

Se aplică pentru/ Applies to:
OID 1.3.6.1.4.1.25017.3.1.3.16

TERMENI și CONDIȚII

privind furnizarea de servicii de încredere
pentru certificate digitale calificate stocate pe
dispozitiv criptografic securizat (token)

Prezentul înscris reprezintă un contract în sensul prevederilor Art. 1270 Cod Civil Român și privește utilizarea unui certificat digital calificat.

Emiterea unui certificat digital implică acceptarea Termenilor și Condițiilor privind furnizarea de servicii de încredere, descriși în continuare.

Furnizarea de servicii de încredere de către certSIGN se face în conformitate cu Codul de Practici și Proceduri al Autorității de Certificare certSIGN Qualified 2023 RSA CA, care este considerat parte integrantă a acestor condiții.

Politicele certSIGN sunt validate prin audit anual efectuat în conformitate cu schema de certificare LSTI-Q055 pentru prestatorii de Servicii de Încredere.

Părțile contractante :

CERTSIGN S.A., cu sediul social în București, Sos. Oltenitei nr. 107 A, cladirea C1, etaj 1, camera 16, sector 4, înregistrată la Registrul Comerțului sub nr. J2006000484402, cod de identificare fiscală RO18288250, cont bancar cu cod IBAN RO90BRDE410SV91167344100 deschis la BRD Sucursala Calderon, 2162 RO01 deschis la OTP Bank Romania SA, S.M.B., denumită în continuare **Prestator sau certSIGN**.

Și

DI/D-na/Mr/Mrs. _____, domiciliat(a) în /residing in localitatea/city _____, judet/sector/district _____, Str./ Street _____, Nr./No. _____, Bloc/Building _____, Sc./Entrance _____, Ap. _____, Cod poștal / Postal Code _____, identificat prin/ identified by BI/CI seria/ serial _____, nr./no _____, emis(ă) la data de/ issued on _____, de către/ by _____, valabil(ă) până la data de/ valid to _____, CNP _____, telefon/ phone _____, denumit în continuare **Subiect/** hereinafter referred to as the **Subject**.

1. Definiții

„**Beneficiar**” reprezintă persoana fizică sau juridică care solicită certificat digital calificat pentru Subiect în temeiul unui raport contractual cu CERTSIGN („Contract”), conform REGULAMENT (UE) nr. 910/2014. În cazul în care Beneficiarul este persoană fizică acesta va avea și calitatea de Subiect.

„**certSIGN**” este prestator de servicii de încredere în condițiile stabilite de Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

„**Condiții Generale**” înseamnă prezentul document „Termeni și condiții privind furnizarea de servicii de încredere pentru certificate digitale calificate stocate pe dispozitiv criptografic securizat”.

„**Servicii de încredere**” reprezintă emiterea, revocarea, reinnoirea cheilor, depozitarea și verificarea stării certificatului prin protocol http utilizând CRL și OCSP, verificarea lanțului (ierarhiei) de încredere, toate acestea în

TERMS AND CONDITIONS

regarding the provision of trust services for qualified digital certificates stored on a secured cryptographic device (token)

This deed is a contract under the provisions of Art. 1270 of the Romanian Civil Code and applies to the use of a qualified certificate.

The issuance of a digital certificate implies the acceptance of the Terms and Conditions on the provision of trust services described below.

The provision of trust services by certSIGN is in accordance with the Certification Practice Statement of certSIGN Qualified 2023 RSA CA Certification Authority, which is considered an integral part of these terms and conditions.

certSIGN policies are validated by annual audit conducted in accordance with the LSTI-Q055 certification scheme for Trust Service providers.

Contracting Parties:

CERTSIGN S.A., having its registered office in Bucharest, 107A, Oltenitei Blvd, C1 building, 1st floor, Sector 4, registered with the Trade Register under no. J2006000484402, with the following Tax Identification Code RO18288250, IBAN code RO90BRDE410SV91167344100 opened with BRD Calderon Branch, hereinafter referred to as the **Provider or certSIGN**.

And

DI/D-na/Mr/Mrs. _____, domiciliat(a) în /residing in localitatea/city _____, judet/sector/district _____, Str./ Street _____, Nr./No. _____, Bloc/Building _____, Sc./Entrance _____, Ap. _____, Cod poștal / Postal Code _____, identificat prin/ identified by BI/CI seria/ serial _____, nr./no _____, emis(ă) la data de/ issued on _____, de către/ by _____, valabil(ă) până la data de/ valid to _____, CNP _____, telefon/ phone _____, denumit în continuare **Subiect/** hereinafter referred to as the **Subject**.

