cea mai recentă versiune	Titlu
Profil de bază CADES	ETSI EN 319 122-1	V1.3.1 (2023-06)	<i>1: Blocuri de construcție și semnături de bază semnături electronice și infrastructuri (ESI); Semnături digitale CAdES; Partea 1: Blocuri de construcție și semnături de bază</i>
Profil de referință PAdES	ETSI EN 319 142-1	V1.2.1 (2024-01)	<i>semnături electronice și infrastructuri (ESI); semnături digitale PAdES; Partea 1: Blocuri de construcție și semnături de bază</i>
Profil de bază ASiC	ETSI EN 319 162-1	V1.2.1 (2024-04)	<i>semnături electronice și infrastructuri (ESI); Containere de semnături asociate (ASiC); Partea 1: Blocuri de construcție și containere de bază</i>

DECIZIA (art. 1 și 3), în conformitate cu Regulamentul 910/2014, aprobă următoarele semnături/sigilii avansate în formate CMS, XML și PDF la nivelurile de conformitate B, T și LT, care ar trebui să fie recunoscute de statele membre.

DECIZIA (articolele 2 și 4) aprobă condițiile în care se confirmă valabilitatea unei semnături/sigiliu electronic avansat:

- (1) certificatul care acceptă semnătura electronică avansată era valabil la momentul semnării și, în cazul în care semnătura electronică avansată este susținută de un certificat calificat, certificatul calificat care acceptă semnătura electronică avansată era, la momentul semnării, un certificat calificat pentru semnătură electronică în conformitate cu anexa I la Regulamentul (UE) nr. 910/2014 și că a fost emis de un prestator de servicii de asigurare a încrederii calificat;
- (2) datele de validare a semnăturii corespund datelor furnizate părții care se bazează;
- (3) setul unic de date care reprezintă semnatarul este furnizat corect părții care se bazează pe bază;
- (4) utilizarea oricărui pseudonim este indicată în mod clar părții care se bazează în cazul în care a fost utilizat un pseudonim în momentul semnării;
- (5) atunci când semnătura electronică avansată este creată de un dispozitiv calificat de creare a semnăturii electronice, utilizarea oricărui astfel de dispozitiv este indicată în mod clar părții care se bazează;
- (6) integritatea datelor semnate nu a fost compromisă;

(7) cerințele prevăzute la articolul 36 din Regulamentul (UE) nr. 910/2014 au fost îndeplinite la ora semnării;

(8) Sistemul utilizat pentru validarea semnăturii electronice avansate oferă părții care se bazează pe rezultatul corect al procesului de validare și permite părții care se bazează pe detectarea oricăror probleme relevante de securitate.

Zipper este un QTSP pentru validarea semnăturilor/sigiliilor electronice și generează un raport de validare bazat pe ETSI EN 319 102-1, folosind QVS Zipper "serviciu de validare calificat" (verifică starea certificatului, revocarea, profilul de semnătură, algoritmi etc.). Raportul de validare este semnat cu un sigiliu electronic calificat (emis pentru Zipper) și TS calificat încorporat.

7. Model, mecanism și schemă

7.1 Model

Această versiune a SERVICIULUI este implementată și furnizată cu o stocare/arhivă proprie asociată și urmează modelul WST (serviciu de conservare cu stocare) conform specificațiilor ETSI TS 119 511.

7.2 Mecanism

Semnătura/sigiliul calificat/avansat cu clasă extinsă (AdES) și nivelul LTA oferă un mecanism intern prin care rămâne verificabil pe o perioadă lungă de timp. Clasa AdES cu semnătură/sigiliu, nivelul B-LTA este cea mai potrivită pentru un recipient de conservare pe termen lung.

Versiunea curentă a SERVICIULUI utilizează containerul de conservare pentru obiectul de date semnat/sigilat cu clasa AdES și nivelul LTA de semnătură/sigilare.

Serviciul calificat de conservare definit în prezentul document oferă interfața de conservare așa cum este specificat în clauza 5 și utilizează Zipper Time-Stamping Authority (TSA), care emite marcaje temporale calificate conform ETSI EN 319 422. Serviciul utilizează un serviciu de validare calificat (QValS) (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).

