Republica Moldova

PARLAMENTUL

LEGE Nr. LP124/2022
din 19.05.2022

privind identificarea electronică și serviciile de încredere

Publicat : 10.06.2022 în MONITORUL OFICIAL Nr. 170-176 art. 317 Data intrării în vigoare

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 și domeniul de aplicare

(1) Prezenta lege are drept scop asigurarea funcționării la un nivel adecvat a pieței naționale în domeniul securității mijloacelor de identificare electronică și a serviciilor de încredere, precum și stabilește cadrul normativ de bază pentru utilizarea semnăturilor electronice, sigiliilor electronice, mărcilor temporale electronice, documentelor electronice, serviciilor de distribuție electronică înregistrate și serviciilor de certificare pentru autentificarea paginilor web.

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

Articolul 2. Noțiuni principale

În sensul prezentei legi, următoarele noțiuni semnifică:

autentificare – proces electronic care permite confirmarea identificării electronice a persoanelor fizice și/sau juridice sau a originii și integrității anumitor date în formă electronică;

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

certificatul cheii publice – document electronic care conține cheia publică, căruia i-a fost aplicată semnătura electronică sau sigiliul electronic al prestatorului serviciilor de încredere, care permite identificarea titularului certificatului cheii publice și care atestă apartenența cheii respective acestui titular;

certificat calificat al cheii publice – certificat al cheii publice care întrunește cerințele

prevăzute la art. 13 și care este eliberat de un prestator de servicii de încredere ce întrunește cerințele prevăzute la art. 8;

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

certificat pentru sigiliu electronic – atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă denumirea persoanei respective;

certificat calificat pentru semnătură electronică – certificat pentru semnătură electronică emis de un prestator de servicii de încredere calificat și care întrunește cerințele prevăzute la art. 25;

certificat calificat pentru sigiliu electronic – certificat pentru sigiliu electronic emis de un prestator de servicii de încredere calificat și care întrunește cerințele prevăzute la art. 25;

creatorul sigiliului electronic – persoană juridică care creează sigiliul electronic;

certificat pentru autentificarea paginii web – atestare electronică care face posibilă autentificarea unei pagini web și face legătura între pagina web respectivă și persoana fizică sau juridică căreia i-a fost emis certificatul;

certificat calificat pentru autentificarea paginii web – certificat pentru autentificarea unei pagini web emis de un prestator de servicii de încredere calificat și care întrunește cerințele prevăzute la art. 34;

cheie publică – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturilor electronice sau a sigiliilor electronice, care corespunde cheii private interdependente și este destinată utilizării pentru verificarea autenticității semnăturii electronice;

cheie privată – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturilor electronice sau a sigiliilor electronice, care este destinată utilizării pentru crearea semnăturilor electronice sau a sigiliilor electronice;

date de identificare personală – set de date care permite stabilirea identității unei persoane fizice sau a datelor de identificare ale unei persoane juridice ori a identității persoanei fizice care reprezintă o persoană juridică;

date de creare a semnăturilor electronice sau a sigiliilor electronice – date unice care sunt utilizate de semnatar sau de creatorul sigiliului electronic 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 a sigiliilor electronice – date care sunt utilizate în scopul verificării unei semnături electronice sau unui sigiliu electronic;

dispozitiv de creare a semnăturilor electronice sau a sigiliilor electronice – software sau hardware configurat, utilizate pentru crearea semnăturilor electronice sau a sigiliilor electronice;

dispozitiv de creare a semnăturilor electronice sau sigiliilor electronice calificate – dispozitiv de

creare a semnăturilor electronice sau a sigiliilor electronice care întrunește cerințele prevăzute la art. 27;

dispozitiv de verificare a semnăturilor electronice sau a sigiliilor electronice – software sau hardware configurat, utilizate pentru punerea în aplicare a datelor de verificare a semnăturilor electronice sau a sigiliilor electronice;

document electronic – conținut în formă electronică, în special sub formă de text ori de înregistrare sonoră, vizuală sau audiovizuală, căruia i-a fost aplicată semnătura electronică sau sigiliul electronic;

identificare electronică – proces de utilizare a datelor de identificare ale persoanelor în formă electronică, 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 numele semnatarului ori creatorului sigiliului electronic și/sau al 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 – elemente, materiale și/sau imateriale, care conțin date de identificare personală și care sunt utilizate în scopul autentificării în cadrul unui serviciu accesibil în regim online;

marcă temporală electronică – date în formă electronică care leagă alte date în formă electronică de un anumit moment, stabilind dovezi că datele din urmă au existat la momentul respectiv;

marcă temporală electronică calificată – marcă temporală electronică care întrunește 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 prestator de servicii de încredere necalificat;

prestator de servicii de încredere calificat – prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și care deține statut de prestator de servicii de încredere calificat, acordat de către organul de supraveghere și control;