1. Definitions

„**Subscriber**” refers to the natural person or legal entity requesting qualified digital certificates for the Subject pursuant to a contractual relationship with certSIGN ("Agreement") according to the (EU) Regulation 910/2014. If the Subscriber is a natural person, he will also have the status of Subject.

„**certSIGN**” is a trust service provider under the conditions laid down in Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions on the internal market.

„**General Conditions**” refer to this document “Terms and conditions regarding the provision of trust services for qualified digital certificates stored on a secured cryptographic device”.

„**Trust Services**” refer to the issuance, revocation, rekeying, storing and verification of the certificate status by means of the http protocol using CRL and OCSP, trust chain (hierarchy) verification all related to

legatura cu certificatele digitale calificate emise de catre Autoritatea de Certificare "certSIGN Qualified 2023 RSA CA".

„**Subiectul**” este persoana fizică, titular al certificatului digital.

„**Dispozitiv de Creare a Semnăturilor Electronice Calificate**” (QSCD) este un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în Anexa II a Regulamentului (UE) 910/2014 în posesia Subiectului.

„**Codul de Practici și Proceduri al Autorității de Certificare certSIGN Qualified 2023 RSA CA**” (CPP) reprezintă ansamblul practicilor și procedurilor care guvernează furnizarea și utilizarea serviciilor de încredere pentru certificate digitale calificate. CPP este public și se găsește la adresa: <https://www.certsig.ro/ro/document/certsig-qualified-2023-rsa-ca-cod-practici-si-proceduri/>.

„**Sisteme vechi**” reprezintă sistemele CASMB, CJAS și OPSNAJ, precum și toate aplicațiile de cabinete medicale, spitale, farmacii etc. care comunică și sunt compatibile cu sistemele Casei Naționale de Asigurări de Sănătate, precum și sistemele altor institutii publice care necesita lucrul cu certificate care au o lungime de cheie PKI de cel mult 2048 biti. Detalii privind sistemele acceptate de certSIGN în: <https://www.certsig.ro/legacy-systems>.

2. Obiectul

Stabilește termenii și condițiile privind furnizarea și utilizarea Serviciilor de Încredere.

Certificatul digital emis în conformitate cu prezentele Condiții Generale poate fi folosit în Sistemele vechi care nu suportă certificate digitale cu chei mai mari de 2048.

3. Durată

3.1 Intră în vigoare în momentul acceptării/semnării prezentelor Condiții Generale de către Subiect.

3.2 Prezentele Condiții Generale sunt valabile pe toată durata de valabilitate a certificatului.

4. Obligațiile Subiectului

Subiectul are următoarele obligații:

- Să furnizeze către certSIGN date corecte la înregistrarea cererii de certificat;
- Să folosească dispozitivul calificat de creare a semnăturii electronice (QSCD) și aplicațiile software recomandate de certSIGN în cazul în care își generează singur cheile;
- Să genereze perechile de chei numai folosind un Dispozitiv calificat de creare a semnăturii electronice (QSCD) agreat de certSIGN;
- Să ia măsurile necesare care să permită generarea corespunzătoare (de către Subiect, Autoritatea de Înregistrare sau Autoritatea de Certificare) și stocarea în siguranță a cheii private din cadrul unei perechi de chei (pentru a preveni pierderea, compromiterea, modificarea

qualified digital certificates issued by certSIGN Certification Authority "certSIGN Qualified 2023 RSA CA".

"**Subject**" is the natural person, future holder of the digital certificate.

"**Electronic Signature Certificate Creation Device**" (QSCD) is an electronic signature creation device that meets the requirements set out in Annex II of Regulation (EU) 910/2014, in the possession of the Subject.

"**Certification Practice Statement of certSIGN Qualified 2023 RSA CA**" (CPS) is the set of practices and procedures governing the provision and use of trust services for qualified digital certificates. The CPS is public and can be found at: <https://www.certsig.ro/en/document/certsig-qualified-2023-rsa-ca-certification-practice-statement/>

"**Legacy systems**" means the systems of CASMB, CJAS and OPSNAJ, as well as all the applications of medical practices, hospitals, pharmacies, etc. that communicate and are compatible with the systems of the National Health Insurance Fund, as well as systems of other public institutions that require working with certificates that have a PKI key length of 2048 bits or less. Details on these systems supported by certSIGN in: <https://www.certsig.ro/legacy-systems>.

2. Subject matter

It lays down the terms and conditions regarding the provision of trusted services.

The digital certificate issued in accordance with these General Conditions may be used in Legacy Systems that do not support digital certificates with keys greater than 2048.

