GUVERNUL REPUBLICII MOLDOVA

Nr. 31-76-3340 Chişinău 30 martie 2022

Biroul Permanent
al Parlamentului

În temeiul art.73 din Constituția Republicii Moldova, se prezintă spre examinare proiectul de lege privind identificarea electronică și serviciile de încredere, aprobat prin Hotărârea Guvernului nr.203 din 30 martie 2022.

Responsabil de prezentarea în Parlament a proiectului de lege este Serviciul de Informații și Securitate.

Anexe:

1. Hotărârea Guvernului privind aprobarea proiectului de lege (în limba română – 1 filă şi în limba rusă – 1 filă);
2. Proiectul de lege (în limba română – 33 file şi în limba rusă – 37 file);
3. Nota informativă la proiectul de lege (7 file);
4. Analiza impactului de Reglementare a proiectului de lege – 13 file;
5. Expertiza Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător (8 file);
6. Avize şi recomandări (50 file);
7. Raportul de expertiză de compatibilitate al Centrului de Armonizare a Legislației (18 file);
8. Raportul de expertiză al Centrului Naţional Anticorupţie (28 file);
9. Raportul de expertiză al Ministerului Justiţiei (7 file);
10. Sinteza obiecțiilor şi propunerilor (100 file);
11. Procesele-verbale interinstituționale (10 file);
1. Tabelul de concordanță (61 file).

Secretargeneral adjunct al Guvernului **Roman Cazan**

SECRETARIATUL PARLAMENTULUI
REPUBLICII MOLDOVA
D.D.P. Nr. 107
"31" 03 2022
Ora

Ex.:Dumitru Celonenco
Tel.:022 250 427
e-mail:dumitru.celonenco@gov.md

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. 203

din 30 martie 2022

Chișinău

Pentru aprobarea proiectului de lege privind identificarea electronică și serviciile de încredere

---

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind identificarea electronică și serviciile de încredere.

Prim-ministru **NATALIA GAVRILIȚA**

Contrasemnează:

Ministrul justiției Sergiu Litvinenco

Proiect
UE

PARLAMENTUL REPUBLICII MOLDOVA

LEGE
privind identificarea electronică şi serviciile de încredere

Parlamentul adoptă prezenta lege organică.

Prezenta Lege transpune parțial Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, publicat în Jurnalul Oficial al Uniunii Europene L 257 din 28 august 2014.

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Scopul legii şi domeniul de aplicare

(1) Prezenta lege are drept scop asigurarea funcţionării la un nivel adecvat a pieţei naţionale în domeniul de securitate a mijloacelor de identificare electronică şi a serviciilor de încredere şi stabileşte cadrul juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuţie electronică înregistrate şi serviciile de certificare pentru autentificarea unei pagini web.

(2) Prezenta lege nu limitează modul de utilizare a documentelor.

Articolul 2. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni semnifică:

autentificare – proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii şi integrităţii unor date în format electronic;

arhiva electronică securizată – depozit structurat de documente electronice, care asigură confidenţialitatea, nonrepudierea şi integritatea acestora şi care garantează valoarea probantă în timp a documentelor electronice;

certificat al cheii publice – document electronic ce conţine cheia publică asupra căruia a fost aplicată semnătura electronică sau sigiliul electronic al prestatorului de servicii de încredere, atestă apartenenţa cheii respective titularului certificatului cheii publice şi permite identificarea acestui titular;

certificat calificat al cheii publice – certificat al cheii publice care întruneşte cerinţele prevăzute la art. 13 şi este eliberat de un prestator de servicii de încredere ce întruneşte cerinţele prevăzute la art. 8;

certificat pentru semnătură electronică – atestare electronică care face legătură între datele de validare a semnăturii electronice şi o persoană fizică şi care confirmă cel puțin numele persoanei respective;

certificat pentru sigiliu electronic – atestare electronică care face legătură între datele de validare a sigiliului electronic şi o persoană juridică şi care confirmă numele persoanei respective;

certificat calificat pentru semnătură electronică – înseamnă un certificat pentru semnătură electronică care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute la art. 25;

certificat calificat pentru sigiliu electronic – înseamnă un certificat pentru sigiliu electronic care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute la art. 25;

creatorul unui sigiliu – persoană juridică care creează un sigiliu electronic;

certificat pentru autentificarea unei pagini web – atestare care face posibilă autentificarea unei pagini web şi face legătura între pagina web şi persoana fizică sau juridică căreia i s-a emis certificatul;

certificat calificat pentru autentificarea unei pagini web – certificat pentru autentificarea unei pagini web care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute la art. 34;

cheie publică – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic, care corespunde cheii private interdependente şi este destinată a fi utilizată pentru verificarea autenticităţii semnăturii electronice;

cheie privată – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic şi destinată a fi utilizată pentru crearea semnăturii electronice sau a sigiliului electronic;

date de identificare personală – set de date care permit stabilirea identității unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;

date de creare a semnăturilor electronice sau sigiliilor electronice – date unice care sunt utilizate de semnatar sau de creatorul sigiliului pentru a crea o semnătură electronică sau un sigiliu electronic;

date de validare – date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;

date de verificare a semnăturii electronice sau sigiliilor electronice – date care sunt utilizate în scopul verificării unei semnături sau unui sigiliu electronic;

dispozitiv de creare a semnăturii electronice sau a sigiliului electronic – software sau hardware configurat, utilizate pentru a crea o semnătură sau un sigiliu electronic;

dispozitiv de creare a semnăturilor electronice sau sigiliilor electronice calificate – dispozitiv de creare a semnăturii electronice sau a sigiliului electronic care îndeplinește cerințele prevăzute în art. 27;

dispozitiv de verificare a semnăturii electronice sau a sigiliului electronic – software sau hardware configurat, utilizate pentru punerea în aplicare a datelor de verificare a semnăturii electronice sau a sigiliului electronic;

document electronic – orice conținut în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală, asupra căruia este aplicată o semnătură electronică sau un sigiliu electronic;

identificare electronică – procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;

intermediar în circulația electronică a documentelor – întreprinzător individual sau persoană juridică care, din însărcinarea semnatarului sau creatorului sigiliului și/sau a destinatarului documentului electronic, organizează și administrează sistemul de circulație electronică a documentelor și/sau prestează servicii legate de circulația electronică a documentelor;

mijloace de identificare electronică – unitate materială sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării în cadrul unui serviciu online;

marcă temporală electronică – date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment;

marcă temporală electronică calificată – reprezintă o marcă temporală electronică care îndeplinește cerințele prevăzute la art. 31;

prestator de servicii de încredere – întreprinzător individual sau persoană juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;

prestator de servicii de încredere calificat – prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statut de calificat de către organul de supraveghere și control;

produs – hardware și/sau software ori componente specifice ale acestora, destinate să fie utilizate pentru prestarea serviciilor de încredere;

semnătură electronică – date în formă electronică, care sunt atașate la sau logic asociate cu alte date în formă electronică și care sunt utilizate ca metodă de autentificare;

semnătură electronică avansată – semnătură electronică ce îndeplinește cerințele stabilite la art. 23;

semnătură electronică calificată – semnătură electronică avansată care este creată prin intermediul unui dispozitiv de creare a semnăturilor electronice calificate și care se bazează pe un certificat calificat pentru semnături electronice;

semnatar – persoana fizică care creează o semnătură electronică;

serviciu de încredere – serviciu electronic, prestat de obicei în schimbul unei remunerații, care constă în una sau mai multe din următoarele activități:

a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective;

b) crearea, verificarea și validarea certificatelor pentru autentificarea unei pagini web;

c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;

serviciu de încredere calificat – reprezintă un serviciu de încredere care îndeplinește cerințele aplicabile, prevăzute de prezenta lege;

sigiliu electronic – date în format electronic atașate la sau asociate logic cu alte date în format electronic pentru asigurarea originii și integrității acestora din urmă;

sigiliu electronic avansat – sigiliu electronic care îndeplinește cerințele prevăzute la art. 23;

sigiliu electronic calificat – sigiliu electronic avansat care este creat prin intermediul dispozitivului de creare a sigiliilor electronice calificate și care se bazează pe un certificat calificat a sigiliilor electronice;

serviciu de distribuție electronică înregistrată – reprezintă un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind transmiterea și recepționarea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;

serviciu de distribuție electronică înregistrată calificat – înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 33;

titularul certificatului cheii publice – persoana fizică sau juridică sau persoana fizică care reprezintă persoana juridică, care utilizează serviciile de încredere;

organul de supraveghere și control – autoritate publică centrală stabilită de prezenta lege cu atribuții de supraveghere și control în domeniul identificării electronice și serviciilor de încredere;

validare – procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.

Articolul 3. Recunoașterea reciprocă

(1) Recunoașterea certificatelor cheilor publice în afara Republicii Moldova este reglementată de tratatele internaţionale la care Republica Moldova este parte. În cazul în care tratatele internaţionale la care Republica Moldova este parte stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaţionale.

(2) Certificatul cheii publice eliberat de către un prestator de servicii de încredere cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent, din punctul de vedere al efectelor juridice, cu certificatul cheii publice eliberat de un prestator de servicii de încredere cu domiciliul sau cu sediul în Republica Moldova dacă este întrunită una dintre următoarele condiţii:

a) prestatorul de servicii de încredere cu domiciliul sau cu sediul în alt stat a fost acreditat în cadrul regimului de acreditare în conformitate cu prevederile prezentei legi;

b) un prestator de servicii de încredere calificat cu domiciliul sau cu sediul în Republica Moldova garantează recunoaşterea certificatului;

c) certificatul sau prestatorul de servicii de încredere care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova şi alte state sau organizaţii internaţionale, pe bază de reciprocitate.

(3) Serviciile de încredere şi documentul electronic nu pot fi considerate lipsite de putere juridică doar în baza faptului că certificatul cheii publice a fost eliberat în corespundere cu normele unui stat străin, dacă acesta a fost recunoscut în condițiile specificate la alin. (2).

(4) Prin derogare de la prevederile alineatelor (1) și (2), un certificat calificat al cheii publice eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene, este recunoscut ca fiind echivalent, din punctul de vedere al efectelor juridice, cu certificatul cheii publice eliberat de un prestator de servicii de încredere cu domiciliul sau cu sediul în Republica Moldova.

(5) Modul de recunoaștere a un certificat calificat al cheii publice eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene, este stabilit de Guvern.

(6) Dispozitivul de verificare a semnăturii electronice sau a sigiliului electronic, utilizat pentru verificarea semnăturii electronice sau a sigiliului electronic în sensul art. 3 alin (4), trebuie să dispună de confirmarea corespunderii cu cerinţele prevăzute de prezenta lege, eliberată de către organul competent.

Capitolul II
IDENTIFICAREA ELECTRONICĂ ȘI SERVICII DE ÎNCREDERE

Secțiunea 1
Generalități privind identificarea electronică și servicii de încredere

Articolul 4. Accesibilitatea pentru persoanele cu dizabilități

Dacă este posibil, serviciile de încredere prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu dizabilități.