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

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

semnătură electronică avansată – semnătură electronică care întrunește 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 – persoană fizică care creează o semnătură electronică;

serviciu de încredere – serviciu electronic, prestat, de regulă, 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 electronice sau a certificatelor aferente serviciilor respective;

serviciu de încredere calificat – serviciu de încredere care întrunește cerințele aplicabile, prevăzute de prezenta lege;

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

sigiliu electronic avansat – sigiliu electronic care întrunește 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 al sigiliilor electronice;

serviciu de distribuție electronică înregistrată – serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv referitoare la 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 – serviciu de distribuție electronică înregistrată care întrunește cerințele prevăzute la art. 33;

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

organ de supraveghere și control – autoritate administrativă centrală abilitată prin prezenta lege cu atribuții de supraveghere și control în domeniul identificării electronice și serviciilor de încredere;

validare – proces 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 peste hotarele Republicii Moldova este reglementată de tratatele internaționale la care Republica Moldova este parte. În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaționale.

(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 condiții:

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 recunoașterea certificatului respectiv;

c) certificatul cheii publice sau prestatorul de servicii de încredere care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova și alte state sau organizații internaționale, pe bază de reciprocitate.

(3) Serviciile de încredere și 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 altui stat, dacă acesta a fost recunoscut în condițiile indicate la alin. (2).

(4) Prin derogare de la prevederile alin. (1) și (2), certificatul 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 unui 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 semnăturilor electronice sau a sigiliilor electronice, utilizat pentru verificarea semnăturii electronice sau a sigiliului electronic în sensul alin. (4), trebuie să dispună de confirmarea corespunderii cu cerințele prevăzute de prezenta lege, eliberată de către organul de supraveghere și control.

Capitolul II

IDENTIFICAREA ELECTRONICĂ

ȘI SERVICIILE DE ÎNCREDERE

Secțiunea 1

Generalități privind identificarea electronică

și serviciile de încredere

Articolul 4. Accesibilitatea pentru persoanele

cu necesități speciale

După posibilitate, serviciile de încredere prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu necesități speciale.

Articolul 5. Identificarea persoanelor în cadrul

sistemelor informaționale

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

(2) În cazul în care se solicită identificarea utilizând serviciile de încredere calificate, se utilizează serviciile de încredere calificate prevăzute de 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 ierarhic. În vârful organizării ierarhice se situează prestatorul de servicii de încredere de nivel superior.

(3) Prestatorii de servicii de încredere necalificați își stabilesc individual organizarea ierarhică.

(4) Organizarea și desfășurarea activității prestatorilor de servicii de încredere calificați, inclusiv ierarhia acestora, sunt stabilite de Guvern, în conformitate cu prevederile prezentei legi.

(5) Evidența prestatorilor de servicii de încredere calificați se ține de către organul de supraveghere și control în cadrul Registrului de evidență a prestatorilor de servicii de încredere calificați, care se actualizează permanent și la care accesul este public.

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

Articolul 7. Cererea de acreditare

În scopul 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 de lei;

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

d) copia de pe ordinul de numire a angajaților în cadrul prestatorului de servicii de încredere și a persoanelor împuternicite să semneze certificatele cheilor publice, precum și copiile de pe actele de identitate ale acestora;

e) copiile de pe documentele care certifică studiile și calificările persoanelor cu funcții de răspundere implicate în prestarea serviciilor de certificare;

f) planul schematic al încăperilor și 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 universal coordonat (UTC).

Articolul 8. Acreditarea prestatorului serviciilor

de încredere

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

(2) Prestatorii de servicii de încredere calificați se supun procedurii de acreditare 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 și 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, ia decizia privind acreditarea prestatorului de servicii de încredere sau privind refuzul acreditării.

(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 și retragere a certificatului de acreditare a prestatorului de servicii de încredere calificat se stabilesc de Guvern.

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

(8) Informația despre prestatorii de servicii de încredere calificați, precum și despre cei cărora le-a fost retrasă acreditarea se publică de către organul de supraveghere și control pe pagina web oficială a acestuia.

(9) Prestatorii de servicii de încredere calificați sunt obligați, pe parcursul întregului termen de acreditare, să asigure respectarea cerințelor în conformitate cu care au fost acreditați. În cazul apariției circumstanțelor care fac imposibilă asigurarea respectării cerințelor respective, prestatorul de servicii de încredere calificat notifică organul de supraveghere și control despre aceasta în decurs de 24 de ore.