Serviciul de conservare calificat elaborat de Zipper oferă interfețe pentru accesul la resursele sistemului sau la serviciile externe. Serviciul calificat de conservare pe termen lung folosește propriul spațiu de depozitare sub controlul Zipper. Serviciul are scopul de a păstra datele generale și de a asigura dovezi ale trimiterii obiectului de date.

7.3 Schemă

Schema de conservare pe termen lung este determinată de conservarea pe termen lung și de înregistrarea probelor care este aplicată pentru a atinge un scop specific sau pentru a stabili scopuri de conservare a documentelor electronice. Versiunea actuală a SERVICIULUI furnizat de QTSP Zipper implementează conservarea pe termen lung:

- Profil de conservare F1 - Schema de conservare cu stocare pe baza de evidențe
- Profil de conservare F3 - Schema de conservare cu mărire a semnăturii și cu stocare

7.4 Validare

Validarea în cadrul SERVICIULUI este un proces de verificare a valabilității semnăturilor digitale ale documentelor electronice și a marcajelor temporale înainte de conservare.

SERVICIUL utilizează un proces de validare intern sau un serviciu de validare calificat extern pentru a verifica starea de valabilitate a unei semnături/sigiliu înainte de stocarea unui document electronic prin containerul de depozitare.

Rapoarte de validare generate atunci când semnătura/sigiliul a fost verificat cu certificate, CRL-uri/OCSP-uri utilizate în timpul validării. Zipper QSP, peste QVS creează raportul de validare care este conform cu ETSI EN 319 102-1 ca document XML definit de ETSI TS 119 102-2. Raportul de validare conține următoarele elemente despre semnătura electronică validată:

- Element de raport de validare a semnăturii, care conține starea generală de validare a semnăturii pentru semnătură, precum și informații suplimentare privind validarea semnăturii efectuată (clauza 4.3).
- Elementul obiectelor de validare a semnăturii, care conține materialele colectate în timpul procedurii de validare, cum ar fi CRL-urile, ancorele de încredere, răspunsurile OCSP etc. și dovada existenței în cel mai timpuriu moment al existenței obiectului (clauza 4.4.)
- Elementul de informații al validatorului, care identifică entitatea care validează semnătura. (clauza 4.5.)
- Semnătura raportului de validare, care conține semnătura raportului de validare. (clauza 4.6.)

Raportul de validare calificat va fi stocat asociat cu pachetul de dovezi de conservare, deoarece dovedește că **la un moment dat**, semnătura/sigiliul a fost valabil conform eIDAS, conține întregul context de validare (algoritmi, lanțuri de certificate, stare de revocare) și reduce povara revalidării în viitor - serviciul de validare oferit de Zipper QVS marcă timp QVR în sine pentru a-i garanta integritatea. Zipper QPSES a implementat o dovadă de înregistrări este în conformitate cu IETF RFC 4998. Această politică este listată în profilul de conservare, care o face cunoscută utilizatorilor QPSES și terților.

7.5 Arhivă/Stocare

Datele constând în software, arhive de date sau informații de audit sunt păstrate în siguranță într-o infrastructură specială în Zipper Data Center cu control implementat al accesului. Centrele de date îndeplinesc următoarele condiții:

- asigurarea securității și integrității datelor, la nivelul securității fizice și al accesului prin mijloace informatice;
- disponibilitatea serviciului de arhivare electronică și copia de rezervă a informațiilor stocate.

Disponibilitatea păstrată a 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.

7.6 Scopuri de conservare pe termen lung

SERVICIUL susține următoarele obiective pentru conservarea pe termen lung:

- Dovada integrității unui document electronic (semnătură/sigiliu);
- Dovada existenței (la un moment dat/în trecut) a unui document electronic (semnătură/sigiliu);
- Păstrarea documentelor electronice semnate/sigilate și menținerea stării de valabilitate a semnăturilor/sigiliilor (documente electronice) pe perioade lungi de timp;
- Menținerea dovezilor de valabilitate (status) a semnăturilor/sigiliilor electronice (documente electronice) pe perioade lungi de timp.

7.7 Dovezi privind scopurile de conservare pe termen lung

SERVICIUL susține și oferă următoarele dovezi cu privire la scopurile de conservare pe termen lung:

- Dovada integrității unui document electronic (semnătură/sigiliu);
- Dovada existenței (la un moment dat/în trecut) a unui document electronic (semnătură/sigiliu);
- Dovada stării de valabilitate a semnăturilor/sigiliilor (documente electronice).

