

„**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 legătură cu certificatele digitale emise de către Autoritatea de Certificare certSIGN Public 2023 RSA CA” sau certSIGN Qualified 2023 RSA CA”.

„**Subiectul**” este persoana fizică sau juridică, 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.certsign.ro/ro/document/certsign-qualified-2023-rsa-ca-cod-practici-si-proceduri/>

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

2. Obiectul

2.1. Stabilește termenii și condițiile privind furnizarea și utilizarea Serviciilor de încredere pentru emiterea de certificate digitale, calificate sau necalificate, după caz, în scop de testare.

2.2. În funcție de opțiunea Beneficiarului, certificatul digital emis în scop de testare poate fi pentru semnătură electronică sau pentru sigiliu electronic.

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.

3.3 Certificatul digital de test are o perioadă de valabilitate de maxim 30 de zile.

4. Obligațiile Subiectului/Beneficiarului

Subiectul/Beneficiarul are următoarele obligații:

- a. Să furnizeze către certSIGN date corecte la înregistrarea cererii de certificat;
- b. Pentru certificatele digitale stocate pe dispozitiv criptografic:
 - Să folosească dispozitivul calificat de creare a semnăturii electronice (QSCD) și aplicațiile software recomandate de certSIGN în cazul în care își generează singur cheile;

"**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 qualified digital certificates issued by certSIGN Certification Authority "certSIGN Public Qualified 2023 RSA CA" or 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.certsign.ro/en/document/certsign-qualified-2023-rsa-ca-certification-practice-statement/>

The "**Certification Practice Statement of the certSIGN Public 2023 RSA CA Certification Authority**" (CPS) represents the set of practices and procedures governing the provision and use of trust services for standard digital certificates. The CPS is public and can be found at:

<https://www.certsign.ro/en/document/certsign-public-2023-rsa-ca-certification-practice-statement/>.

2. Subject matter

2.1 It lays down the terms and conditions regarding the provision of trusted services for issuing digital certificates, qualified or standard, as applicable, for testing purposes.

2.2 Depending on the Subscriber's choice, the digital certificate issued for testing purposes may be for electronic signature or for electronic seal.

3. Duration

3.1 It shall enter into force upon acceptance/signing of these General Terms and Conditions by the Subject.

3.2 These General Terms and Conditions shall remain valid for the entire duration of the certificate.

3.3 The digital test certificate shall be valid for a maximum period of 30 days.

4. Obligations of the Subject/Subscriber

The Subjects/Subscriber undertakes:

- a. To send to certSIGN correct data upon registration of the certificate request;
- b. For digital certificates stored on a cryptographic device:
 - To use the qualified electronic signature creation device (QSCD) and software applications recommended by certSIGN if they generate their own keys;

Se aplică pentru/ Applies to:
Certificate de test pentru orice OID PKI2023 certSIGN / Test certificates for any certSIGN PKI2023 OID