Articolul 5. Identificarea persoanelor în cadrul sistemelor informaționale

(1) Identificarea persoanelor în cadrul sistemelor informaționale nu poate fi limitată de date de identitate sau alte date de identificare a acestuia.

(2) În cazul în care se solicită identificarea utilizând serviciile de încredere calificate, se vor utiliza serviciile de încredere calificate, prevăzute în prezenta lege.

Articolul 6. Prestatorul de servicii de încredere

(1) Prestatorii de servicii de încredere pot fi calificați sau necalificați.

(2) Prestatorii de servicii de încredere sunt organizați în mod ierarhic. În vârful ierarhiei se află prestatorul de servicii de încredere de nivel superior.

(3) Prestatorii de servicii de încredere necalificați își organizează ierarhia de sine stătător.

(4) Activitatea prestatorilor de servicii de încredere calificați, inclusiv ierarhia acestora, se organizează în modul stabilit de Guvern, în conformitate cu prevederile prezentei legi.

(5) Evidenţa prestatorilor de servicii de încredere calificați se ţine de către organul de supraveghere și control în cadrul Registrului de evidenţă a prestatorilor de servicii de încredere calificați, care se actualizează permanent şi la care accesul este public.

(6) Introducerea în Registrul de evidenţă a prestatorilor de servicii de încredere calificați se efectuează de către organul de supraveghere și control la data acreditării acestora.

Articolul 7. Cererea de acreditare

(1) În vederea acreditării, prestatorul de servicii de încredere prezintă următoarele acte:

a) cererea de acreditare, conform modelului aprobat de către organul de supraveghere și control;

b) garanția bancară sau polița de asigurare în sumă de 300 000 lei;

c) regulamentul de funcționare a prestatorului de servicii de încredere;

d) copia ordinului de numire a angajaţilor în cadrul prestatorului de servicii de încredere şi a persoanelor împuternicite să semneze certificatele cheilor publice, precum şi copia actelor de identitate ale acestora;

e) copia documentelor care certifică studiile şi calificările persoanelor cu funcţii de răspundere implicate în prestarea serviciilor de certificare;

f) planul schematic al încăperilor şi ordinea de acces în încăperile cu regim special;

g) actul ce reglementează modul de păstrare a copiilor de rezervă ale registrului certificatelor cheilor publice;

h) ordinea de sincronizare cu Timpul Mondial Coordonat (UTC).

Articolul 8. Acreditarea prestatorului de servicii de încredere

(1) Prestatorul de servicii de încredere obține statutul de calificat în urma procedurii de acreditare.

(2) Prestatorii de servicii de încredere calificați se supun acreditării în conformitate cu prevederile prezentei legi.

(3) Acreditarea prestatorului de servicii de încredere se efectuează de către organul de supraveghere și control în baza cererii depuse. Acreditarea prestatorului de servicii de încredere este gratuită şi se acordă pentru un termen de 5 ani, dacă în cererea de acreditare nu este indicat un termen mai mic.

(4) Organul de supraveghere și control, în baza documentelor prezentate, în termen de 30 de zile, adoptă decizia privind acreditarea prestatorului de servicii de încredere sau privind refuzul de acreditare.

(5) Prestatorul de servicii de încredere se consideră calificat din ziua emiterii certificatului de acreditare.

(6) Procedura și cerințele detaliate privind modul de solicitare, acordare, suspendare şi retragere a certificatului de acreditare a prestatorului de servicii de încredere calificat se stabileşte de Guvern.

(7) Modul de solicitare, acordare, suspendare şi retragere a certificatului de acreditare a prestatorului de servicii de încredere calificat se stabileşte de Legea nr. 160/2011 privind reglementarea prin autorizare a activităţii de întreprinzător, în partea în care nu este reglementat de prezenta lege.

(8) Informaţia despre prestatorii de servicii de încredere calificaţi acreditaţi, precum şi despre cei cu acreditarea retrasă se publică de către organul de supraveghere și control pe pagina sa web oficială.

(9) Prestatorii de servicii de încredere calificați sunt obligați, pe parcursul întregului termen de acreditare, să asigure respectarea cerinţelor în conformitate cu care a fost acreditat. În cazul apariţiei circumstanţelor care fac imposibilă asigurarea respectării acestor cerinţe, prestatorul de servicii de încredere calificat urmează să notifice organul de supraveghere și control despre acest fapt în decurs de 24 de ore.

(10) Prestatorii de servicii de încredere necalificați sunt obligaţi să comunice organului de supraveghere şi control, cel târziu în termen de 10 zile, orice modificare a procedurilor de securitate şi de certificare, cu precizarea datei şi orei la care modificarea a intrat sau va intra în vigoare.

(11) Prestatorul de servicii de încredere calificat de nivel superior nu este supus acreditării în conformitate cu prevederile prezentei legi.

Articolul 9. Activitatea prestatorului de servicii de încredere

(1) Prestatorul de servicii de încredere:

a) creează şi eliberează certificatele cheilor publice;

b) suspendă şi revocă certificatele cheilor publice, restabileşte valabilitatea certificatelor cheilor publice suspendate;

c) ţine registrul certificatelor cheilor publice, asigură actualizarea acestuia şi accesul public la registru;

d) prestează, în bază de contract servicii de încredere.

(2) Activitatea prestatorului de servicii de încredere reprezintă o activitate în domeniul protecţiei criptografice şi tehnice a informaţiei şi este supusă licenţierii în conformitate cu legislaţia în domeniul reglementării prin licenţiere a activităţii de întreprinzător.

Articolul 10. Obligaţiile prestatorului de servicii de încredere

(1) Prestatorul de servicii de încredere este obligat:

a) să verifice autenticitatea datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză;

b) să asigure corespunderea informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;

c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai târziu de data şi ora la care începe să curgă termenul de valabilitate a certificatului;

d) să asigure accesul la registrul certificatelor cheilor publice, cu respectarea prevederilor art. 52;

e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege şi să facă menţiunea respectivă în registrul certificatelor cheilor publice în termenele stabilite;

f) să acopere prejudiciile aduse oricărei entităţi sau persoane fizice, care se încrede în mod rezonabil în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de încredere, prin faptul că a omis să înregistreze revocarea certificatului;

g) să înştiinţeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de încredere şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;

h) să prezinte informaţiile necesare pentru autentificarea serviciilor de încredere.

(2) Prestatorul de servicii de încredere calificat este obligat, suplimentar celor stipulate la alin. (1):

1) să certifice, în modul stabilit de legislaţie, cheia sa publică destinată certificării cheilor publice;

2) să informeze organul de supraveghere și control cu privire la orice schimbare survenită în prestarea de servicii de încredere calificate și cu privire la intenția de a își înceta activitatea respectivă;

3) să utilizeze sisteme sigure pentru stocarea datelor care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât:

a) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul subiectului la care se referă datele;

b) numai persoanele autorizate să poată introduce și/sau modifica datele

stocate;

c) autenticitatea datelor să poată fi controlată;

4) să verifice, prin mijloace corespunzătoare și în conformitate cu legislația, identitatea și, după caz, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat. Informațiile menționate sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe:

a) de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau

b) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice;

c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat;

d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent, din perspectiva fiabilității, cu prezența fizică. Metodele alternative de identificare de la distanță a persoanei sunt stabilite de către Guvern.

5) să ia măsuri adecvate împotriva falsificării și furtului de date;

6) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art. 13, toate informaţiile pertinente referitoare la un certificat calificat al cheii publice, în special pentru a putea furniza dovezi privind certificarea în justiţie. Înregistrările pot fi efectuate prin mijloace electronice;

7) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul serviciului său de încredere, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele şi condiţiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării acestui certificat, la existenţa unui sistem de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Informaţiile transmise pe cale electronică, trebuie comunicate în scris, într-un limbaj accesibil. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat;

8) să solicite eliberarea duplicatului certificatului de acreditare în cazul pierderii sau deteriorării acestuia;

9) să înregistreze și mențină accesibile pentru o perioadă de 15 ani, inclusiv ulterior încetării activității, toate informațiile relevante referitoare la datele emise și primite, în special în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic.

Articolul 11. Cererea de certificare a cheii publice

(1) Cererea de certificare a cheii publice se depune în formă electronică semnată cu semnătură electronică sau sigiliu electronic şi/sau în formă de document pe suport de hârtie, semnat cu semnătura olografă a solicitantului.

(2) Cererea de certificare a cheii publice va conţine:

a) datele de identificare a solicitantului;

b) alte date ale solicitantului, în funcţie de scopul pentru care se eliberează certificatul cheii publice, precum şi informaţiile necesare pentru comunicarea cu acesta.

Articolul 12. Examinarea cererii de certificare a cheii publice

(1) Cererea de certificare a cheii publice este examinată de către prestatorul de servicii de încredere în termen de 5 zile lucrătoare de la data înregistrării cererii, dacă părţile nu stabilesc altfel.

(2) În baza deciziei de certificare a cheii publice, prestatorul de servicii de încredere creează şi eliberează certificatul cheii publice.

(3) Decizia privind refuzul de certificare a cheii publice se adoptă de către prestatorul de servicii de încredere în cazul:

a) depunerii cererii de certificare a cheii publice cu încălcarea prevederilor art. 11;

b) încălcării drepturilor unor terţi în procesul de întocmire sau de depunere a cererii de certificare;

c) prezentării în cererea de certificare a unor informaţii ce nu corespund realităţii.

(4) Decizia privind refuzul de certificare a cheii publice poate fi contestată în instanţa de judecată în modul stabilit.

(5) Decizia privind refuzul de certificare a cheii publice nu-l privează pe solicitant de dreptul de a depune o nouă cerere după înlăturarea tuturor încălcărilor admise.

Articolul 13. Certificatul cheii publice

(1) La crearea certificatului cheii publice, prestatorul de servicii de încredere este obligat să verifice unicitatea cheii publice.

(2) Certificatul cheii publice trebuie să conţină:

a) numărul unic de înregistrare a certificatului cheii publice;

b) datele de identificare ale prestatorului de servicii de încredere care a eliberat certificatul cheii publice;

c) datele de identificare şi alte date ale titularului certificatului cheii publice, în funcţie de scopul pentru care se eliberează certificatul, precum şi informaţiile necesare pentru comunicarea cu acesta;

d) cheia publică;

e) data şi ora la care începe să curgă termenul de valabilitate a certificatului cheii publice şi data şi ora la care acest termen încetează;

f) date despre algoritmul criptografic utilizat;

g) restricţiile privind utilizarea certificatului cheii publice şi/sau limitele valorii operaţiunilor în care acesta poate fi utilizat, dacă acestea se aplică;

h) alte informaţii prevăzute de legislaţie.

(3) Certificatul calificat al cheii publice se emite de către prestatorul de servicii de încredere calificat şi trebuie să conţină, suplimentar:

a) menţiunea care să indice că certificatul este eliberat ca certificat calificat al cheii publice;

b) datele de verificare a semnăturii electronice sau a sigiliului electronic care corespund datelor de creare a semnăturii electronice sau a sigiliului electronic, controlate de titularul certificatului cheii publice, în cazul în care certificatul este eliberat pentru semnături electronice sau sigilii electronice.