3. Duration

3.1 These General Conditions enter into force upon the acceptance/signing by the Subject.

3.2 These General Conditions are valid for the duration of the digital certificate validity.

4. Obligations of the Subject

The Subjects undertakes:

- To send to certSIGN correct data upon registration of the certificate request;
- To use the Qualified Electronic Signature Creation Device (QSCD) and software applications recommended by certSIGN if generating their own keys;
- To generate key pairs only using a Qualified Electronic Signature Device (QSCD) approved by certSIGN;
- To take the necessary measures to allow the proper generation (by the Subject, the Registration Authority or the Certification Authority) and the safe storage of the private key within a key pair (to prevent its loss, compromise, alteration and unauthorized use);

Se aplică pentru/ Applies to:
OID 1.3.6.1.4.1.25017.3.1.3.16

și folosirea neautorizată a acesteia);

e. Să schimbe codul PIN de acces la cheia privată de pe token înainte de prima utilizare;

f. Să folosească certificatul digital calificat emis de Autoritatea de certificare certSIGN Qualified 2023 RSA CA cu:

- OID 1.3.6.1.4.1.25017.3.1.3.16 pentru semnătură electronică cu QSCD și care poate fi utilizat în relație cu sisteme vechi, în concordanță cu arile de aplicabilitate și restricțiile stabilite prin CPP;

g. Prin semnarea/acceptarea prezentelor Condiții Generale înțelege că certSIGN pentru a emite certificatul digital calificat trebuie să verifice identitatea Subiectului;

h. Să ceară, de îndată, certSIGN revocarea certificatului, atunci când a pierdut datele de creare a semnăturii electronice sau când are motive să creadă că datele de creare a semnăturii electronice au ajuns la cunoștința unui terț neautorizat sau când informațiile cuprinse în certificat nu mai corespund realității;

i. Subiectul înțelege și acceptă că în cazul introducerii greșite a PIN/PUK de mai multe ori și blocarea token-ului sau deteriorării token-ului din culpa Subiectului, certSIGN va revoca certificatul;

j. Să respecte prevederile CPP;

k. Subiectul este responsabil cu privire la conținutul și natura documentelor pe care va aplica semnătura electronică calificată;

l. Prin acceptarea/semnarea prezentelor Condiții Generale, Subiectul înțelege și este de acord ca certSIGN să utilizeze datele din certificat pentru a pune la dispoziția publicului Registrul de certificate în formă electronică în vederea furnizării Serviciilor de încredere;

m. Prin acceptarea/semnarea prezentelor Condiții Generale, Subiectul ia cunoștință că certSIGN va păstra o copie a actului de identitate al Subiectului în vederea procesării informațiilor necesare exclusiv prestării Serviciilor de încredere. certSIGN păstrează datele și logurile legate de ciclul de viață al certificatelor emise timp de 10 ani de la expirarea certificatului.

n. Prin acceptarea/semnarea prezentelor Condiții Generale, Subiectul înțelege și este de acord că certificatul digital se emite pentru a fi utilizat în Sistemele vechi. Utilizarea certificatului digital în alte scopuri poate atrage revocarea certificatului.

Orice nerespectare de către Subiect a obligațiilor sale va fi considerată o încălcare a prezentelor Condiții Generale.

5. Obligațiile certSIGN

certSIGN are următoarele obligații:

5.1. Să respecte prevederile prezentelor Condiții Generale și ale CPP;

5.2. certSIGN va emite certificatul digital calificat doar după identificarea Subiectului exclusiv pe baza actului de identitate, validarea cererii și a informațiilor transmise de

e. To change the token key access PIN code before the first use;

f. To use the qualified digital certificate issued by the Certification Authority certSIGN Qualified 2023 RSA CA with:

- OID 1.3.6.1.4.1.25017.3.1.3.16 for electronic signatures with QSCD that can be used in relation with Legacy systems, as to the scopes and restrictions of the CPS;

g. By signing/accepting these General Conditions, understands that in order for certSIGN to issue the qualified digital certificate, it must verify the Subject's identity;

h. To request, immediately, certSIGN to revoke the certificate, when he has lost the data for creating the electronic signature or when there are reasons to believe that the data for creating the electronic signature has come to the knowledge of an unauthorized third party; or when the essential information contained in the certificate no longer corresponds to reality;

i. The Subject understands and accepts that in case of incorrect introduction of PIN/PUK several times and the blocking of the token or the deterioration of the token due to the fault of the Subject, certSIGN will revoke the certificate;

j. To comply with the provisions of the CPS;

k. The Subject is responsible for the content and nature of the documents to which the electronic signature will be applied;

l. By accepting/signing these General Conditions, the Subject understands and agrees that certSIGN will use the data in the certificate to make the electronic Certificate Repository available to the public for the provision of Trust Services;

m. By accepting/signing these General Conditions, the Subject understands and agrees that certSIGN will keep a copy of the Subject's identity document in order to process the information necessary exclusively for the provision of trusted services. certSIGN retains the data and logs related to the lifecycle of issued certificates for 10 years after certificate expiry.

n. By accepting/signing the present General Conditions, the Subject understands and agrees that the digital certificate is issued for use in the Legacy Systems. Use of the digital certificate for other purposes may result in revocation of the certificate.