- Să genereze perechile de chei numai folosind un Dispozitiv calificat de creare a semnăturii electronice (QSCD) agreat de certSIGN;
- Să schimbe codul PIN de acces la cheia privată de pe token înainte de prima utilizare;
- 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, certificatul nu mai poate fi folosit;
- c. Pentru certificatul digital pentru semnare electronică sau aplicare sigiliu electronic la distanță, să furnizeze certSIGN numărul de telefon al dispozitivului mobil care se va afla doar în posesia și sub controlul Subiectului pe perioada de valabilitate a certificatului; este responsabilitatea Subiectului dacă dispozitivul mobil va fi înstrăinat, pierdut sau altă persoană va avea acces la el.
- d. 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 și folosirea neautorizată a acesteia);
- e. Subiectul/ Beneficiarul înțelege și acceptă că certSIGN nu va emite certificate digitale pentru minori în scop de testare.
- f. Să folosească certificatul digital emis de Autoritatea de certificare certSIGN Public 2023 RSA CA sau certSIGN Qualified 2023 RSA CA cu OID-ul corespunzător certificatului pentru testare solicitat. OID-urile certificatelor digitale se găsesc la art. 7.1.6 din CPP.
- g. Pentru certificatele pentru semnare electronică sau aplicare sigiliu electronic la distanță, să dețină sau să folosească resurse hardware și software necesare utilizării Serviciilor, asumându-și în această privință orice responsabilitate pentru funcționalitatea lor și compatibilitatea acestora cu Serviciile de încredere, precum și pentru configurarea lor corectă.
- h. Prin semnarea/acceptarea prezentelor Condiții Generale înțelege că certificatul digital este emis în scop de testare și nu poate fi utilizat pentru semnarea de documente care să producă efecte juridice. certSIGN nu verifică datele furnizate de Subiect sau Beneficiar în scopul emiterii certificatelor digitale pentru testare.
- i. Să ceară, de îndată, certSIGN revocarea certificatului, atunci când a pierdut datele de creare a semnăturii electronice ori a sigiliului electronic sau când are motive să creadă că aceste date au ajuns la cunoștința unui terț neautorizat;
- j. Să respecte prevederile CPP certSIGN Public 2023 RSA CA, respectiv certSIGN Qualified 2023 RSA CA;
- k. Subiectul este responsabil cu privire la conținutul și natura documentelor pe care va aplica semnătura electronică sau sigiliul electronic;
- l. Prin acceptarea/semnarea prezentelor Condiții Generale, Subiectul/ Beneficiarul înțelege și este de acord ca certSIGN să utilizeze datele din certificat pentru a pune b. To generate key pairs only using a Qualified Electronic Signature Device (QSCD) approved by certSIGN;
- To change the token key access PIN code before the first use;
- The Subject understands and accepts that in the event of multiple incorrect PIN/PUK entries and token blocking or damage to the token due to the Subject's fault, the certificate can no longer be used;
- c. For the digital certificate for electronic signing or remote electronic seal application, provide certSIGN with the phone number of the mobile device that will be solely in the possession and under the control of the Subject during the certificate validity; it is the Subject's responsibility if the mobile device is lost, stolen, or another person gains access to it;
- d. To take the necessary measures to enable the proper generation (by the Subject, Registration Authority, or Certification Authority) and secure storage of the private key within a key pair (to prevent its loss, compromise, modification, and unauthorized use);
- e. The Subject/Subscriber understands and accepts that certSIGN will not issue digital certificates to minors for testing purposes.
- f. To use the qualified digital certificate issued by the Certification Authority certSIGN Public Qualified 2023 RSA CA or certSIGN Qualified 2023 RSA CA with the OID corresponding to the requested test certificate. The OIDs of digital certificates can be found in Article 7.1.6 of the CPS.
- g. For certificates for electronic signature or remote electronic seal application, to possess or use the hardware and software resources necessary for the use of the Services, undertaking in this regard any responsibility for their functionality and compatibility with the Trust Services, as well as for their correct configuration.
- h. By signing/accepting these General Terms and Conditions, understands that the digital certificate is issued for testing purposes and cannot be used to sign documents that have legal effect. certSIGN does not verify the data provided by the Subject or Subscriber for the purpose of issuing digital certificates for testing.
- i. To immediately request certSIGN to revoke the certificate when the data used to create the electronic signature or electronic seal has been lost or when there is reason to believe that this data has been disclosed to an unauthorized third party;
- j. To comply with the provisions of CPS certSIGN Public 2023 RSA CA, respectively certSIGN Qualified 2023 RSA CA;
- k. The Subject is responsible for the content and nature of the documents to which the electronic signature or seal will be applied;
- l. By accepting/signing these General Conditions, the Subject/Subscriber understands and agrees that certSIGN will use the data in the certificate to make the

la dispoziția publicului Registrul de certificate în formă electronică în vederea furnizării Serviciilor de Încredere;
m. Prin acceptarea/semnarea prezentelor Condiții Generale, Beneficiarul ia cunoștință că certSIGN va păstra o copie a actului de identitate al Beneficiarului 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. Orice nerespectare de către Subiect/Beneficiar 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 doar după identificarea Beneficiarului exclusiv pe baza actului de identitate, validarea cererii transmise de Beneficiar, în acord cu CPP.