(4) În cazul serviciilor de încredere necalificate, structura certificatului cheii publice se stabileşte de către prestatorul de servicii de încredere, în conformitate cu prevederile prezentei legi. În cazul serviciilor de încredere calificate, structura certificatului cheii publice se stabileşte de către organul de supraveghere şi control, în conformitate cu prevederile prezentei legi.

(5) Certificatului cheii publice i se aplică semnătura electronică sau sigiliul electronic al prestatorului de servicii de încredere corespunzătoare tipului certificatului solicitat.

(6) În cazurile stabilite de legislaţie sau prin acordul părţilor, prestatorul de servicii de încredere creează certificatul cheii publice şi în formă de document pe suport de hârtie, în două exemplare. Certificatul cheii publice în formă de document pe suport de hârtie este semnat cu semnăturile olografe ale titularului certificatului cheii publice şi ale persoanei împuternicite a prestatorului de servicii de încredere. Un exemplar al certificatului cheii publice se transmite titularului, iar celălalt se păstrează la prestatorul de servicii de încredere.

(7) Prestatorul de servicii de încredere, de comun acord cu titularul certificatului cheii publice, poate indica în certificatul cheii publice cazurile în care certificatul respectiv va putea fi utilizat, precum şi unele restricţii cu privire la utilizarea acestuia.

(8) La cererea titularului certificatului cheii publice, prestatorul de servicii de încredere poate indica în certificatul cheii publice şi alte informaţii decât cele specificate la alin. (2) şi (3), cu condiţia că acestea nu contravin legislaţiei şi nu pun în pericol securitatea naţională sau ordinea publică, şi numai după o prealabilă verificare a exactităţii informaţiilor în cauză.

(9) Prestatorul de servicii de încredere introduce certificatul în registrul certificatelor cheilor publice nu mai târziu de data şi ora la care începe să curgă termenul de valabilitate a certificatului.

Articolul 14. Cheia privată şi cheia publică

(1) Cheia privată şi cheia publică utilizate la crearea serviciilor de încredere se creează de către persoana fizică sau juridică. Acestea pot fi create de

persoane terţe, prin acordul expres al persoanei respective, cu condiţia asigurării imposibilităţii de copiere a acestor chei.

(2) Cheia privată şi cheia publică interdependente se creează concomitent.

(3) Persoana fizică sau juridică poate fi titular al unui număr nelimitat de chei private şi chei publice.

(4) Cheia privată este utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea al altei persoane.

(5) Cheia publică este certificată de către prestatorul de servicii de încredere şi este accesibilă tuturor.

Articolul 15. Termenul de valabilitate şi termenul de păstrare a certificatului cheii publice

(1) Termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de încredere de nivel superior constituie 20 de ani, termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de încredere de nivelul II constituie 10 ani, termenul de valabilitate a certificatului cheii publice al utilizatorului se stabileşte de către prestatorul de servicii de încredere, dar nu poate constitui mai mult de 5 ani, în funcţie de capacităţile mijloacelor tehnice de creare a semnăturii electronice.

(2) Prestatorul de servicii de încredere este obligat să păstreze certificatul cheii publice cel puţin 15 ani de la data revocării sau expirării certificatului.

Articolul 16. Suspendarea şi revocarea certificatului cheii publice

(1) Prestatorul de servicii de încredere suspendă certificatul cheii publice la cererea titularului certificatului cheii publice.

(2) Prestatorul de servicii de încredere revocă certificatul cheii publice:

a) la cererea titularului certificatului cheii publice;

b) la cererea conducătorului persoanei juridice în care activează titularul certificatului cheii publice, în cazul certificatelor eliberate titularilor acestora pentru reprezentarea persoanei juridice;

c) la depistarea unor informaţii neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

d) la încălcarea confidenţialităţii cheii private (compromiterea cheii private);

e) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice şi în lipsa unei cereri din partea titularului certificatului cheii publice privind restabilirea valabilităţii acestuia;

f) la modificarea informației cuprinse în certificatul cheii publice;

g) în cazul decesului titularului certificatului cheii publice sau al instituirii unei măsuri de ocrotire judiciare (ocrotire provizorie, curatelă sau tutelă) în privinţa titularului;

h) la solicitarea organului de supraveghere și control, în cazul încălcării prezentei legi;

(3) În cazul în care prestatorul de servicii de încredere primeşte informaţii ce impun revocarea certificatului cheii publice, acesta este obligat, în termen de 3 ore de lucru, să facă menţiunile respective în registrul certificatelor cheilor publice.

(4) Prestatorul de servicii de încredere este obligat să înştiinţeze titularul certificatului cheii publice despre motivele revocării certificatului acestuia, cu excepția cazului în care procedura de revocare a fost inițiată de către titular.

Articolul 17. Obligaţiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

1) să asigure condiţiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;

2) să nu utilizeze cheia privată pentru serviciile de încredere dacă are motive să presupună că este încălcată confidenţialitatea cheii private;

3) să solicite imediat suspendarea valabilităţii certificatului cheii publice sau revocarea acestuia în cazul în care:

a) a pierdut cheia privată;

b) are motive să creadă că a fost încălcată confidenţialitatea cheii private;

c) informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

4) să înştiinţeze, în decurs de 24 de ore, prestatorul de servicii de încredere despre orice modificare a informaţiilor cuprinse în certificatul cheii publice;

5) să îndeplinească alte obligaţii prevăzute de prezenta lege şi de acordul încheiat cu prestatorul de servicii de încredere.

Articolul 18. Registrul certificatelor cheilor publice

(1) Prestatorul de servicii de încredere este obligat să ţină registrul certificatelor cheilor publice.

(2) Registrul certificatelor cheilor publice va conţine:

a) certificatele valabile ale cheilor publice;

b) certificatele revocate şi suspendate ale cheilor publice;

c) data şi ora eliberării certificatelor cheilor publice;

d) data şi ora revocării certificatelor cheilor publice;

e) alte informaţii în conformitate cu actele normative în domeniul serviciilor de încredere.

(3) În vederea verificării autenticităţii serviciilor de încredere, prestatorul de servicii de încredere este obligat să asigure accesul gratuit la registrul certificatelor cheilor publice, inclusiv în regimul timpului real.

Secțiunea a 2-a
Semnătura electronică și sigiliul electronic

Articolul 19. Principiile de utilizare a semnăturii electronice și sigiliului electronic

Principiile de utilizare a semnăturii electronice şi sigiliului electronic sunt:

a) libertatea alegerii şi utilizării oricărui tip de semnătură electronică sau sigiliului electronic, dacă actele normative sau acordul părţilor nu prevăd cerinţa de utilizare a unui tip concret de semnătură electronică sau sigiliu electronic, în corespundere cu obiectivele de utilizare a acesteia;

b) posibilitatea alegerii oricăror tehnologii şi/sau mijloace tehnice care permit utilizarea tipurilor concrete de semnături electronice sau sigiliului electronic în conformitate cu prevederile prezentei legi;

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice sau a sigiliului electronic şi/sau a documentului electronic pe care acestea sunt aplicate doar în baza faptului că semnătura electronică sau sigiliul electronic a fost creat prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic şi/sau al produsului.

Articolul 20. Tipuri de semnături electronice şi sigilii electronice

Tipurile de semnături electronice și sigilii electronice, ale căror principii şi mecanisme de utilizare sunt reglementate de prezenta lege, sunt:

a) avansată;

b) calificată.

Articolul 21. Regimul juridic de utilizare a semnăturii electronice și sigiliului electronic

(1) Semnătura electronică şi sigiliul electronic, indiferent de gradul de protecţie de care dispune, produce efecte juridice şi este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă:

a) se prezintă în formă electronică; sau

b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau

c) nu se bazează pe un certificat calificat al cheii publice; sau

d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic.

(2) Semnătura electronică calificată are aceeaşi valoare juridică ca şi semnătura olografă.

(3) Semnătura electronică calificată și sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă semnătura electronică sau sigiliul electronic calificat.

(4) Modalitatea în care se asigură gradul de protecţie a semnăturii electronice calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hârtie se stabileşte de organul de supraveghere şi control, conform atribuţiilor prevăzute la art. 35 alin. (2).

(5) Modalitatea de aplicare a semnăturilor electronice de către funcţionarii persoanelor juridice de drept public se stabileşte de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanţii acestora. Semnătura electronică şi sigiliul electronic nu constituie mijloace de criptare a informaţiei.

Articolul 22. Limitele utilizării unor tipuri de semnături sau sigilii electronice

(1) Nu se admite utilizarea semnăturii electronice avansate și sigiliului electronic avansat pentru:

a) aplicarea pe documente electronice ce conţin informaţie atribuită la secretul de stat;

b) aplicarea pe documentele electronice în raporturile juridice ale persoanelor juridice de drept public cu persoanele fizice şi cu persoanele juridice de drept privat.

(2) Prin derogare de la prevederile alin. (1) lit. a), se admite semnarea documentelor electronice ce conțin informații atribuite la secret de stat, cu semnătura electronică avansată, de către persoanele ale căror identitate și calitate constituie secret de stat, în condițiile Legii nr. 245/2008 cu privire la secretul de stat, din cadrul Serviciului de Informații și Securitate, Centrul Național Anticorupție și Ministerul Afacerilor Interne, la circulația electronică a documentelor din cadrul acestora.

Articolul 23. Cerințe pentru semnăturile electronice și sigiliile electronice avansate

Semnăturile electronice sau sigiliile electronice avansate îndeplinesc cumulativ următoarele cerinţe:

a) fac trimitere exclusiv la titular;

b) permit identificarea titularului;

c) sunt create utilizând date de creare a semnăturilor electronice, sau a sigiliilor electronice, pe care semnatarul, sau creatorul sigiliului, le poate utiliza cu un nivel ridicat de încredere, exclusiv sub controlul său;

d) sunt legate de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.

Articolul 24. Cerințe pentru semnăturile și sigiliile electronice calificate

Semnăturile electronice sau sigiliile electronice calificate îndeplinesc toate cerinţele semnăturilor electronice sau sigiliilor electronice avansate şi, suplimentar:

a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de încredere calificat;

b) se creează prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic şi se verifică cu ajutorul dispozitivului de

verificare a semnăturii electronice sau sigiliului electronic şi/sau al produsului, care dispun de confirmarea corespunderii cu cerinţele prevăzute de prezenta lege.

Articolul 25. Cerințe pentru certificatele calificate pentru semnături electronice sau pentru sigilii electronice

Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conțin:

a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice;

b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;

c) datele de identificare şi alte date ale semnatarului sau creatorului sigiliului electronic;

d) datele de validare a semnăturilor electronice sau sigiliilor electronice care corespund datelor de creare a acestora;

e) data şi ora la care începe să curgă termenul de valabilitate a certificatului şi data şi ora la care acest termen încetează;

f) numărul unic de înregistrare a certificatului;

g) date de verificare a certificatului calificat pentru semnătura electronică sau sigiliul electronic care corespund datelor de creare a acestora;

h) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent, sau;

i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice recunoscute conform art. 3, sau;

j) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere de nivel superior, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice ale prestatorilor de servicii de încredere acreditați.