Any breach by the Subject of its obligations will be considered a violation of these General Conditions.

5. Obligations of CERTSIGN

certSIGN undertakes:

5.1. To comply with the provisions of the General Conditions herein and the CPS.

5.2. certSIGN will issue the qualified digital certificate only after having identified Subject solely based on the identity document and after having validated the

acesta, în acord cu CPP.

5.3. Să depună toate eforturile pentru a elibera certificatul digital în termen de 5 (cinci) zile lucrătoare, după primirea Contractului, de la data:

i) identificării Subiectului de către un reprezentant certSIGN și a semnării/acceptării prezentelor Condiții Generale ; sau

ii) primirii de către certSIGN a prezentelor Condiții Generale semnate de către Subiect, a copieii actului de identitate, marcată „Conform cu originalul”, semnată și datată de către Subiect și a Declarației autentificate notarial; sau

iii) primirii de către certSIGN a prezentelor Condiții Generale și copieii actului de identitate ambele semnate de către Subiect cu semnătură electronică calificată bazată pe certificat digital calificat valid emis de certSIGN, în conformitate cu art. 3.2.3. din CPP pe care îl puteți citi <https://www.certsig.ro/ro/document/certsig-qualified-2023-rsa-ca-cod-practici-si-proceduri/>

5.4. Să asigure securitatea propriilor sisteme informatice utilizate pentru oferirea serviciilor de încredere, folosind practici recunoscute în domeniu și recomandate de standarde aplicabile;

5.5. certSIGN are obligația să revocare orice certificat în conformitate cu CPP. certSIGN îl va informa de urgență pe Subiect despre revocarea certificatului, împreună cu motivele care au stat la baza deciziei sale. certSIGN va înscrie revocarea certificatului în Registrul de certificate.

5.6. În cazul compromiterii cheilor Autorității de Certificare care a emis certificatul Subiectului, certSIGN are obligația să revocare certificatul(e) în conformitate cu CPP.

5.7. certSIGN informează Subiectul despre expirarea perioadei de valabilitate a certificatului calificat care are o valabilitate de cel puțin 1 an, pe adresa de e-mail din certificat, cu cel puțin 30 de zile înainte de expirare.

6. Acceptarea certificatelor

La primirea unui certificat, Subiectul se angajează să verifice conținutul acestuia, în special corectitudinea datelor. Dacă certificatul prezintă nereguli, greșeli sau orice altă neconcordanță cu datele prezentate pentru înregistrare, Subiectul va sesiza imediat Autoritatea de Certificare a certSIGN în vederea revocării certificatului. Certificatul este considerat acceptat în cazul în care Subiectul îl acceptă fie explicit, la momentul ridicării acestuia de pe site-ul certSIGN, fie implicit, prin trecerea unui număr de 3 zile calendaristice de la data primirii pachetului conținând certificatul (trimis de certSIGN); Acceptarea certificatului este o decizie unilaterală a Subiectului, anterior utilizării lui în efectuarea oricărei operații criptografice.

Pentru fiecare tert sau parte interesată, care utilizează certificate emise de certSIGN, condițiile de utilizare și limitările sunt detaliate în #1.4 și #4.5.2 din CPP.

request and the information submitted by the Subject in accordance with the CPS.

5.3. To make every effort to issue the certificate within 5 (five) working days, after receiving the Agreement, from the date:

i) of Subject identification by a certSIGN representative and the signing/acceptance of these General Conditions; Or

ii) Of receipt by certSIGN of these General Conditions signed by the Subject, along with a copy of the identification document, with the “Certified true copy” specification, signed and dated by the Subject and the Notary Public Authentication Statement; or

iii) when certSIGN receives these General Conditions and a copy of the identification document, with the “Certified true copy” specification, in electronic format, both being signed with a qualified electronic signature based on a qualified digital certificate issued by certSIGN, as per art. 3.2.3 of the CPS, which you can find at: <https://www.certsig.ro/en/document/certsig-qualified-2023-rsa-ca-certification-practice-statement/>

5.4. To ensure the security of his own information systems used for providing trust services, using the practices recognized in the field and recommended by applicable standards;

5.5. CERTSIGN is bound to revoke any certificate, according to the CPS. certSIGN shall immediately notify the Subject of the certificate revocation, together with the reasons for this decision. certSIGN shall register the revocation of the certificate in its Repository.