(10) Prestatorii de servicii de încredere necalificați sunt obligați să comunice organului de supraveghere și control, în termen de 10 zile, modificarea procedurilor de securitate și/sau de certificare, cu indicarea datei și 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 și eliberează certificatele cheilor publice;

b) suspendă valabilitatea și revocă certificatele cheilor publice, restabilește valabilitatea

certificatelor cheilor publice suspendate;

c) ține registrul certificatelor cheilor publice, asigură actualizarea acestuia și 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 protecției criptografice și tehnice a informației și este supusă licențierii în conformitate cu legislația în domeniul reglementării prin licențiere a activității de întreprinzător.

Articolul 10. Obligațiile 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 respective;

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

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

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 și să introducă mențiunea respectivă în registrul certificatelor cheilor publice în termenele stabilite;

f) să acopere prejudiciile aduse entităților sau persoanelor fizice, care se încred, în mod rezonabil, în datele conținute în certificatul cheii publice eliberat de către prestatorul de servicii de încredere, prin faptul că a omis să înregistreze revocarea certificatului;

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

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

(2) Suplimentar obligațiilor stipulate la alin. (1), prestatorul de servicii de încredere calificat este obligat:

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

2) să informeze organul de supraveghere și control cu privire la modificările survenite în prestarea serviciilor de încredere calificate și cu privire la intenția de a-și 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 persoanei 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; sau

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

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, în conformitate cu art. 13, toate informațiile pertinente referitoare la un certificat calificat al cheii publice, în special pentru a putea furniza dovezi privind certificarea în justiție. Înregistrările pot fi efectuate prin mijloace electronice;

7) înainte să stabilească o relație contractuală cu o persoană care solicită un certificat în sprijinul serviciului său de încredere, să informeze persoana respectivă, prin mijloace de comunicație fiabile, cu privire la termenele și condițiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării acestui certificat, la existența unui sistem de acreditare și la procedurile de contestare și soluționare a litigiilor. Informațiile transmise în formă electronică trebuie furnizate ca text, într-un limbaj accesibil. Elementele pertinente ale informațiilor trebuie puse, la cerere, și la dispoziția părților terțe care beneficiază de certificat al cheii publice;

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

9) să înregistreze și să mențină accesibile pentru o perioadă de 15 ani, inclusiv după încetarea activității, toate informațiile relevante referitoare la datele emise și primite, în special în scopul furnizării probelor în procedurile judiciare și în scopul asigurării continuității serviciului. Înregistrările respective pot fi efectuate în format 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 căreia i s-a aplicat sigiliul electronic, și/sau în formă de document pe suport de hârtie, semnat cu semnătura olografă a solicitantului.

(2) Cererea de certificare a cheii publice conține:

a) datele de identificare ale solicitantului;

b) alte date ale solicitantului, în funcție de scopul pentru care se eliberează certificatul cheii publice, precum și informațiile 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 părțile nu stabilesc altfel.

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

(3) Decizia privind refuzul certificării cheii publice este luată de prestatorul de servicii de încredere în cazul:

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

b) încălcării drepturilor unor terți în procesul de întocmire sau de depunere a cererii de certificare a cheii publice;

c) prezentării în cererea de certificare a cheii publice a unor informații care nu sunt veridice.

(4) Decizia privind refuzul certificării cheii publice poate fi contestată în instanța de judecată în modul stabilit.

(5) Decizia privind refuzul certificării 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 conțină:

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 și alte date ale titularului certificatului cheii publice, în funcție de scopul pentru care se eliberează certificatul, precum și informațiile necesare pentru comunicarea cu acesta;

d) cheia publică;

e) data și ora la care începe să curgă termenul de valabilitate a certificatului cheii publice și

data și ora la care acest termen încetează;

f) date despre algoritmul criptografic utilizat;

g) restricțiile privind utilizarea certificatului cheii publice și/sau limitele valorii operațiunilor în care acesta poate fi utilizat, dacă acestea se aplică;

h) alte informații prevăzute de legislație.

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

a) mențiunea despre faptul 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 stabilește de către prestatorul de servicii de încredere, în conformitate cu prevederile prezentei legi. În cazul serviciilor de încredere calificate, structura certificatului cheii publice se stabilește de către organul de supraveghere și 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 legislație sau prin acordul părților, prestatorul de servicii de încredere creează certificatul cheii publice și 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 și 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 poate fi utilizat, precum și restricțiile cu privire la utilizarea acestuia.

(8) La cererea titularului certificatului cheii publice, prestatorul de servicii de încredere poate indica în certificatul cheii publice și alte informații decât cele specificate la alin. (2) și (3), cu condiția că aceasta nu contravine legislației și nu pune în pericol securitatea națională sau ordinea publică, precum și numai după verificarea prealabilă a exactității informațiilor respective.