Articolul 26. Crearea semnăturii electronice sau sigiliului electronic

(1) Crearea semnăturii electronice sau a sigiliului electronic se efectuează prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic şi/sau al produsului, cu utilizarea datelor de creare a semnăturii electronice sau a sigiliului electronic.

(2) Generarea sau gestionarea datelor de creare a semnăturilor electronice calificate sau sigiliilor electronice calificate, în numele semnatarului sau creatorului sigiliului, pot fi realizate numai de către un prestator de servicii de încredere calificat, cu acordul titularului certificatului cheii publice.

Articolul 27. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice

(1) Dispozitivele de creare a semnăturilor electronice sau sigiliilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice şi proceduri corespunzătoare, cel puţin că:

a) datele de creare a semnăturii sau a sigiliului electronic nu pot apărea decât o singură dată, iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege;

b) datele de creare a semnăturii electronice sau a sigiliului electronic nu pot fi deduse prin calcul şi semnătura electronică sau sigiliul electronic sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată;

c) datele de creare a semnăturii electronice sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane;

d) oferă posibilitatea afişării conţinutului documentului electronic pe care se aplică semnătura electronică sau sigiliul electronic sau face referinţa irevocabilă la documentul dat;

e) semnătura electronică sau sigiliul electronic este creat numai după confirmarea de către semnatar sau creatorul unui sigiliu a operaţiunii de creare a semnăturii electronice sau a sigiliului electronic;

f) confirmă în mod univoc crearea semnăturii sau a sigiliului electronic.

(2) Generarea sau gestionarea datelor de creare a semnăturilor electronice sau a sigiliului electronic în numele semnatarului sau creatorului sigiliului se pot realiza numai de către un prestator de servicii de încredere calificat.

(3) Dispozitivele de creare a semnăturii electronice sau a sigiliului electronic avansate sau calificate nu trebuie să modifice datele asupra cărora se aplică semnătura electronică sau sigiliul electronic avansat sau calificat, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.

Articolul 28. Verificarea autenticităţii semnăturii electronice sau sigiliului electronic

(1) Verificarea autenticităţii semnăturii electronice sau sigiliului electronic se efectuează prin intermediul dispozitivului de verificare a semnăturii electronice sau sigiliului electronic şi/sau al produsului, cu utilizarea datelor de verificare a semnăturii electronice sau sigiliului electronic.

(2) La verificarea semnăturii electronice avansate sau sigiliului electronic avansat şi semnăturii electronice calificate sau sigiliului electronic calificat, dispozitivul de verificare a semnăturii electronice sau sigiliului electronic şi/sau produsul trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic sau să facă referinţă irevocabilă la documentul dat;

b) să afişeze faptul modificării documentului electronic;

c) să facă referinţă la semnatar sau creatorul sigiliului electronic.

(3) La verificarea semnăturii electronice sau sigiliului electronic avansat şi a semnăturii electronice şi sigiliului electronic calificat trebuie să se garanteze, cu o siguranţă suficientă, că:

a) datele de verificare a semnăturii electronice sau sigiliului electronic corespund datelor afişate persoanei care verifică semnătura electronică sau sigiliul electronic;

b) semnătura electronică sau sigiliul electronic este verificat cu certitudine, iar rezultatul verificării şi identitatea semnatarului sau creatorului sigiliului sunt corect afişate;

c) autenticitatea şi valabilitatea certificatului cheii publice solicitat în momentul verificării semnăturii electronice sau sigiliului electronic sunt verificate cu certitudine;

d) conţinutul certificatului cheii publice este redat clar;

e) orice modificări care pot influenţa securitatea semnăturii electronice sau sigiliului electronic pot fi detectate.

Articolul 29. Cerințe pentru validarea semnăturii și sigiliului electronic calificate

Procesul de validare a unei semnături electronice sau sigiliu electronic calificat confirmă validitatea acestora cu următoarele condiții:

a) certificatul care stă la baza semnăturii electronice sau sigiliului electronic a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 25;

b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul aplicării semnăturii electronice sau sigiliului electronic;

c) datele de validare a semnăturilor electronice sau sigiliilor electronice corespund datelor furnizate de titularul certificatului cheii publice;

d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice;

e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim;

f) semnătura electronică sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate;

g) integritatea datelor asupra cărora a fost aplicată semnătura electronică sau sigiliul electronic nu a fost compromisă;

h) cerințele prevăzute la art. 23 au fost îndeplinite la momentul semnării.

Secțiunea a 3-a
Mărcile temporale electronice

Articolul 30. Efectul juridic al mărcilor temporale electronice

(1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată.

(2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate.

Articolul 31. Cerințe pentru mărcile temporale electronice

(1) Cerințele pentru mărcile temporale electronice avansate sunt stabilite de către prestatorii de servicii de încredere.

(2) O marcă temporală electronică calificată, se eliberează de către prestatorul de servicii de încredere calificat și îndeplinește următoarele cerințe:

i) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;

j) se bazează pe o sursă de timp precisă, legată de ora universală coordonată;

k) asupra acesteia este aplicată o semnătură electronică calificată sau un sigiliu electronic calificat al prestatorului de servicii de încredere calificat sau o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul mărcilor temporale recunoscute conform art. 3.

Secțiunea a 4-a
Serviciul de distribuție electronică înregistrată și autentificarea unei pagini web

Articolul 32. Efectul juridic al unui serviciu de distribuție electronică înregistrată

(1) Datelor transmise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca dovadă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru serviciul de distribuție electronică înregistrată calificat.

(2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată calificat beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de către destinatarul identificat și a preciziei datei și orei trimiterii și primirii datelor indicate de serviciul de distribuție electronică înregistrată.

Articolul 33. Cerințe pentru serviciile de distribuție electronică înregistrată calificate

Serviciile de distribuție electronică înregistrată calificate îndeplinesc următoarele cerințe:

a) sunt prestate de către unul sau mai mulți prestatori de servicii de încredere calificați;

b) asigură identificarea expeditorului;

c) asigură identificarea destinatarului înainte de furnizarea datelor;

d) trimiterea și primirea datelor este securizată printr-o semnătură electronică sau un sigiliu electronic al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea că datele să fie schimbate fără ca acest lucru să fie detectat;

e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului și destinatarului datelor;

f) data și ora trimiterii, primirii și ale oricărei modificări a datelor este indicată printr-o marcă temporală electronică calificată.

Articolul 34. Cerințe pentru certificatele calificate pentru autentificarea unei pagini web

Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină:

a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web;

b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;

c) datele de identificare și alte date ale titularului certificatului cheii publice, precum și informațiile necesare pentru comunicarea cu acesta;

d) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează;

e) numele domeniului (domeniilor) gestionate de titularul certificatului cheii publice căruia i s-a emis certificatul;

f) numărul unic de înregistrare a certificatului;

g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent sau semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru autentificarea unei pagini web recunoscute conform art. 3;

h) date de verificare a certificatului calificat pentru autentificarea unei pagini web care corespund datelor de creare a acestuia.

Capitolul III
SUPRAVEGHEREA ȘI CONTROLUL

Articolul 35. Organul de supraveghere și control

(1) Organ de supraveghere și control este Serviciul de Informații și Securitate al Republicii Moldova;

(2) Organul de supraveghere și control are următoarele atribuții:

a) este responsabil de elaborarea și promovarea politicii de stat și de exercitarea controlului în domeniul serviciilor de încredere;

b) efectuează acreditarea prestatorilor de servicii de încredere și retrage statutul respectiv;

c) exercită funcţia prestatorului de servicii de încredere calificat de nivel superior pentru prestatorii de servicii de încredere calificați;

d) asigură ţinerea, actualizarea şi accesul public la datele Registrului de evidenţă a prestatorilor de servicii de încredere;

e) menține și publică, în mod securizat, liste sigure, asupra cărora este aplicată semnătura electronică sau sigiliul electronic al organului de supraveghere și control, care includ informații referitoare la prestatorii de servicii de încredere calificați și informații referitoare la serviciile de încredere calificate prestate de aceștia, într-o formă pasibilă de prelucrare automată;

f) elaborează şi aprobă, prin acte normative, cerinţele în domeniul serviciilor de încredere;

g) monitorizează şi controlează respectarea cerinţelor la prestarea serviciilor de încredere;

h) participă la elaborarea și aprobarea reglementărilor tehnice și a standardelor în domeniul serviciilor de încredere;

i) acordă, la solicitare, asistenţă metodică şi practică la utilizarea serviciilor de încredere;

j) supraveghează prestatorii de servicii de încredere calificați privind calitatea și securitatea serviciilor de încredere calificate pe care le prestează precum și îndeplinirea cerințelor stabilite în prezenta lege;

k) suspendă sau retrage acreditarea prestatorului de servicii de încredere, în cazul în care acesta nu îndeplinește cerințele în domeniul serviciilor de încredere;

l) cooperează cu autoritatea naţională pentru protecţia datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, cu privire la rezultatele controalelor prestatorilor de servicii de încredere calificați, în cazul în care se presupune că normele de protecție a datelor cu caracter personal au fost încălcate;

m) solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezenta lege;

n) realizează colaborarea internaţională în domeniul serviciilor de încredere.

(3) Autoritatea sau instituţia publică responsabilă de prestarea serviciului de sursă unică de sincronizare cu Timpul Mondial Coordonat (UTC) este stabilită de Guvern.

Articolul 36. Controlul în domeniul serviciilor de încredere

(1) Controlul privind respectarea cerinţelor stabilite de prezenta lege la prestarea serviciilor de încredere şi la acordarea sau prelungirea acreditării este efectuat de către organul de supraveghere şi control.

(2) Controlul se efectuează de către comisia de control în domeniul serviciilor de încredere (în continuare – *Comisie*) în baza regulamentului aprobat de organul de supraveghere şi control.

(3) Comisia se creează în cadrul organului de supraveghere şi control în baza ordinului privind efectuarea controlului, emis de conducătorul acestui organ.

(4) Componenţa nominală a Comisiei se stabileşte pentru fiecare caz în parte.

(5) Comisia are dreptul:

a) să beneficieze de acces liber la materialele documentare, pe suport de hârtie şi în format electronic, necesare pentru desfăşurarea lucrărilor ce ţin de prestarea serviciilor de încredere, precum şi la sistemele de distribuţie de aplicaţii soft, la aplicaţiile soft şi mijloacele hardware instalate;

b) să obţină informaţii complete despre condiţiile şi modul de exploatare a mijloacelor hardware şi software;

c) să obţină de la persoanele responsabile şi de la personalul prestatorului de servicii de încredere informaţiile privind prestarea serviciilor de încredere ce ţin de obiectul controlului;

d) să beneficieze de acces, în decursul zilei lucrătoare (în perioada efectuării controlului), în încăperile prestatorului de servicii de încredere.