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

i) identificării Beneficiarului de către un reprezentant certSIGN și

ii) primirii de către certSIGN a prezentelor Condiții Generale semnate de către Subiect,;

5.4. Să genereze certificatul digital pentru semnare electronică sau aplicare sigiliu electronic la distanță după înrolarea în aplicație a Subiectului și autorizarea de către Subiect a primei semnături.

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

5.6. certSIGN are obligația să revoce 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.

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

6. Acceptarea certificatelor

6.1. La primirea unui certificat, Subiectul se angajează să verifice conținutul acestuia. 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.

6.2. Certificatul stocat pe dispozitiv criptografic este considerat acceptat în cazul în care Subiectul îl acceptă fie

electronic Certificate Repository available to the public for the provision of Trust Services;

m. By accepting/signing these General Terms and Conditions, the Subscriber acknowledges that certSIGN will keep a copy of the Subscriber's identity document for the purpose of processing the information necessary exclusively for the provision of Trust Services. certSIGN retains the data and logs related to the life cycle of the certificates issued for 10 years after the expiration of the certificate.

n. Any breach by the Subject/Subscriber of their 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 shall issue the qualified digital certificate only after having identified the Subscriber solely based on the identity document and after having validated the application submitted by the Subscriber, as per 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 Subscriber identification by a certSIGN representative;

ii) Of receipt by certSIGN of these General Conditions signed by the Subject;

5.4. To issue the digital certificate for electronic signing or remote electronic seal application after the Subject has enrolled in the application and authorized the first signature.

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

5.6. 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 the Certificate Repository.

5.7. 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.

6. Certificate acceptance

6.1 Upon receipt of a certificate, the Subject undertakes to verify its contents. 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.

6.2 The certificate stored on a cryptographic device is considered accepted if the Subject accepts it either

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).

6.3. Certificatul pentru semnare electronică sau sigiliu electronic la distanță este considerat acceptat de către Subiect în momentul utilizării acestuia în aplicația sau platforma de semnare.

6.4. Acceptarea certificatului este o decizie unilaterală a Subiectului, anterior utilizării lui în efectuarea oricărei operații criptografice.

Pentru fiecare terț 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.

7. Revocarea certificatului. Efecte

7.1. Revocarea certificatului poate fi făcută în condițiile prevăzute în CPP la cererea Subiectului, Beneficiarului, a certSIGN sau a unei autorități competente, în cazuri precum : finalizarea perioadei de testare înainte de încetarea valabilității certificatului digital, utilizarea certificatului în alt scop decât cel de testare, și în altele prevăzute la art. 4.9.1 din CPP.

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

7.3. 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.

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

explicitly, at the time of its collection from the certSIGN website, or by default, after 3 calendar days from the receipt of the certificate kit (sent by certSIGN);

6.3 The certificate for electronic signing or remote electronic seal is considered accepted by the Subject when used in the signing application or platform.

6.4 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 terms of use and limitations are detailed in #1.4 and #4.5.2 of the CPS.

7 Certificate revocation. Effects

7.1. The certificate may be revoked under the conditions set forth in the CPS at the request of the Subject, the Subscriber, certSIGN, or a competent authority, in cases such as: completion of the testing period before the expiration of the digital certificate, use of the certificate for purposes other than testing, and others provided for in Article 4.9.1 of the CPS.

7.2 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.

7.3 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 Subject's written consent for such disclosure has been obtained;
- certSIGN was legally bound to disclose the information.

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

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, Bucuresti, sector 5.

8.8. 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/>.

9. Garanții

certSIGN nu oferă niciun fel de garanții cu privire la certificatele digitale emise pentru testare.