5.6. If the key of the Certification Authority that issued the Subject's certificate gets compromised, certSIGN will revoke the certificate(s) according to the CPS.

5.7. certSIGN informs the Subject about the expiry of the qualified certificate, which has a validity of at least 1 year, on the email address in the certificate, at least 30 days before the expiry date.

6. Certificate acceptance

Upon receipt of a certificate, the Subject undertakes to verify its contents, in particular the accuracy of the data. If the certificate shows irregularities, mistakes or any other inconsistency with the data submitted for registration, the Subject shall immediately refer the matter to the certSIGN Certification Authority for revocation of the certificate. The certificate is considered accepted if the Subject accepts it either explicitly, at the time of its collection from the certSIGN website, or implicitly, after 3 calendar days from the receipt of the certificate kit (sent by certSIGN); Certificate acceptance is a unilateral decision of the Subject, prior to its use in any cryptographic operation.

Certificate acceptance is a unilateral decision of the Subject, prior to its use in any cryptographic operation.

For each third party or relying party, which uses certificates issued by certSIGN, the conditions of use and limitations are detailed in #1.4 and #4.5.2 from the CPS.

7. Revocare certificat. Efecte

7.1. Subiectul poate solicita revocarea certificatului digital:

- a. online, prin introducerea datelor de identificare: nume, prenume, CNP, selectarea certificatului de revocat, și utilizarea codului de revocare primit de la certSIGN, conform instrucțiunilor de pe site la: <https://www.certsign.ro/ro/resurse/revoca-certificat-eidas/>
- b. În format electronic, prin trimiterea la revocare@certsign.ro a unei cereri semnate cu o semnătură electronică calificată creată utilizând un certificat digital calificat, emis de certSIGN Subiectului
- c. Prin completarea și depunerea cererii de revocare, însoțită de un act original de identitate, la unul din punctele de lucru ale certSIGN. Informații despre punctele de lucru ale certSIGN găsiți la <https://www.certsign.ro/ro/contact/>.

7.2. Revocarea certificatului poate fi făcută în condițiile prevăzute în CPP la cererea Subiectului, beneficiarului, a certSIGN sau a unei autorități competente, în cazuri precum : schimbarea datelor care apar în certificat (de ex. nume sau/si prenume), a CNP sau numărului personal de identificare, încetarea relației contractuale dintre Subiect și Beneficiar, compromiterea cheilor, utilizare ilegală și în altele prevăzute la art. 4.9.1 din CPP.

7.3. Revocarea certificatului digital, indiferent de motiv, nu duce la restituirea prețului sau la o reemitere gratuită a acestuia, ci va atrage încetarea furnizării serviciilor.

7.4. După revocarea din orice motiv a certificatului digital, Subiectul nu va mai avea dreptul să îl folosească.

8. Confidențialitate. Prelucrarea datelor cu caracter personal

8.1. „Informații Confidențiale” înseamnă orice date și/sau informații, indiferent de natura acestora, dezvăluite în mod direct și/sau indirect de către Subiect Prestatorului pe perioada derulării prezentelor Condiții Generale, precum și datele și/sau informațiile despre care Părțile iau cunoștință și/sau la care au acces în timpul/ca efect al executării prezentelor Condiții Generale, indiferent de suportul în/pe care sunt cuprinse/transmise datele și/sau informațiile și indiferent dacă este specificat sau nu ca acestea sunt confidențiale.

8.2. certSIGN se obligă să folosească Informațiile Confidențiale doar în vederea îndeplinirii obligațiilor asumate prin prezentele Condiții generale, să le protejeze și să păstreze confidențialitatea acestora.

8.3. certSIGN va fi exonerată de răspunderea pentru dezvăluirea de informații confidențiale, dacă sunt îndeplinite una sau mai multe dintre următoarele condiții:

- informația era cunoscută în mod legal și fără interdicție de divulgare înainte ca ea să fi fost primită de la Subiect
- informația a fost dezvăluită după ce a fost obținut acordul scris al Subiectului pentru asemenea dezvăluire;
- certSIGN a fost obligată în mod legal să dezvăluie informația.

7. Certificate revocation. Effects

7.1. The subject can request the digital certificate revocation:

- a. online, by entering the identification data: name, surname, CNP, selecting the certificate to be revoked, and using the revocation code received from certSIGN, according to the instructions on the website at: <https://www.certsign.ro/ro/resurse/revoca-certificat-eidas/>
- b. In electronic format, by sending to revocare@certsign.ro an application signed with a qualified electronic signature created using a qualified digital certificate issued by certSIGN to the Subject
- c. By completing and submitting the application, accompanied by an original identity document, at one of the certSIGN's offices. Info on certSIGN working offices are at <https://www.certsign.ro/ro/contact/>.