(6) Comisia nu are dreptul să efectueze controlul fără prezentarea ordinului privind efectuarea controlului şi fără prezentarea actelor de identitate ale membrilor Comisiei.

(7) La efectuarea controlului privind respectarea condiţiilor prevăzute de prezenta lege, Comisia va ţine cont de următoarele reguli:

a) legalitatea şi respectarea competenţei stabilite de lege;

b) neadmiterea aplicării sancţiunilor care nu sunt stabilite de lege;

c) tratarea dubiilor, apărute la aplicarea legislaţiei, în favoarea prestatorului de servicii de încredere;

d) efectuarea controlului pe cheltuiala statului;

e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului;

f) dreptul prestatorului de servicii de încredere de a contesta acţiunile organului de supraveghere şi control, inclusiv în instanţa judecătorească.

(8) Controalele planificate privind respectarea de către prestatorul de servicii de încredere calificaţi a obligaţiilor prevăzute de prezenta lege se efectuează de către organul de supraveghere şi control cel mult o dată în decursul

anului calendaristic, cu cooptarea, după caz, a reprezentanţilor instituţiilor cu funcţii de reglementare şi de control, conform competenţei.

(9) Planurile controalelor, elaborate de organul de supraveghere şi control şi aprobate în modul stabilit, se coordonează, în privinţa termenelor de efectuare, cu conducerea prestatorului de servicii de încredere, cu cel puţin 5 zile lucrătoare înainte de începerea acestor controale.

(10) Controalele inopinate se efectuează la decizia organului de supraveghere şi control, numai în temeiul:

a) depistării şi confirmării, de către organul supraveghere şi control, a faptelor de încălcare a prezentei legi; şi/sau

b) recepţionării cererilor şi reclamaţiilor argumentate adresate în formă scrisă organului supraveghere şi control referitoare la încălcările sau la îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către prestatorul de servicii de încredere.

(11) Prestatorul de servicii de încredere este informat despre efectuarea controlului inopinat în ziua demarării controlului.

(12) Controalele repetate se efectuează numai în scopul verificării executării prescripţiei privind lichidarea încălcărilor prezentei legi, indicate în actul de control precedent (planificat sau inopinat). Controlul repetat se consideră parte componentă a controlului precedent.

(13) Controlul se efectuează strict în termenele stabilite în ordinul privind efectuarea controlului.

(14) Termenul de efectuare a controlului planificat şi a controlului inopinat nu poate depăşi 10 zile lucrătoare, iar a celui repetat – 5 zile lucrătoare. În cazul controalelor inopinate, termenul de 10 zile poate fi prelungit cu încă 10 zile de către conducătorul organului supraveghere şi control în baza unei decizii motivate, adusă la cunoştinţa prestatorului de servicii de încredere supus controlului, care poate fi contestată de către prestatorul de servicii de încredere.

(15) La efectuarea controlului privind respectarea obligaţiilor prevăzute de prezenta lege, prestatorul de servicii de încredere prezintă informaţia şi documentele relevante scopului controlului şi nu împiedică efectuarea acestuia.

(16) În baza rezultatelor controlului se întocmeşte un act în 2 exemplare, unul dintre care se expediază/înmânează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de încredere, iar al doilea se păstrează la organul de supraveghere şi control. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de încredere, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexând documentele de rigoare.

(17) În cazul în care se depistează încălcări ale obligaţiilor prevăzute de prezenta lege, organul supraveghere şi control emite, în baza actului de control, prescripţia privind lichidarea acestor încălcări, ce cuprinde recomandările privind modul de remediere a tuturor încălcărilor depistate, precum şi avertizarea despre

posibila suspendare sau retragere a acreditării dacă acestea nu vor fi lichidate în termenul stabilit.

(18) Termenul pentru lichidarea încălcărilor depistate constituie 15 zile lucrătoare, calculat din ziua următoare celei în care a fost primită prescripţia expediată/înmânată împreună cu actul de control.

(19) Dacă în termenul stabilit prestatorul de servicii de încredere nu a lichidat toate încălcările depistate, la solicitarea oficială a acestuia, termenul pentru lichidarea încălcărilor este prelungit cu termenul solicitat de prestatorul de servicii de încredere, dar care nu poate depăşi 20 de zile lucrătoare.

(20) Prestatorul de servicii de încredere calificat care a primit prescripţia privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripţie, să comunice organului de supraveghere şi control informaţia privind lichidarea încălcărilor.

(21) Informaţiile despre rezultatele efectuării controlului se publică de către organul de supraveghere și control pe pagina sa web oficială.

(22) Prestatorul de servicii de încredere are dreptul să depună la organul de supraveghere şi control reclamaţii în scris privind încălcările prevederilor prezentei legi admise de Comisie sau să conteste acţiunile acesteia în instanţa judecătorească.

Articolul 37. Suspendarea şi reluarea valabilităţii acreditării

(1) Acreditarea este suspendată în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător.

(2) Drept temei pentru realizarea acţiunilor prevăzute de lege pentru suspendarea acreditării servesc:

a) cererea prestatorului de servicii de încredere calificat privind suspendarea acreditării;

b) încălcarea de către prestatorul de servicii de încredere a obligaţiilor stabilite de prezenta lege;

c) depistarea unor date neautentice în documentele prezentate organului de supraveghere şi control;

d) nevalabilitatea garanţiei bancare sau a poliţei de asigurare;

e) nerespectarea de către prestatorul de servicii de încredere a prescripţiei privind lichidarea încălcărilor prevăzute de prezenta lege, depistate în urma controlului efectuat de Comisie.

(3) Decizia privind suspendarea acreditării se aduce la cunoştinţă prestatorului de servicii de încredere calificat în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăşi 2 luni.

(4) Prestatorul de servicii de încredere calificat este obligat să înştiinţeze în scris organul de supraveghere şi control despre înlăturarea circumstanţelor care au dus la suspendarea acreditării.

(5) Decizia privind reluarea valabilităţii acreditării se adoptă de către organul de supraveghere şi control în temeiul hotărârii instanţei de judecată care a emis hotărârea de suspendare a acreditării sau a instanţei de judecată ierarhic superioare, în termen de 3 zile lucrătoare de la data primirii înştiinţării. Decizia se aduce la cunoştinţă prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data adoptării acesteia.

(6) Termenul de valabilitate a acreditării nu se prelungeşte pe perioada de suspendare a acesteia.

Articolul 38. Retragerea acreditării

(1) Acreditarea este retrasă în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător.

(2) Drept temei pentru realizarea acţiunilor prevăzute de lege în vederea retragerii acreditării servesc:

a) cererea prestatorului de servicii de încredere calificat privind încetarea activităţii, depusă cu 30 de zile înainte de încetarea planificată;

b) decizia cu privire la anularea înregistrării de stat a întreprinzătorului individual sau a persoanei juridice în cadrul căreia activează prestatorul de servicii de încredere;

c) constatarea faptului de transmitere a certificatului de acreditare sau a copiei de pe acesta altei persoane în scopul desfăşurării genului de activitate acreditat;

d) neînlăturarea, în termenul stabilit, a circumstanţelor care au dus la suspendarea acreditării;

e) nerespectarea repetată a prescripţiilor privind lichidarea încălcărilor obligaţiilor stabilite de prezenta lege.

(3) Menţiunea referitoare la data şi numărul deciziei privind retragerea acreditării se înscrie în Registrul de evidenţă a prestatorilor de servicii de încredere nu mai târziu de ziua lucrătoare imediat următoare zilei adoptării deciziei.

(4) Toate certificatele cheilor publice emise de către prestatorul de servicii de încredere calificat care şi-a încetat activitatea se revocă şi se transmit spre păstrare altui prestator de servicii de încredere calificat, în modul stabilit de organul de supraveghere şi control, pe cheltuiala prestatorului de servicii de încredere care îşi încetează activitatea.

(5) Prestatorul de servicii de încredere calificat este obligat, în decurs de 10 zile lucrătoare de la data adoptării deciziei de retragere a acreditării, să depună la organul de supraveghere şi control certificatul de acreditare retras.

Articolul 39. Cerinţe de securitate aplicabile prestatorilor de servicii de încredere

(1) Prestatorii de servicii de încredere calificaţi şi necalificaţi aplică măsurile tehnice şi organizaţionale corespunzătoare pentru gestionarea riscurilor

la adresa securității serviciilor de încredere pe care le prestează.

(2) Prestatorii de servicii de încredere calificați și necalificați notifică organului de supraveghere și control imediat, dar nu mai târziu de 24 de ore de la momentul constatării, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice în cauză încălcarea securității sau pierderea integrității fără întârzieri nejustificate.

(3) Organul de supraveghere şi control notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării securității sau pierderea integrității servește interesului public.

Capitolul IV
REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC ŞI CIRCULAŢIA ELECTRONICĂ A DOCUMENTELOR

Articolul 40. Regimul juridic de utilizare a documentului electronic

(1) Documentul electronic semnat cu semnătură electronică calificată este asimilat, după efectele sale, cu documentul analog pe suport de hârtie, semnat cu semnătură olografă.

(2) Documentul electronic semnat cu alt tip de semnătură electronică decât cea calificată, este asimilat, după efectele sale, cu documentul analog pe suport de hârtie, semnat cu semnătură olografă, doar în cazurile stabilite expres de actele normative sau de acordul părţilor privind aplicarea semnăturilor sau sigiliilor electronice, cu respectarea condiţiilor stipulate la art. 43 alin. (1).

(3) Actele normative sau acordul părţilor privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaştere a documentelor electronice, semnate cu alt tip de semnătură electronică decât cea calificată, asimilate, după efectele lor, cu documente analoage pe suport de hârtie, semnate cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum şi obligaţiile părţilor privind confidenţialitatea şi răspunderea materială.

(4) În cazul în care, conform legislaţiei, se cere ca documentul să fie perfectat sau prezentat pe suport de hârtie şi semnat cu semnătură olografă, documentul electronic se consideră a fi corespunzător acestei cerinţe.

(5) În cazul în care, conform legislaţiei, se cere ca documentul pe suport de hârtie să fie autentificat cu ştampilă, documentul electronic se consideră a fi corespunzător acestei cerinţe.

(6) Asupra mai multor documente legate între ele (set de documente electronice) poate fi aplicat o singură semnătură electronică sau sigiliu

electronic.

(7) Modul de utilizare a documentelor electronice în cadrul procedurilor judiciare este reglementat de legislaţia procesuală.

(8) Documentul electronic este echivalat, după valoarea sa probantă, cu probele scrise sau mijloacele materiale de probă şi nu poate fi respins în calitate de probă doar pentru motivul că are o formă electronică.

(9) În cazul în care legislaţia prevede înregistrarea de stat a documentului, documentul electronic se supune înregistrării.

(10) Toate exemplarele identice ale documentului electronic sunt considerate originale şi produc aceleaşi efecte juridice.

(11) În cazul în care o persoană creează un document electronic şi un document pe suport de hârtie semnat cu semnătură olografă, identice după conţinut, ambele se consideră documente de sine stătătoare şi originale.

