

APROBAT

GUVERNANȚA PMO

DORU VIJIANU

JUDIT FEKETE

MIRELA OJOG

**-Autoritatea Zipper-
Serviciu de arhivare calificat (QAS)**

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	01.10.2025 – 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. DESCRIEREA SERVICIULUI DE ARHIVARE (DOMENIUL DE APLICARE ȘI CICLUL DE VIAȚA)	7
7.1 MECANISM	7
7.2 PACHETE DE INFORMAȚII — FORMATUL PACHETULUI DE INFORMAȚII	7
7.3 DEPUNEREA TRANSFERULUI	7
7.4 VERIFICAREA ȘI CONSERVAREA PACHETULUI DE INFORMAȚII (CREAREA POC)	8
7.5 ACCES	9
7.6 PASTRARE ȘI ȘTERGERE.....	9
7.7 DOVEZI PRIVIND SCOPURILE DE CONSERVARE PE TERMEN LUNG	10
8. ADMINISTRAREA DECLARAȚIILOR DE POLITICA ȘI PRACTICA	10
9. REZILIEREA CONTRACTULUI DE SERVICII	10
10. DREPTURILE ȘI OBLIGAȚIILE UTILIZATORILOR ȘI ALE PARȚILOR DE INCREDERE	11
1. RESPONSABILITATEA UTILIZATORULUI	11
2. OBLIGAȚIILE UTILIZATORULUI.....	11
3. DREPTURILE UTILIZATORULUI.....	11
4. RESPONSABILITATEA PARȚII DE INCREDERE	11
11. GARANȚIE LIMITATA ȘI DECLINAREA RASPUNDERII/LIMITAREA RASPUNDERII IN FURNIZAREA SERVICIULUI	11
12. ACORDURI APLICABILE, CPS, CP	12
13. POLITICA/DECLARAȚIE DE CONFIDENȚIALITATE	12
14. POLITICA DE RAMBURSARE	13
15. LEGEA APLICABILĂ, RECLAMAȚII ȘI SOLUȚIONAREA LITIGIILOR	13
16. EVALUARI ALE CONFORMITAȚII, MARCI DE INCREDERE/LOGO-URI ȘI AUDIT	13
17. PUNCTE DE INREGISTRARE ȘI VERIFICARE A IDENTITAȚII	13

1. Introducere

Zipper QTSP oferă serviciul de "arhivare electronică" care asigură primirea, stocarea, preluarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe toată perioada de păstrare.

Acest document este declarația **de dezvăluire** a furnizorului de servicii de încredere calificat (QTSP) Zipper privind serviciul de arhivare calificat. 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 Procedurile (PCPP) pentru SERVICIUL de arhivare, conform căruia este furnizat un serviciu calificat de arhivare pe termen lung.

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

<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. 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)
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

Serviciul Zipper QAS 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.

QAS este destinat Abonaților care au nevoie de arhivarea 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, în condițiile art. 8 alin. (2) și (3) din Legea română nr. 135/2007, republicată.

5. Acronime

CA Autoritatea de certificare
LCR Lista de revocare a certificatelor
OCSF Protocol de stare a certificatului on-line
QTSP Furnizor de servicii de încredere calificat
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
PSP - Furnizor de servicii de conservare
RepoZip - Aplicația Zipper Archiving, înregistrată în Registrul Român al sistemelor de arhivare electronică <https://www.adr.gov.ro/arhivare-electronica/>
QC - Certificat calificat
QES - Semnătură electronică calificată sau sigiliu electronic calificat
QPS – Serviciu de conservare calificat
QVS – Serviciu de validare calificat
QAS – Serviciu de arhivare calificat
SubDO - Obiect de date de trimitere
QTSP – Furnizor de servicii de încredere calificat
TSA - Autoritatea de marcare temporală
Zipper Services SRL - Zipper
WST - serviciu de conservare cu depozitare

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 1: Blocuri de construcție și semnături de bază</i>
Profil de bază CAdES	ETSI EN 319 122-1	V1.3.1 (2023-06)	<i>semnături electronice și infrastructuri (ESI); Semnături digitale CAdES; Partea 1: Blocuri de construcție și semnături de bază</i>

Tip	Standard curent	Cea mai recentă versiune	Titlu
Profil de referință PAdES	ETSI EN 319 142-1	V1.2.1 (2024-01)	<i>semnături electronice și infrastructuri (ESl); 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 (ESl); 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 oricărui

probleme relevante de securitate.

7. Descrierea serviciului de arhivare (domeniul de aplicare și ciclul de viață)

7.1 Mecanism

Zipper QAS utilizează următoarele servicii:

- Zipper QPS: este implementat și prevăzut cu o stocare/arhivă proprie asociată și urmează modelul WST (serviciu de conservare cu stocare) conform specificațiilor ETSI TS 119 511, bazat pe QPS PCPP;
- Zipper QVS pentru validarea semnăturilor/sigiliilor electronice conform ETSI TS 119 441 și ETSI TS 119 442 și generează un raport de validare bazat pe ETSI EN 319 102-1, folosind Zipper 'qualified validation service' QVS (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.
- Zipper QTS emite marcate temporale calificate conform ETSI EN 319 422

Obiectele arhivate utilizează containerul de conservare pentru obiectul de date semnat/sigilat cu clasa AdES și nivelul LTA de semnătură/sigilare.

7.2 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 metadata 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 în alte metadata – de exemplu, data închiderii documentului)

7.3 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.

7.4 Verificarea și conservarea pachetului de informații (crearea POC)

În funcție de tipul documentului, RepoZip face asocierea la nomenclatorul arhivistic al companiei utilizatoare și completarea metadatelor obligatorii (în baza legislației române). Conservarea containerului de obiecte pe baza serviciului de conservare calificat, a schemei de conservare cu mărire a semnăturii/sigiliului și cu depozitare (F3 – conform ETSI ES 119 512 Anexa F) va aplica următoarele verificări:

- Aplicația verifică automat semnătura electronică a documentului. Semnătura/sigiliul emitentului oficial al documentului trebuie să fie valabil și întocmit cu un certificat calificat
- Generați un raport de validare bazat pe ETSI EN 319 102-1, folosind QVS Zipper 'qualified validation service' (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.
- 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_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). Primiți trimiterea este furnizată.
- Creșterea 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 act de identitate unic (IDDoc/POID) pentru identificare în

arhivă. Metadatele create automat sunt generate. "Fișierul electronic" atașat fiecărui document arhivat va conține cel puțin lista de metadate specificată în Legea 135/2007.

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 și se aplică marca temporală calificată (nivel B-LTA)

7.5 Acces

Accesul la sistemul de arhivare electronică RepoZip se realizează prin linii de comunicare securizate între Beneficiar și Furnizor (Servicii Zipper). 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.

7.6 Păstrare și ștergere

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.

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

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 sigur

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.

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 prealabile 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.

9. Rezilierea contractului de servicii

La rezilierea Contractului pentru SERVICIU, Furnizorul va furniza documentele și materialele de validare pe termen lung, a căror arhivare/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. Drepturile și obligațiile utilizatorilor și ale părților de încredere

1. Responsabilitatea utilizatorului

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

2. 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 pentru acest SERVICIU calificat, de contractul de servicii și de condițiile standard ale acestuia care fac parte integrantă din Politica comună a Furnizorului.

3. 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.

4. 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.

11. 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).

12. Acorduri aplicabile, CPS, CP

Documentul Serviciul de arhivare calificat (QPS) Politica, Codul de practică și procedurile poate fi găsit 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.

13. 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.

14. 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.

15. 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.

16. 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).

17. 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/>