Aceste dovezi se bazează pe schema de conservare pe termen lung implementată, prin care materialele de probă sunt colectate, îmbunătățite și stocate împreună cu documentele/fișierele electronice semnate/sigilate inițial în Arhiva SERVICIULUI.

7.8 Administrarea declarațiilor de politică și practică

Politica și Declarația de practică a Furnizorului sunt supuse managementului administrativ, iar aprobarea și modificările ulterioare sunt făcute de persoanele dedicate Zipper. Aceste persoane alcătuiesc echipa de management al politicilor.

Sunt admisibile modificări, modificări și completări, care nu afectează drepturile și obligațiile care

decurg din prezentul document și din acordul standard de servicii dintre Furnizor și Utilizatori/părțile de bază. Declarația de politică și practică trebuie revizuită cel puțin o dată pe an pentru a reflecta cerințele potențiale și cerințele prelabile pentru modificările nivelurilor de securitate ale algoritmilor, formatelor și profilurilor semnăturilor/sigiliilor. Fiecare nouă versiune trimisă și aprobată a acestui document va fi publicată imediat pe site-ul web al Furnizorului.

Declarația de politică și practică a furnizorului pentru SERVICIU trebuie utilizată împreună cu următoarele documente pentru servicii calificate de:

- Zipper QVS pentru semnături/sigilii electronice
- Zipper QTSA.

8. SERVICIU de conservare pe termen lung

Sarcina principală a SERVICIULUI este păstrarea pe termen lung a valabilității semnăturii sau a sigiliului electronic de pe documentul electronic. În acest sens și în conformitate cu Politica, SERVICIUL nu acceptă păstrarea obiectelor de date (documente) fără semnătură/sigiliu.

Proceduri de bază

8.1 Încărcare/Păstrare

- Încărcarea documentului electronic: SERVICIUL încarcă documentul, care trebuie arhivat, numai după identificarea abonatului/transmițătorului într-o sesiune/procedură securizată. Sesiunea securizată asigură integritatea și confidențialitatea documentului încărcat.
- Politica și Declarația de practică informează Abonatul/Transmițătorul cu privire la tipul de semnătură/sigiliu pe documentul acceptat de SERVICIU, modul în care sunt validate semnăturile și sigiliile electronice și care sunt condițiile de încărcare a documentelor.
- Valabilitatea semnăturii electronice sau a sigiliilor documentului primit de SERVICIU este validată prin materialul complet de validare pe termen lung prin intermediul serviciului de validare calificat Zipper QSVS. Validarea se poate baza pe un material de validare parțial sau complet pe termen lung, atașat la o semnătură sau la un sigiliu electronic. Orice informație încă necesară pentru validare și pentru un material de probă pe termen lung este colectată din surse interne sau externe și este păstrată împreună cu documentul. Zipper QSVS generează un raport de validare bazat pe ETSI EN 319 102-1, folosind Zipper "serviciu de validare calificat" QVS (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.
- Validarea va avea ca rezultat o stare TOTAL_FAILED OT TOTAL_PASSED, NEDETERMINATĂ, 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
- 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.
- SERVICIUL stochează containerul păstrat încărcat criptat, pe Zipper Data Center Object Storage.
- Dacă procesul de compilare a materialului dovedit eșuează, Furnizorul (SERVICIUL) notifică Abonatul printr-un mesaj de eroare. Pe baza mesajului de eroare, documentul și motivul respingerii ar trebui să fie clar stabilite. În cazul în care verificarea acceptării documentului electronic nu este confirmată Abonatului în termenul specificat, se presupune că Furnizorul (SERVICIUL) nu a acceptat documentul electronic.
- Furnizorul este responsabil pentru stocarea POC și asigurarea recipientului de valabilitate pe termen lung numai după trimiterea unei confirmări pozitive pentru acceptarea documentului electronic pentru păstrare.

8.2 Descărca

Furnizorul, prin intermediul SERVICIULUI, se asigură că Abonatul își poate descărca documentele stocate în Arhivă și materialele respective pentru validare pe termen lung (materiale dovezi) pe durata Contractului de servicii.

1. Abonatul are acces la documente electronice și la materiale de validare pe termen lung (dovezi), numai printr-un canal securizat
2. SERVICIUL asigură că fiecare Abonat are acces doar la documente electronice și materiale de validare pe termen lung, pe care este efectiv autorizat să le acceseze.