(12) Copia documentului electronic se consideră reprezentarea (redarea) acestuia pe suport de hârtie, într-o formă perceptibilă. Copia documentului electronic se autentifică în modul prevăzut de legislaţie pentru autentificarea copiilor documentelor pe suport de hârtie şi conţine menţiunea despre faptul că este copie a documentului electronic.

Articolul 41. Domeniile şi scopul de utilizare a documentului electronic

(1) Documentul electronic poate fi utilizat de către persoanele fizice şi juridice în toate domeniile de activitate în care este posibilă utilizarea mijloacelor hardware şi software ce permit crearea, prelucrarea, expedierea, recepţionarea, păstrarea, modificarea şi/sau nimicirea informaţiei în formă electronică.

(2) Documentul electronic poate fi utilizat în scopul expedierii informaţiei, ţinerii corespondenţei, întocmirii actelor juridice, precum şi în calitate de document care reflectă fapte economice.

Articolul 42. Cerinţele faţă de documentul electronic

Documentul electronic trebuie să corespundă următoarelor cerinţe principale:

a) să fie creat, prelucrat, expediat, recepţionat, păstrat, modificat şi/sau nimicit cu ajutorul mijloacelor hardware şi/sau software;

b) să conţină, pentru confirmarea autenticităţii acestuia, una sau mai multe semnături sau sigilii electronice ce corespund condiţiilor şi cerinţelor stabilite de prezenta lege;

c) să fie creat şi utilizat prin metode şi într-o formă ce ar permite identificarea semnatarului sau creatorului sigiliului electronic;

d) să fie afişat într-o formă perceptibilă;

e) să permită utilizarea sa repetată.

Articolul 43. Autenticitatea documentului electronic

(1) Documentul electronic este considerat autentic dacă întruneşte

cumulativ următoarele condiţii:

a) semnătura electronică sau sigiliul electronic este aplicat de persoana abilitată, în modul stabilit, să semneze cu semnătură olografă documentul echivalent pe suport de hârtie;

b) pe document este aplicată semnătura electronică sau sigiliul electronic autentic a semnatarului sau creatorului sigiliului indicat în document.

(2) Verificarea autenticităţii documentului electronic se efectuează prin verificarea, cu ajutorul dispozitivelor de verificare a semnăturii electronic sau sigiliului electronic şi/sau al produsului, a autenticităţii acestei semnături sau sigilii.

Articolul 44. Organizarea circulaţiei electronice a documentelor

(1) Circulaţia electronică a documentelor este organizată conform prevederilor prezentei legi şi regulilor stabilite de către proprietarul sistemului de circulaţie electronică a documentelor, precum şi conform contractelor încheiate între subiecţii circulaţiei electronice a documentelor.

(2) Circulaţia electronică a documentelor poate include:

a) crearea şi prelucrarea documentului electronic cu aplicarea semnăturii electronice sau sigiliului electronic;

b) expedierea şi recepţionarea documentului electronic;

c) verificarea autenticităţii documentului electronic;

d) confirmarea recepţionării documentului electronic;

e) evidenţa documentelor electronice;

f) păstrarea, modificarea şi/sau nimicirea documentului electronic;

g) crearea exemplarelor suplimentare ale documentului electronic;

h) crearea şi autentificarea copiilor documentului electronic pe suport de hârtie;

i) aplicarea mărcii temporale.

(3) Modul de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentului electronic pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept public se stabileşte de Guvern, iar pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept privat – de către proprietarii acestora.

Articolul 45. Intermediarul în circulaţia electronică a documentelor

(1) La organizarea şi efectuarea circulaţiei electronice a documentelor pot participa intermediari în condiţiile prezentei legi şi în conformitate cu regulile stabilite de proprietarul sistemului de circulaţie electronică a documentelor.

(2) Intermediarul în circulaţia electronică a documentelor este obligat:

a) să dispună mijloace hardware şi/sau software ce asigură fiabilitatea şi securitatea sistemelor informaţionale utilizate;

b) să dispună de personal cu competenţă şi experienţă în domeniul tehnologiei informaţiei şi/sau al securităţii informaţionale;

c) să asigure condiţiile necesare pentru stabilirea exactă a timpului şi a sursei de expediere a documentului electronic, precum şi a timpului recepţionării şi a adresei electronice a destinatarului;

d) să asigure protecţia şi păstrarea documentelor electronice;

e) să păstreze documentele electronice conform contractului cu utilizatorii sistemului de circulaţie electronică a documentelor.

Articolul 46. Crearea documentului electronic

(1) Documentul electronic conţine informaţia ce constituie conţinutul documentului electronic şi semnătura electronică sau sigiliul electronic al semnatarului sau creatorului sigiliului electronic.

(2) Crearea documentului electronic se finalizează prin aplicarea semnăturii electronice sau sigiliului electronic de către semnatar sau creator al sigiliului electronic şi, după caz, prin aplicarea mărcii temporale.

Articolul 47. Expedierea şi recepţionarea documentului electronic

(1) Documentul electronic poate fi expediat şi recepţionat cu ajutorul sistemelor informaţionale şi de comunicaţii electronice şi/sau al purtătorilor materiali.

(2) Documentul electronic se expediază într-o formă ce permite păstrarea şi utilizarea lui de către destinatar.

(3) În cazul în care semnatarul sau creatorul sigiliului şi destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră expediat dacă:

a) este expediat de către semnatar sau creatorul sigiliului ori de către un intermediar în circulaţia electronică a documentelor, care acţionează în numele semnatarului sau creatorul sigiliului, sau prin sistemul informaţional utilizat de către semnatar sau creatorul sigiliului;

b) este adresat în mod corespunzător sau este direcţionat în sistemul informaţional indicat de destinatar;

c) este redat într-o formă ce permite prelucrarea lui în sistemul informaţional indicat de destinatar;

d) intră într-un sistem informaţional ce nu este controlat de către semnatar sau creatorul sigiliului sau de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului sau creatorul sigiliului.

(4) În cazul în care semnatarul şi destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră recepţionat de către destinatar dacă acesta:

a) intră în sistemul informaţional din care destinatarul poate să extragă documentele electronice;

b) intră în sistemul informaţional indicat de destinatar într-o formă accesibilă pentru utilizare în sistemul respectiv.

(5) Documentul electronic se consideră neexpediat în cazul în care destinatarul ştia sau trebuia să ştie că:

a) persoana indicată în document ca semnatar nu este semnatarul adevărat al acestuia;

b) semnatarul nu este iniţiatorul expedierii documentului electronic;

c) documentul electronic este recepţionat de către destinatar cu modificări sau fără semnătură electronică.

(6) Documentul electronic nu se consideră recepţionat dacă persoana care l-a recepţionat nu este destinatarul preconizat al acestuia.

Articolul 48. Momentul expedierii şi recepţionării documentului electronic

(1) Dacă semnatarul sau creatorul sigiliului şi destinatarul documentului electronic nu au convenit altfel, moment al expedierii documentului electronic se consideră momentul intrării acestuia în sistemul informaţional ce nu este controlat de către semnatar sau creatorul sigiliului sau de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului sau creatorului sigiliului.

(2) Dacă semnatarul sau creatorul sigiliului şi destinatarul documentului electronic nu au convenit altfel, moment al recepţionării documentului electronic se consideră momentul intrării acestuia în sistemul informaţional indicat de destinatar. În cazul în care destinatarul documentului electronic nu a indicat sistemul informaţional respectiv, documentul electronic se consideră recepţionat din momentul intrării acestuia în sistemul informaţional al destinatarului, iar în cazul în care destinatarul nu dispune de un asemenea sistem – din momentul extragerii de către destinatar a documentului electronic din sistemul informaţional prin care a fost transmis.

(3) Momentul expedierii documentului electronic în sistemele informaţionale poate fi confirmat, la necesitate, prin aplicarea mărcii temporale pe documentul electronic respectiv.

(4) Dacă semnatarul sau creatorul sigiliului şi destinatarul documentului electronic au convenit asupra confirmării recepţionării documentului electronic, moment al recepţionării acestuia se consideră momentul expedierii de către destinatar a confirmării privind recepţionarea, cu aplicarea mărcii temporale după caz.

Articolul 49. Evidenţa documentelor electronice

(1) Evidenţa documentelor electronice ale persoanelor fizice şi/sau juridice se efectuează în conformitate cu legislaţia cu privire la registre.

(2) Ţinerea registrelor electronice cuprinde procedurile tehnologice şi de program de completare şi administrare a acestora, precum şi mijloacele de păstrare a documentelor electronice.

Articolul 50. Păstrarea documentelor electronice

(1) Subiecţii circulaţiei electronice a documentelor sunt obligaţi să păstreze originalele documentelor electronice într-o formă ce permite verificarea autenticităţii acestora.

(2) Termenul de păstrare a documentelor electronice este identic cu termenul prevăzut de legislaţie pentru păstrarea documentelor echivalente pe suport de hârtie.

(3) Subiecţii circulaţiei electronice a documentelor pot asigura păstrarea acestora utilizând serviciile intermediarului în circulaţia electronică a documentelor, cu condiţia respectării prevederilor prezentei legi.

(4) Pentru păstrarea în arhivă a documentelor electronice se utilizează arhiva electronică. Guvernul stabileşte categoriile de documente electronice pentru a căror păstrare se utilizează arhiva electronică securizată.

Articolul 51. Protecţia documentului electronic

(1) Documentul electronic beneficiază de protecţie juridică egală cu cea a documentului analog pe suport de hârtie.

(2) Informaţia ce constituie conţinutul documentului electronic este utilizată şi protejată, conform legislaţiei, în funcţie de statutul şi gradul de protecţie a acesteia.

(3) Crearea, prelucrarea, expedierea, recepţionarea, păstrarea, modificarea şi/sau nimicirea documentului electronic trebuie să corespundă cerinţelor de securitate stabilite de Guvern pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept public. Cerinţele de securitate pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept privat sunt stabilite de către proprietarii acestora.

(4) În procesul de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentului electronic se impune păstrarea informaţiei ce permite stabilirea originii, apartenenţei şi destinaţiei documentului electronic, precum şi a datei creării, expedierii şi recepţionării acestuia.

Capitolul V
PROTECŢIA DATELOR CU CARACTER PERSONAL ŞI RĂSPUNDEREA

Articolul 52. Protecţia datelor cu caracter personal

(1) Prestatorii de servicii de încredere vor asigura respectarea legislaţiei în domeniul protecţiei datelor cu caracter personal în procesul de prestare a serviciilor de încredere.

(2) Datele cu caracter personal se colectează de către prestatorul de servicii de încredere numai în măsura în care acestea sunt necesare pentru eliberarea şi menţinerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimţământul expres al persoanei interesate.

Articolul 53. Răspunderea persoanelor fizice şi juridice care cad sub incidenţa prezentei legi

(1) Persoanele fizice şi juridice poartă răspundere, conform legislaţiei, pentru neîndeplinirea prevederilor prezentei legi.