7.2 The revocation of the certificate can be made under the conditions stipulated in the CPP at the request of the Subject, the beneficiary, certSIGN or a competent authority, in cases such as: change of data appearing in the certificate (e.g. name or / and surname), the CNP or personal identification number, termination of the contractual relationship between the Subject and the Beneficiary, compromise of keys, illegal use and others provided in art. 4.9.1 of the CPP.

7.3 Revocation of the digital certificate, for whatever reason, will not result in a refund of the price or a free re-issue, but will result in termination of the service.

7.4 After the digital certificate is revoked for any reason, the Subject will no longer have the right to use it.

8. Confidentiality. Processing of personal data

8.1. "Confidential Information" means any data and / or information, regardless of its nature, disclosed directly and / or indirectly by the Subject to the Provider during the performance of these General Conditions, as well as the data and / or information of which the Parties become aware; / or to which they have access during / as a result of the execution of these General Conditions, regardless of the medium in / on which the data and / or information are contained / transmitted and regardless of whether or not it is specified that they are confidential.

8.2. CERTSIGN undertakes to use the Confidential Information only for the purpose of fulfilling the obligations undertaken by these General Conditions, to protect it and to keep it confidential.

8.3. certSIGN will be exempted from liability for the disclosure of confidential information if one or more of the following conditions are met:

- the information was legally known and without a disclosure ban before it was received from the Subject
- the information was disclosed after the Submission's written consent for such disclosure has been obtained;
- certSIGN was legally bound to disclose the information.

Se aplică pentru/ Applies to:
OID 1.3.6.1.4.1.25017.3.1.3.16

8.4. certSIGN este operator de date cu caracter personal.

8.5. certSIGN prelucrează datele cu caracter personal aparținând Subiectului în vederea prestării serviciilor de încredere în concordanță cu prevederile REGULAMENTULUI (UE) nr. 910/2014, a Regulamentului UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date („GDPR”) și a altor dispoziții de drept ale Uniunii sau drept intern aplicabile referitoare la protecția datelor.

8.6. În calitate de persoană vizată, Subiectul are drepturile prevăzute de art. 13 – 22 din GDPR.

8.7. În vederea exercitării drepturilor asupra datelor sale cu caracter personal, Subiectul se poate adresa Departamentului Protecția Datelor cu Caracter Personal CERTSIGN la următoarele date de contact:

- adresă de email: dpd@certsign.ro
- adresă poștală: Bdul. Tudor Vladimirescu, nr. 29A, clădirea AFI Tech Parc 1, et.2, București, sector 5.

8.8. Datele din certificat pot fi dezvăluite terților care-și bazează conduita pe serviciile de încredere furnizate de CERTSIGN (în relația cu care Subiectul folosește certificatul), iar în cazul în care terții sunt instituții publice, pot fi dezvăluite și alte date personale din actul de identitate, în afară de cele din certificat, în scopul dovedirii certificării. De asemenea, datele mai pot fi dezvăluite destinatarilor prevăzuți în Nota de informare GDPR.

8.9. Detalii despre prelucrarea datelor cu caracter personal de către certSIGN găsiți în Nota de informare GDPR disponibilă la <https://www.certsign.ro/ro/nota-de-informare-gdpr-pentru-servicii-de-incredere/> .

8.4. certSIGN is a personal data controller.

8.5. certSIGN processes personal data belonging to the Subject in order to provide trust services in accordance with the provisions of REGULATION (EU) no. 910/2014 of EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (“GDPR”) and other applicable provisions of Union or national law relating to the protection of data.

8.6. As a data subject, the Subject has the rights provided in art. 13 - 22 of the GDPR.

8.7. In order to exercise the rights to his/her personal data, the Subject may address the CERTSIGN Personal Data Protection Department to the following contact details:

- email address: dpd@certsign.ro
- mailing address: 29A, Tudor Vladimirescu Bvd., AFI Tech h Park 1, 2nd floor, Bucharest, Sector 5.

8.8. The data in the certificate may be disclosed to third parties who base their conduct on the trust services provided by certSIGN (in relation to which the Subject uses the certificate), and if the third parties are public institutions, other personal data may be disclosed, other than those in the certificate, for the purpose of proving certification. The data may also be disclosed to the addressees provided for in the GDPR Information Note.

8.9. Details on the processing of personal data by certSIGN can be found in the GDPR Information Note available at <https://www.certsign.ro/en/information-note-on-the-processing-of-personal-data/> .