8.3 Afișarea unui document păstrat

SERVICIUL oferă Abonatului posibilitatea de a-și vizualiza containerele/documentele păstrate în aplicația RepoZip LTA. Abonatul are acces doar la documente și materiale de validare pe termen lung, pe care este efectiv autorizat să le acceseze.

8.4 Ștergerea unui document electronic păstrat

SERVICIUL asigură, la cererea Abonatului, ștergerea selectivă a documentelor și a tuturor materialelor de validare pe termen lung corespunzătoare (dovezi) păstrate în Arhiva RepoZip. Ștergerea înseamnă ștergerea fizică a unui document electronic păstrat într-un mod în care acesta nu poate fi restaurat ulterior (sau numai cu costuri financiare nerezonabil de mari). Ștergerea se realizează pe întregul sistem al Furnizorului prin ștergerea oricărei copii salvate a documentului electronic.

9. Rezilierea contractului de servicii

La rezilierea Contractului pentru SERVICIU, Furnizorul va furniza documentele și materialele de validare pe termen lung, a căror păstrare a Abonatului a ordonat, pentru a fi descărcate de către Abonat sau de către o altă persoană autorizată. După reziliere, Furnizorul va șterge documentele și materialul de validare pe termen lung al Abonatului. Formatul de export va fi un format standardizat (Associated Signature Container Extended (ASiC-E) conform ETSI EN 319 162-1 -clauza 4.4). Coletele de export sunt furnizate numai unei persoane fizice sau juridice autorizate.

10. Aplicabilitate

A se vedea secțiunea 6 și secțiunea 7 din prezentul document.

11. Drepturile și obligațiile utilizatorilor și ale părților de încredere

12. Responsabilitatea utilizatorului

Responsabilitatea Utilizatorului atunci când utilizează SERVICIUL este stabilită de Acordul de servicii și de Declarația de politică și practică a Furnizorului.

13. Obligațiile utilizatorului

Obligația Utilizatorului este de a acționa în conformitate cu termenii contractuali și cu Declarația de Politică și Practică a Furnizorului în timpul utilizării SERVICIULUI.

Obligațiile Utilizatorului sunt determinate de termenii și procedurile Declarației de politică și practică pentru acest SERVICIU calificat, de contractul de servicii și de condițiile standard ale acestuia care fac parte integrantă din Politica comună a Furnizorului.

14. Drepturile utilizatorului

Utilizatorii au dreptul de a utiliza SERVICIUL în conformitate cu Declarația de politică și practică a Furnizorului pentru Serviciul de conservare pe termen lung calificat.

15. Responsabilitatea părții de încredere

Părțile care se bazează pe baza discreției lor și/sau a politicilor lor cu privire la modul de acceptare și utilizare a semnăturilor și sigiliilor păstrate. În timpul verificării valabilității pentru menținerea nivelului de securitate garantat de SERVICIU este necesar ca Partea de Încredere să acționeze cu prudență, de aceea se recomandă:

- Evaluarea conformității cu Declarația de Politică și Practică a Furnizorului pentru SERVICIU;
- să utilizeze medii și aplicații IT fiabile;
- verifică răspunsul curent CRL sau OCSP;
- luați în considerare orice restricție în legătură cu utilizarea sigiliului de semnătură care este inclus în Declarația de politică și practică pentru SERVICIU.

16. Garanție limitată și declinarea răspunderii/limitarea răspunderii în furnizarea SERVICIULUI

Zipper ca QTSP declară și garantează următoarele:

- cerințele și procedurile operaționale ale SERVICIULUI sunt în conformitate cu Declarația de politică și practică a Furnizorului respectiv;
- se păstrează numai formatele/profilurile specificate de semnături/sigilii;
- materialele de validare a dovezilor eliberate de SERVICIU corespund statutului semnăturii/sigiliului la momentul validării și nu la momentul aplicării/utilizării pentru un anumit scop comercial
- respectarea cerințelor de confidențialitate a informațiilor dintr-un document/dosar semnat/sigilat;
- Disponibilitatea serviciului 24x7;

Zipper nu își asumă responsabilitatea pentru:

- Indisponibilitatea SERVICIULUI din cauza dezastrelor naturale, războiului, telecomunicațiilor/perturbărilor energetice etc.;
- Aplicabilitatea ilegală a semnăturilor/sigiliilor validate tehnic de SERVICIUL în scopuri comerciale specifice (aplicații) Aplicabilitatea ilegală a semnăturilor/sigiliilor validate tehnic de SERVICIUL în scopuri comerciale specifice (aplicații).