(2) Intermediarul în circulaţia electronică a documentelor poartă răspundere, conform legislaţiei, pentru neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege, pentru calitatea necorespunzătoare a serviciilor prestate, precum şi pentru prejudiciul cauzat de aceste acţiuni şi/sau inacţiuni.

(3) Litigiile apărute în cadrul circulaţiei electronice a documentelor, precum şi cele legate de utilizarea documentelor electronice şi a serviciilor de încredere se soluţionează de către subiecţii circulaţiei electronice a documentelor în conformitate cu legislaţia şi contractele încheiate.

Articolul 54. Răspunderea şi sarcina probei

(1) Prestatorul de servicii de încredere poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligaţiilor prevăzute de prezenta lege, cu excepţia cazurilor în care prestatorul de servicii de încredere aduce probe pertinente că nu a putut împiedica cauzarea prejudiciului.

(2) Sarcina de a proba intenţia sau neglijenţa unui prestator de servicii de încredere necalificat revine persoanei fizice sau juridice care pretinde despăgubiri pentru prejudiciul cauzat.

(3) Intenţia sau neglijenţa prestatorului de servicii de încredere calificat se prezumă, până la proba contrară.

(4) Prestatorii de servicii de încredere nu poartă răspundere pentru prejudiciile rezultate din utilizarea serviciilor care depăşesc restricţiile stabilite, în cazul în care prestatorii informează clienţii în prealabil în mod corespunzător cu privire la restricţiile privind utilizarea serviciilor pe care aceştia le prestează.

Articolul 55. Răspunderea titularului certificatului cheii publice

Titularul certificatului cheii publice poartă răspundere civilă pentru prejudiciul cauzat de:

a) neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege;

b) utilizarea serviciilor de încredere, inclusiv în perioada de la solicitarea suspendării valabilităţii sau revocării certificatului cheii publice până la înscrierea, în termenul stabilit, a menţiunii respective în registrul certificatelor cheilor publice, cu excepţia cazurilor în care titularul certificatului va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.

Capitolul VI
DISPOZIŢII FINALE ŞI TRANZITORII

Articolul 56. Dispoziţii finale

(1) Prezenta lege intră în vigoare la expirarea a 6 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) La data intrării în vigoare a prezentei legi se abrogă Legea nr. 91/2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr.174-177, art. 397), cu modificările ulterioare.

(3) Guvernul, în termen de 6 luni de la data publicării prezentei legi:

a) va prezenta propuneri Parlamentului privind aducerea legislaţiei în vigoare în concordanţă cu prezenta lege;

b) va aduce actele sale normative în concordanţă cu prezenta lege;

c) va elabora şi va adopta actele normative necesare pentru implementarea prezentei legi.

Articolul 57. Dispoziţii tranzitorii

(1) Certificatele cheilor publice eliberate în baza Legii nr. 91/2014 privind semnătura electronică şi documentul electronic rămân valabile până la expirarea termenului de valabilitate a acestora.

(2) În termen de 12 luni de la data intrării în vigoare a prezentei legi, prestatorii de servicii de certificare a cheilor publice acreditaţi în baza Legii nr. 91/2014 privind semnătura electronică şi documentul electronic sunt obligaţi să treacă procedura de acreditare în conformitate cu prevederile prezentei legi.

(3) În cazul în care prestatorii de servicii de certificare a cheilor publice acreditaţi în baza Legii nr. 91/2014 privind semnătura electronică şi documentul electronic nu trec procedura de acreditare în conformitate cu prevederile prezentei legi în termenul stabilit la alin. (2), acestora li se retrage certificatul de acreditare.

Preşedintele Parlamentului

NOTĂ INFORMATIVĂ
la proiectul Legii privind identificarea electronică și serviciile de încredere

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

Proiectul Legii privind identificarea electronică și serviciile de încredere este elaborat de către Serviciul de Informații și Securitate al Republicii Moldova (în continuare - *Serviciul*), în calitate de organ competent responsabil de elaborarea și promovarea politicii de stat și de exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice.

2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite

Necesitatea elaborării proiectului rezultă din Planul național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioadă 2017-2019, aprobat prin Hotărîrea Guvernului nr. 1472 din 30.12.2016, conform căruia, Serviciul a fost desemnat în calitate de instituție responsabilă de realizarea art. 255 al Planului – *elaborarea proiectului de lege pentru transpunerea Regulamentului 910/2014 în legislația națională*.

Prin transpunerea Regulamentului UE nr. 910/2014, proiectul urmărește alinierea legislației naționale în domeniul semnăturii electronice la normele europene. Totodată, acesta va impulsiona dezvoltarea serviciilor electronice, precum și va reglementa noi servicii aferente semnăturii electronice, care la moment nu se regăsesc în legislația națională, cum ar fi: identificarea electronică, sigilii electronice, mărci temporale electronice, certificate de securitate pentru pagini web.

Stabilirea între Republica Moldova și Uniunea Europeană a unui mecanism unic de funcționare a serviciilor de certificare a cheilor publice va facilita dezvoltarea cooperării internaționale în domeniul comerțului electronic.

Nu în ultimul rând, obiectivul reglementărilor propuse este de a crește încrederea în tranzacțiile electronice prin furnizarea unei baze comune pentru realizarea de interacțiuni electronice sigure între cetățeni, întreprinderi și autorități publice, contribuind astfel la creșterea eficienței serviciilor online în sectorul public și privat, a activității economice și a comerțului electronic.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul Legii a fost elaborat în vederea realizării angajamentelor asumate de Republica Moldova în cadrul Acordului de Asociere cu Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, ratificat de Parlamentul Republicii Moldova prin Legea nr. 112 din 02.07.2014.

Proiectul urmărește realizarea armonizării legislației naționale cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014

privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.

Tabelul de concordanţă a fost elaborat şi completat conform propunerilor Centrului de armonizare a legislaţiei şi remis împreună cu proiectul actului normativ.

4. Principalele prevederi ale proiectului şi evidenţierea elementelor noi

La moment, domeniul vizat este reglementat parţial prin Legea nr. 91/2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial nr.174-177/397 din 04.07.2014).

Menţionăm că, legislaţia în vigoare reglementează doar domeniul semnăturii electronice, alte servicii de încredere, cum ar fi sigiliul electronic sau certificatele de securitate pentru pagini web, nefiind reglementate prin acte normative naţionale. Prin urmare, cadrul normativ actual nu permite utilizarea de către persoanele juridice a sigiliilor electronice sau utilizarea sigiliilor în cadrul aparatelor de casă şi control, fapt care creează incomodităţi în activitatea acestora.

Principalele elemente noi propuse de proiect sunt:

- definirea noţiunilor noi pentru legislaţia naţională: *serviciu de încredere, sigiliu electronic, serviciu de distribuţie electronică înregistrată, certificat pentru autentificarea unei pagini web, creator al sigiliului electronic;*
- Instituirea şi reglementarea serviciilor de încredere noi:

- *sigiliul electronic*, care permite aplicarea acestuia pe documente electronice de către persoanele juridice. La moment legislaţia în vigoare stabileşte doar posibilitatea utilizării semnăturii electronice la semnarea documentelor electronice, care sunt eliberate exclusiv persoanelor fizice, care acţionează fie în nume propriu, fie în numele persoanei juridice sau al entităţii pe care o reprezintă. Totodată, sigiliul electronic va putea fi eliberat pentru utilizare în cadrul sistemelor informaţionale automatizate.

- *identificarea electronică,* care reprezintă procesul de utilizare a datelor de identificare a persoanelor în format electronic, în scopul identificării persoanei în cadrul sistemelor informaţionale;

- *serviciul de distribuţie electronică înregistrată,* care reprezintă un serviciu ce permite transmiterea datelor între părţi terţe prin mijloace electronice şi furnizează dovezi referitoare la gestiunea datelor transmise, inclusiv dovezi privind transmiterea şi recepţionarea datelor. Totodată, serviciul este menit să protejeze datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;

- *serviciul de autentificare a paginilor web*, care permite autentificarea unei pagini web şi face legătura între pagina web şi persoana fizică sau juridică căreia i s-a emis certificatul.

- Stabilirea unui nou temei pentru revocarea certificatelor cheilor publice – *la cererea conducătorului persoanei juridice în care activează titularul certificatului*

cheii publice, în cazul certificatelor eliberate pentru exercitarea atribuţiilor funcţionale. Legislaţia în vigoare stabileşte temeiul de revocare menţionat doar pentru persoanele juridice de drept public (Hotărîrea Guvernului nr.1141 din 20.12.2017 pentru aprobarea Regulamentului privind modalitatea de aplicarea semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora (Monitorul Oficial nr.451-463/1269 din 29.12.2017), fapt care provoacă o delimitare nejustificată a condiţiilor de revocare a certificatelor cheilor publice emise pentru persoanele juridice de drept public şi cele de drept privat.

Totodată, menţionăm că, la finele anului 2018, Ministerul Finanţelor a expediat spre avizare Serviciului proiectul hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului Informaţional Automatizat „Monitorizarea Electronică a Vânzărilor", care descrie eliberarea cheilor publice pentru echipamentele de casă şi de control, adică a sigiliilor electronice. Prin urmare, proiectul de lege propus, instituind sigiliul electronic, stabileşte posibilitatea eliberării certificatelor cheilor publice pentru sisteme informaţionale şi va permite implementarea conceptului propus de Ministerul Finanţelor.

5. Fundamentarea economico-financiară

Punerea în aplicare a legii nu va determina cheltuieli bugetare suplimentare, iar implementarea tehnică a noilor servicii de încredere este posibilă în cadrul infrastructurii cheilor publice deja existente.

6. Modul de încorporare a actului în cadrul normativ în vigoare

La intrarea în vigoare a legii, se va abroga Legea nr. 91/2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial nr.174-177/397 din 04.07.2014), cu modificările ulterioare.

Totodată, proiectul prevede aducerea legislaţiei în vigoare în concordanţă cu noua lege, în termen de 18 luni de la data publicării acesteia. Printre acestea evidenţiem:

- Legea nr. 753/1999 privind Serviciul de Informaţii şi Securitate al Republicii Moldova (Monitorul Oficial nr. 156/764 din 31.12.1999);
- Hotărîrea Guvernului nr. 1140 din 20.12.2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.451-463/1268 din 29.12.2017);
- Hotărîrea Guvernului nr. 1141 din 20.12.2017 pentru aprobarea Regulamentului privind modalitatea de aplicarea semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora (Monitorul Oficial nr.451-463/1269 din 29.12.2017);

- Ordinul directorului Serviciului de Informații și Securitate nr. 69 din 15.07.2016 cu privire la aprobarea Normelor tehnice în domeniul semnăturii electronice avansate calificate (Monitorul Oficial nr.215-216/1201 din 19.07.2016);

- Ordinul directorului Serviciului de Informații și Securitate nr. 70 din 15.07.2016 cu privire la aprobarea unor acte normative în domeniul organizării funcționării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.215-216/1202 din 19.07.2016);

- Ordinul directorului Serviciului de Informații și Securitate nr. 25 din 17.03.2017 cu privire la aprobarea Regulamentului privind procedura de avizare a dispozitivelor de creare și/sau verificare a semnăturii electronice și a produselor asociate semnăturii electronice (Monitorul Oficial nr.322-328/1637 din 01.09.2017);

- Ordinul directorului Serviciului de Informații și Securitate nr. 29 din 16.04.2009 cu privire la aprobarea Regulamentului de soluționare a situațiilor litigioase în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.86-88/372 din 08.05.2009).