9. Încetarea aplicabilității

9.1. Prezentele Condiții Generale își vor înceta aplicabilitatea în următoarele situații: la expirarea certificatului; la revocarea certificatului; la respingerea cererii de certificat; la neacceptarea certificatului de către Subiect. În cazul în care Subiectul încalcă oricare dintre prevederile prezentelor Condiții Generale sau ale CPP, încetarea se va produce în termen de 30 de zile de la primirea de către Subiect a unei notificări transmise de CERTSIGN cu privire la încălcarea obligațiilor sale, dacă această încălcare nu este remediată în acest interval. Dacă remedierea nu este posibilă încetarea va interveni imediat odată cu comunicarea notificării.

9.2. După încetarea aplicabilității prezentelor Condiții Generale din cauzele prevăzute la art. 10.1, CERTSIGN va revoca certificatul emis și neexpirat, în termen de maxim 24 de ore.

10. Răspundere și excluderi

10.1. Răspunderea certSIGN poate fi atrasă în condițiile și în limitele prevăzute în legea aplicabilă, în prezentele Condiții Generale și în Contract.

9. Cessation of Applicability

9.1 These General Conditions shall cease their applicability under the following situations: upon certificate expiry; upon certificate revocation; upon the rejection of the certificate request; upon non-acceptance of the certificate by the Subject. If the subject breaches any provision of these General Conditions or the CPS the cessation will occur within 30 days from the moment the Subject receives a notification from certSIGN, regarding the failure to fulfill his obligations, if this failure is not remedied during this timeframe. If remediation is not possible termination will take place upon notification.

9.2 After these General Conditions cease to be applicable, due to causes stipulated in art. 10.1, certSIGN will revoke the issued and not expired certificate within 24 hours.

10. Liability and Exceptions

10.1. certSIGN may be held liable under the conditions and within the limits laid down in the applicable law, the General Conditions herein and the contract.

Se aplică pentru/ Applies to:
OID 1.3.6.1.4.1.25017.3.1.3.16

10.2. certSIGN nu este responsabilă pentru:

(a) daunele cauzate de forța majoră și/sau cazul fortuit. Se înțelege prin caz de forță majoră acel eveniment imprevizibil și de neînălăturat produs ulterior perfectării contractului precum: incendiu, cutremur, orice altă calamitate naturală, precum și războiul. Împrejurarea relativ imprevizibilă și relativ invincibilă, neavând caracter extraordinar, precum: grevele, restricțiile legale, nefuncționarea rețelelor de internet, alte asemenea evenimente, definesc cazul fortuit;

(b) daunele cauzate de instalarea și utilizarea aplicațiilor sau dispozitivelor folosite pentru generarea și gestionarea cheilor criptografice, criptare, creare de semnături electronice, care nu îndeplinesc condițiile specificate în CPP;

(c) daunele cauzate de furtul, pierderea sau deteriorarea suporturilor materiale ale certificatelor digitale, stocarea de date eronate în bazele de date ale CERTSIGN și includerea acestora în certificate digitale emise Subiectului, în cazul în care Subiectul a declarat că aceste date sunt corecte.

(d) daunele cauzate de utilizarea necorespunzătoare a certificatelor emise. „Necorespunzător” reprezintă situații cum ar fi: utilizarea unui certificat revocat sau expirat ori în neconcordanță cu scopul declarat al certificatului (respectiv utilizarea lui în alt scop decât în Sistemele vechi), ori cu încălcarea obligațiilor ce revin Subiectului;

(e) prezentarea de către Subiect de date false, inexacte, incomplete sau de acte de identitate false sau declarații false. În cazul compromiterii de către Subiect a procesului de verificare a identității, acesta va fi unicul responsabil pentru daunele suferite de Prestator și de terți din cauza inexactității și/sau falsului informațiilor și documentelor prezentate.

Situațiile prevăzute la (b), (c), (d) și (e) de mai sus sunt în responsabilitatea Subiectului.

10.3. În măsura permisă de lege, niciuna dintre părți nu poate fi obligată la plata de daune pentru prejudicii indirecte, beneficiul sau profitul nerealizat, pierderi de afaceri, clienți sau date.

10.4. În orice caz răspunderea certSIGN va fi limitată la 200 euro pentru fiecare certificat. Răspunderea totală a Prestatorului pentru acoperirea prejudiciilor produse va fi limitată la 10.000 euro indiferent de numărul de persoane afectate.

10.5. certSIGN garantează că certificatele digitale sunt emise în conformitate cu standardele în domeniu și cu Regulamentul 910/2014 conform listei prestatorilor calificați de servicii care se găsește la adresa <https://webgate.ec.europa.eu/tl-browser/#/>.

11.6. certSIGN nu garantează că certificatele emise sunt potrivite pentru orice fel de operațiune sau document sau validarea automată pe toate sistemele de operare sau aplicațiile client dacă acestea nu fac verificarea în conformitate cu lista de încredere arătată mai sus.