Subiectul înțelege și acceptă că certificatele digitale emise pentru testare nu beneficiază de garanții comerciale sau de conformitate.

10. Încetarea aplicabilității

10.1. 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 imediat, la data revocării sau încetării valabilității certificatului

11. Răspundere și excluderi

11.1. 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 neînlăturat 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

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 their 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. 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. Guarantees

certSIGN does not offer any guarantees regarding digital certificates issued for testing purposes.

The subject understands and accepts that digital certificates issued for testing purposes do not benefit from commercial or compliance guarantees.

10. Cessation of Applicability

10.1 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 take effect right away, at the date of revocation or certificate expiry.

11. Liability and Exceptions

11.1. certSIGN is not liable for:

(a) damages caused by force majeure and/or a fortuitous event. 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 fortuitous event;

(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

suporturilor materiale ale certificatelor digitale, 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, ori cu încălcarea obligațiilor ce revin Subiectului), stocarea de date eronate în bazele de date ale CERTSIGN și includerea acestora în certificatul digital emis Subiectului, în cazul în care Subiectul a declarat că aceste date sunt corecte.

(d) prezentarea de către Beneficiar de acte de identitate false sau declarații false. Beneficiarul va fi unicul responsabil pentru daunele suferite de Prestator și de terți din cauza inexactității și/sau falsului informațiilor și documentelor de identitate prezentate.

(e) orice act ilegal realizat prin folosirea codurilor de utilizare a serviciului;

(f) funcționalitatea rețelei de Internet pe care o utilizează Subiectul și conținutul informațiilor care sunt transmise prin aceasta;

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

11.2. Subiectul înțelege și acceptă că certificatul digital poate fi folosit doar în scop de testare și nu poate fi utilizat pentru semnarea de documente care produc efecte juridice și se obligă să aducă la cunoștința oricărei persoane căreia îi comunică un document semnat cu certificatul de testare că semnăturile/sigiliile create cu certificatul pentru testare nu produc efecte juridice, Subiectul fiind singurul responsabil pentru daunele produse certSIGN sau oricărei alte persoane de neîndeplinirea acestor obligații.

11.3. 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.

11.4. În orice caz răspunderea totală a certSIGN va fi limitată la 50 euro pentru certificat.

11.5. 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.

12. 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.

material media of digital certificates, by improper use of the issued certificates the inappropriate use of the issued certificates (“inappropriate” refers to situations like: the use of a revoked or expired certificate or inconsistent with the declared purpose of the certificate, or in breach of the obligations incumbent on the Subject), 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) presentation by the Subscriber of false identity documents or false statements. The Subscriber shall be solely liable for damages suffered by the Provider and third parties due to the inaccuracy and/or falsity of the information and identity documents presented.

(e) any illegal act performed using the service usage codes;

(f) the functionality of the Internet network used by the Subject and the content of the information transmitted through it

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

11.2. The subject understands and accepts that the digital certificate can only be used for testing purposes and cannot be used to sign documents that have legal effect and undertakes to inform any person to whom they communicate a document signed with the test certificate that signatures/seals created with the test certificate have no legal effect, the subject being solely responsible for any damages caused to certSIGN or any other person for failure to fulfil these obligations.

11.3 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.

11.4. In any case, certSIGN liability will be limited to EUR 50 for each certificate.

11.5. Digital certificates are issued in accordance with industry standards and Regulation 910/2014, as per the list of qualified service providers available at <https://webgate.ec.europa.eu/tl-browser/#/>.

11.6. certSIGN does not guarantee that the certificates issued are suited 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.

12. GOVERNING LAW. LITIGATION

These General Conditions are governed by the Romanian laws. 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.

13. 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.

14. Modificarea Condițiilor Generale

14.1. 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.

13. 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.

14. Changes to the General Conditions

14.1 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 terms and conditions are considered accepted upon signing or confirming acknowledgment of their content.

SUBIECT/SUBJECT