7. Avizarea și consultarea publică a proiectului

La 09.03.2020 proiectul a fost remis spre avizare Cancelariei de Stat, cu indicarea listei autorităților și instituțiilor a căror avizare este necesară. Cancelaria de Stat a restituit proiectul în temeiul pct. 11 subpct. 2^1 lit. c) din Metodologia de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărîrea Guvernului nr. 23/2019.

La 11.03.2020 proiectul și AIR a fost remis spre expertizare Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător. La 16.04.2020 Grupul de lucru a expediat Serviciului procesul-verbal al ședinței din 31.03.2020, în cadrul căruia AIR nu a fost susținut de către Grupul de lucru.

La 04.06.2020 proiectul și AIR, completat conform obiecțiilor expertului Grupului de lucru, a fost remis repetat spre expertizare Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător. La ședința Grupului de lucru din 16.06.2020, AIR a fost susținut cu condiția luării în considerare a obiecțiilor și recomandărilor expertului SEIR și membrilor Grupului de lucru.

La 26.06.2020 proiectul cu toate anexele a fost remis spre avizare Cancelariei de Stat, cu indicarea listei autorităților și instituțiilor a căror avizare este necesară.

Ministerul Finanțelor (nr. 29/1700 din 31.07.2020) a avizat pozitiv proiectul fără obiecții și propuneri. Ministerul justiției (nr. 04/5285 din 18.07.2020), Ministerul Economiei și Infrastructurii (nr. 08-4392 din 21.07.2020), Centrul Național Anticorupție (nr. 06/2-4749 din 10.08.2020), Agenția de Guvernare Electronică (nr.3007-73 din 07.08.2020), Serviciul Tehnologia Informației și Securitatea Cibernetică (nr. 1.4/1201/44-20 din 14.08.2020), Agenția Servicii Publice (nr.01/5006 din 14.08.2020) și Centrul de Armonizare a legislației (nr. 31/02-3-7450 din 14.08.2020) au avizat pozitiv proiectul, cu prezentarea obiecțiilor și propunerilor.

La 21.10.2020, prin scrisoarea cu nr. 7/3-3102, proiectul definitivat conform avizelor a fost expediat spre avizare repetată autorităților interesate.

Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (nr. 03-DRAS/1479 din 29.10.2020) a avizat pozitiv proiectul fără obiecții și propuneri. Centrul de Armonizare a Legislației (nr. 31/02-4-9771 din 28.10.2020), Ministerul Justiției (nr. 04/8250 din 30.10.2020), Ministerul Economiei și Infrastructurii (nr. 08-6749 din 03.112020), Serviciul Tehnologia Informației și Securitate Cibernetică (nr. 1.4/1693/44-20 din 05.11.2020), Agenția Servicii Publice (nr. 01/7704 din 06.11.2020), Ministerul Finanțelor (nr. 15/3-06/368 din 09.11.2020), Centrul Național Anticorupție (nr. 06/2-6976 din 05.11.2020) au avizat pozitiv proiectul, cu prezentarea obiecțiilor și propunerilor. Agenția de Guvernare Electronică (nr. 3007-105 din 30.10.2020) a comunicat despre susținerea și promovarea proiectului de lege în Guvern doar în condițiile în care acesta va fi revizuit esențial cu acceptarea obiecțiilor incluse în aviz.

La 04.12.2020, 26.02.2021 și 01.03.2021 au fost desfășurate ședințe comune interinstituționale pe marginea proiectului cu participarea reprezentanților autorului și Ministerului Economiei și Infrastructurii, Ministerului Finanțelor, I.P. „Agenția de Guvernare Electronică", I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică", I.P. „Agenția Servicii Publice" și Centrul de Armonizare a Legislației. În cadrul ședințelor au fost dezbătute obiecțiile neacceptate sau acceptate parțial asupra proiectului. În urma desfășurării ședințelor Ministerul Finanțelor, I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică", I.P. „Agenția Servicii Publice" și Centrul de Armonizare a Legislației au susținut proiectul și au comunicat despre lipsa obiecțiilor și propunerilor. Suplimentar, Ministerul Finanțelor a accentuat necesitatea acordării unui termen și resurse financiare și umane suficiente pentru ajustarea sistemelor informaționale guvernamentale la noile prevederi normative, în vederea încadrării în termenul de intrare în vigoare a legii. Totodată, asupra obiecțiilor I.P. „Agenția de Guvernare Electronică" și Ministerului Economiei și Infrastructurii nu s-a ajuns la un consens. Rezultatele ședinței, pozițiile părților și argumentarea acestora sunt reflectate în procese-verbale ale ședințelor și Sinteza obiecțiilor și propunerilor la proiect.

La 29.03.2021, prin scrisoarea cu nr. 7/3-1273, proiectul definitivat în urma ședințelor interinstituționale a fost expediat spre avizare repetată autorităților interesate.

Agenția de Guvernare Electronică (nr. 3007-20 din 01.04.2021), Serviciul Tehnologia Informației și Securitate Cibernetică (nr. 1.4/493/44-21 din 02.04.2021) și Agenția Servicii Publice (nr. 01/3462 din 07.04.2021) au avizat pozitiv proiectul fără obiecții și propuneri. Centrul de Armonizare a Legislației (nr. 31/02-69-2603 din 07.04.2021) a comunicat că proiectul național și-a atins finalitatea propusă, asigurând transpunerea parțială corespunzătoare a prevederilor Regulamentului

910/2014 şi a reiterat necesitatea aprobării şi înregistrării de stat a actelor de implementare a legii. Ministerul Economiei şi Infrastructurii (nr. 08-1604 din 05.04.2021) a prezentat unele propuneri care au fost expuse în Sinteza obiecţiilor şi propunerilor la proiect. Ministerul Justiţiei, Ministerul Finanţelor, Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, Centrul Naţional Anticorupţie nu a prezentat avize suplimentare.

La 23.11.2021, prin scrisoarea Cancelariei de Stat cu nr. 31-06-836-9103, proiectul a fost expediat spre avizare repetată.

Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei (nr. 02-DCAJ/1421 din 25.11.2021), Centrul de Armonizare a Legislaţiei (nr. 31/02-69-9456 din 26.11.2021), Ministerul Economiei (nr. 07-5052 din 29.11.2021), Agenţia Servicii Publice (nr. 01/9221 din 01.12.2021), Ministerul Finanţelor (nr. 29/3634 din 30.11.2021), Ministerul Infrastructurii şi Dezvoltării Regionale (nr. 09-5633 din 02.12.2021) şi Ministerul Justiţiei (nr. 04/592 din 19.01.2022) au avizat pozitiv proiectul fără obiecţii şi propuneri. Serviciul Tehnologia Informaţiei şi Securitate Cibernetică (nr. 1.4/1562/44-21 din 30.11.2021) şi Centrul Naţional Anticorupţie (nr. 06/2-8135 din 03.12.2021) au prezentat unele obiecţii şi propuneri care au fost expuse în Sinteza obiecţiilor şi propunerilor la proiect.

La 25.01.2022, prin intermediul convorbirii telefonice, a fost desfăşurată şedinţa comună interinstituţională pe marginea proiectului cu participarea reprezentanţilor autorului şi I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică". În urma desfăşurării şedinţei telefonice, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" a acceptat argumentele autorului asupra obiecţiei respinse şi a comunicat despre susţinerea proiectului. Rezultatele şedinţei, poziţiile părţilor şi argumentarea acestora sunt reflectate în procesul-verbal al şedinţei şi Sinteza obiecţiilor şi propunerilor la proiect.

La 18.02.2022, prin intermediul conferinţei video, a fost desfăşurată şedinţa comună interinstituţională pe marginea proiectului cu participarea reprezentanţilor autorului şi Centrului Naţional Anticorupţie. În cadrul şedinţei, autorul a argumentat formularea prezentată în proiectul legii, totodată în scopul depăşirii divergenţelor a fost propusă modificarea proiectului legii, care a fost acceptată de către CNA. Rezultatele şedinţei, poziţiile părţilor şi argumentarea acestora sunt reflectate în procesul-verbal al şedinţei şi Sinteza obiecţiilor şi propunerilor la proiect.

În vederea respectării prevederilor Legii nr. 239/2008 privind transparenţa în procesul decizional, proiectul legii a fost plasat pe pagina web oficială a Serviciului de Informaţii şi Securitate www.sis.md, compartimentul *Transparenţa*, subcompartimentul *Transparenţa decizională*.

8. Constatările expertizei anticorupţie

În urma desfăşurării şedinţei comune interinstituţională pe marginea proiectului cu participarea reprezentanţilor autorului şi Centrului Naţional Anticorupţie din 18.02.2022, autorul proiectului şi Centrului Naţional Anticorupţie au ajuns la numitori comun asupra obiecţiilor înaintate în Raportul de expertiză anticorupţie cu nr. ELO21/7587 din 03.12.2021 iar proiectul a fost modificat corespunzător.

Obiecţiile şi recomandările detaliate ale Centrului Naţional Anticorupţie au fost expuse în Sinteza obiecţiilor şi propunerilor (recomandărilor) la proiect şi procesul-verbal al şedinţei comune interinstituţionale din 18.02.2022.

9. Constatările expertizei de compatibilitate

În ceea ce priveşte versiunea actuală a proiectului naţional, constatăm că, urmare a procedurii de avizare/expertizare, acesta a suferit mai multe modificări de ordin tehnic şi redacţional care, însă, nu afectează gradul de compatibilitate cu Regulamentul (UE) nr.910/2014 constatat iniţial. Prin urmare, se comunică privind lipsa unor observaţii sau obiecţii suplimentare.

Obiecţiile şi propunerile ce ţin de formulările utilizate în proiect, precum şi opinia autorului proiectului sunt reflectate în Sinteza obiecţiilor şi propunerilor (recomandărilor) la proiect.

10. Constatările expertizei juridice

Ministerul Justiţiei a comunicat lipsa obiecţiilor şi propunerilor de ordin conceptual.

11. Constatările altor expertize

La 16.06.2020, Grupul de lucru al Comisiei de stat pentru reglementarea activităţii de întreprinzător a examinat analiza impactului de reglementare la proiect şi a decis în mod unanim că:

Analiza impactului de reglementare se susţine cu condiţia luării în considerare a obiecţiilor şi recomandărilor expertului Secretariatului Evaluării Impactului de Reglementare şi ale membrilor Grupului de lucru al Comisiei de stat pentru reglementarea activităţii de întreprinzător.

Alexandr ESAULENCO
Director

Digitally signed by Esaulenco Alexandr
Date: 2022.03.09 09:46:53 EET
Reason: MoldSign Signature
Location: Moldova