10.2. certSIGN is not liable for:

(a) damages caused by force majeure and/or act of God. The term "force majeure" refers to that unpredictable and un-removable event that occurred after the contract was concluded, such as: fire, earthquake, any other natural calamity, as well as war. The relatively unpredictable and relatively invincible circumstance, with no extraordinary character, such as: strikes, legal restrictions, Internet network malfunctioning, other such events, define the act of God;

(b) damages caused by the installation and use of applications and devices used for the generation and management of cryptographic keys, encryption, creation of electronic signatures, which do not meet the conditions specified in the CPS;

(c) damages caused by theft, loss or deterioration of the material media of digital certificates, storage of erroneous data in certSIGN database and their inclusion in the digital certificates issued for the Subject, in case the Subject declared that these data are correct.

(d) damage caused by improper use of the certificates issued. "Inappropriate" means situations such as: use of a revoked or expired certificate or use of a certificate that is inconsistent with the stated purpose of the certificate (i.e. use for a purpose other than in Legacy Systems), or in breach of the obligations incumbent on the Subject;

(e) submission by the Subject of false, inaccurate or incomplete data or false identity documents or statements. In the event that the Subject compromises the identity verification process, the Subject shall be solely liable for damages suffered by the Provider and third parties due to inaccurate and/or false information and documents submitted.

The situations referred to in (b),(c), (d) and (e) fall under the Subject's responsibility.

10.3. To the extent permitted by law, neither party may be ordered to pay damages for consequential damages, or benefit or profit, loss of business, clients or data.

10.4. In any case, certSIGN's liability will be limited to 200 euros for each certificate. The total liability of the Provider to cover the damages caused will be limited to EUR 10,000, regardless of the number of affected persons.

10.5. certSIGN guarantees that digital certificates are issued in accordance with the relevant standards in the field and Regulation 910/2014 according to the list of qualified service providers found at <https://webgate.ec.europa.eu/tl-browser/#/>.

10.6. certSIGN does not guarantee that the certificates issued are suitable for any kind of operation or document or automatic validation on all operating systems or client applications if they do not verify according to the trusted list shown above.

11. LEGEA APLICABILĂ. LITIGII

Prezentele Condiții Generale se supun legii române. Litigiile de orice fel decurgând din prezentele Condiții Generale se vor soluționa pe cale amiabilă sau, în caz de nereușită, vor fi supuse soluționării instanțelor judecătorești, de la sediul certSIGN, în conformitate cu legislația română în vigoare.

12. COMUNICĂRI

Orice comunicare între părți, referitoare la îndeplinirea prezentelor Condiții Generale, trebuie să fie transmisă în scris fie prin serviciile poștale și de curierat, fie prin e-mail la adresa office@certsign.ro, cu condiția confirmării în scris a primirii comunicării. Orice document scris trebuie înregistrat atât în momentul transmiterii, cât și în momentul primirii.

13. Modificarea Condițiilor Generale

13.1. certSIGN își rezervă dreptul de a modifica prezentele Condiții Generale atunci când modificarea este cerută de legislația sau standardele aplicabile serviciilor de încredere sau ca urmare a îmbunătățirii serviciilor, ori la cererea autorităților competente. Modificarea prezentelor Condiții Generale va fi publicată pe site-ul www.certsign.ro și va fi aplicabilă de la data publicării.

Prezentul document s-a întocmit bilingv, română-engleză. În caz de neconcordanță între cele două variante, varianta în limba română va prevala.

Prezentele condiții se consideră acceptate prin semnarea lor sau prin confirmarea luării la cunoștință de conținutul acestora.

**PRESTATOR/PROVIDER
CERTSIGN S.A.**

11. GOVERNING LAW. LITIGATION

These General Conditions are governed by the Romanian law. Disputes of any kind arising out of these General Conditions shall be settled amicably or, in case of failure, shall be submitted to the courts of law, at certSIGN headquarters, in accordance with the Romanian law in force.

12. COMMUNICATIONS

Any communication between the parties regarding the performance of this contract must be sent in writing either by post or courier, or by e-mail to office@certsign.ro, confirming in writing the communication receipt. Any written document must be recorded both at the time of transmission and at the time of receipt.

13. Modification of General Conditions

certSIGN reserves the right to amend these General Terms and Conditions when the amendment is required by legislation or standards applicable to trust services or as a result of service improvements, or at the request of competent authorities. The modification of these General Conditions will be published on the website www.certsign.ro and will be applicable from the date of publication.

This document has been prepared bilingually, Romanian English. In case of inconsistency between the two versions, the Romanian version shall prevail.

These conditions shall be deemed accepted by signing them or by confirming the acknowledgement of their content.

SUBIECT/SUBJECT