17. Acorduri aplicabile, CPS, CP

Serviciul de conservare calificat (QPS) pentru semnături/sigilii electronice calificate (QES)

Politicile, Codul de practică și procedurile pot fi găsite în depozitul de documente ZIPPER la

<https://pki.ca.ezipper.ro/repository/policies.php>

În consecință, Acordul de abonat al serviciilor de încredere, Termenii și condițiile privind deținătorii/părțile de încredere ale SERVICIULUI pot fi găsite pe adresa web de mai sus.

18. Politică/Declarație de confidențialitate

Angajamentul de respectare a confidențialității explică toate aspectele referitoare la prelucrarea datelor cu caracter personal și asigură respectarea tuturor principiilor legate de prelucrare stabilite de legislația în vigoare, în special de Regulamentul (UE) 679/2016 (GDPR), activități desfășurate de companie în calitate de Persoană Autorizată a Operatorului (pe perioada de executare a contractelor cu clienții săi).

ZIPPER prelucrează datele cu caracter personal în conformitate cu legislația aplicabilă privind protecția datelor în vigoare. Pentru mai multe detalii, vă rugăm să consultați Declarația de confidențialitate ZIPPER

<https://pki.ca.ezipper.ro/repository/compliance.php>

Toate informațiile care au devenit cunoscute în timpul furnizării serviciilor și care nu sunt destinate divulgării sunt confidențiale. Abonatul are dreptul de a obține informații de la ZIPPER cu privire la prelucrarea datelor sale cu caracter personal în conformitate cu legislația aplicabilă.

ZIPPER are dreptul de a dezvălui informații despre Abonat unei terțe părți care, în conformitate cu legea relevantă sau o hotărâre judecătorească, are dreptul să primească astfel de informații. 10.5 ZIPPER poate publica date statistice nepersonalizate despre serviciile sale.

19. Politica de rambursare

ZIPPER se străduiește să ofere cel mai înalt nivel de calitate a serviciilor de încredere pe care le oferă și le oferă. ZIPPER depune eforturi pentru a asigura cel mai înalt nivel de calitate a serviciilor sale. Cu toate acestea, Abonatul are dreptul de a se retrage din contractul de cumpărare din orice motiv în cazul în care achiziționarea Serviciului de Validare se efectuează prin internet sau printr-un telefon al Abonatului.

Exercitarea acestui drept se va face în scris de către Abonat la ZIPPER, prin trimiterea unui e-mail către suport.pki@ezipper.ro în termen de 14 zile de la data achiziției.

Sub rezerva secțiunii anterioare, ZIPPER poate gestiona rambursările de la caz la caz.

20. Legea aplicabilă, reclamații și soluționarea litigiilor

Orice litigii legate de serviciile de încredere furnizate în conformitate cu acești termeni vor fi guvernate în toate privințele și interpretate în conformitate cu legile din România.

În măsura permisă de lege, părțile vor încerca inițial să rezolve orice litigiu pe cale amiabilă și dacă litigiul nu este soluționat în termen de treizeci (30) de zile de la cererea inițială, atunci instanțele din București, România vor avea competența exclusivă de a o judeca și de a o soluționa.

Orice solicitări de litigiu sau reclamații trebuie trimise la informațiile de contact furnizate în acești Termeni și condiții.

21. Evaluări ale conformității, mărci de încredere/logo-uri și audit

Audituri pentru verificarea conformității cu prevederile procedurale și legale, în special conformitatea cu documentul Serviciul de conservare calificat (QPS) pentru semnături/sigilii electronice calificate (QES)

Politica, Codul de Practică și Procedura FURNIZATE DE ZIPPER SERVICES sunt efectuate la fiecare 24 de luni de către o Autoritate de Evaluare a Conformității, în baza Art. 20 din REGULAMENTUL 910/2014 UE (eIDAS).

22. Puncte de înregistrare și verificare a identității

ZIPPER înregistrează și încheie Contracte de servicii de încredere. Mai multe informații despre acordurile de servicii de încredere pot fi găsite la adresa web: <https://pki.ca.ezipper.ro/>