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

Articolul 14. Cheia privată și cheia publică

(1) Cheia privată și cheia publică utilizate la crearea serviciilor de încredere se creează de către persoana fizică sau juridică. Acestea pot fi create de persoane terțe, prin acordul expres al persoanei respective, cu condiția asigurării imposibilității de copiere a acestor chei.

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

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

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

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

Articolul 15. Termenul de valabilitate și termenul

de păstrare a certificatului cheii publice

(1) Termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de încredere de nivel superior este de 20 de ani, iar termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de încredere de nivelul II – 10 ani. Termenul de valabilitate a certificatului cheii publice al utilizatorului se stabilește de către prestatorul de servicii de încredere, dar nu poate fi mai mare de 5 ani, în funcție de capacitățile mijloacelor tehnice de creare a semnăturii electronice.

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

Articolul 16. Suspendarea valabilității și revocarea

certificatului cheii publice

(1) Prestatorul de servicii de încredere suspendă valabilitatea certificatului 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 informații neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

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

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

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

(3) În cazul în care prestatorul de servicii de încredere primește informații care impun revocarea certificatului cheii publice, acesta este obligat, în termen de 3 ore de lucru, să introducă mențiunile respective în registrul certificatelor cheilor publice.

(4) Prestatorul de servicii de încredere este obligat să înștiințeze 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. Obligațiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

1) să asigure condițiile necesare pentru excluderea accesului altei persoane la cheia sa privată;

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

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

a) a pierdut cheia privată;

b) are motive să presupună că a fost compromisă confidențialitatea cheii private;

c) informațiile cuprinse în certificatul cheii publice nu sunt veridice;

4) să înștiințeze, în decurs de 24 de ore, prestatorul de servicii de încredere despre modificarea informațiilor cuprinse în certificatul cheii publice;

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

Articolul 18. Registrul certificatelor cheilor publice

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

(2) Registrul certificatelor cheilor publice conține:

a) certificatele valabile ale cheilor publice;

b) certificatele revocate și suspendate ale cheilor publice;

c) data și ora eliberării certificatelor cheilor publice;

d) data și ora revocării certificatelor cheilor publice;

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

(3) În scopul verificării autenticității serviciilor de încredere, prestatorul de servicii de încredere este obligat să asigure accesul gratuit la registrul certificatelor cheilor publice, inclusiv în regim de timp real.

Secțiunea a 2-a

Semnătura electronică și sigiliul electronic

Articolul 19. Principiile utilizării semnăturii electronice

și a sigiliului electronic

Principiile utilizării semnăturii electronice și a sigiliului electronic sunt:

a) libertatea alegerii și utilizării oricărui tip de semnătură electronică sau de sigiliu electronic, dacă actele normative sau acordul părților nu prevăd utilizarea unui tip concret de semnătură electronică sau de sigiliu electronic, în corespundere cu obiectivele de utilizare a acestora;

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

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice ori a sigiliului electronic și/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 semnăturilor electronice sau a sigiliilor electronice și/sau al produsului.

Articolul 20. Tipuri de semnături electronice și de sigilii

electronice

Semnăturile electronice și sigiliile electronice, ale căror principii și mecanisme de utilizare se reglementează de prezenta lege, sunt:

a) de tip avansat;

b) de tip calificat.

Articolul 21. Regimul juridic de utilizare a semnăturii

electronice și a sigiliului electronic

(1) Semnătura electronică și sigiliul electronic, indiferent de gradul de protecție de care dispun, produc efecte juridice și sunt acceptate ca probe, 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 de servicii de încredere; sau

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

d) nu sunt create prin intermediul dispozitivului de creare a semnăturilor electronice sau a sigiliilor electronice.

(2) Semnătura electronică calificată are aceeași valoare juridică ca și semnătura olografă.

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

(4) Modalitatea în care se asigură gradul de protecție a semnăturii electronice calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hârtie se stabilește de organul de supraveghere și control, conform art. 35 alin. (2).

(5) Modalitatea de aplicare a semnăturilor electronice și a sigiliilor electronice de către angajații persoanelor juridice de drept public se stabilește de Guvern. Persoanele juridice de drept privat stabilesc individual modalitatea de aplicare a semnăturilor electronice și a sigiliilor electronice de către reprezentanții acestora.

(6) Semnătura electronică și sigiliul electronic nu constituie mijloace de criptare a informației.

Articolul 22. Limitele utilizării unor tipuri de semnături

sau de sigilii electronice

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

a) aplicarea pe documente electronice ce conțin informație atribuită la secret de stat;

b) aplicarea pe documentele electronice în raporturile juridice ale persoanelor juridice de drept public cu persoanele fizice și 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, al Centrului Național Anticorupție și al Ministerului Afacerilor Interne, la circulația electronică a documentelor din cadrul acestora.

Articolul 23. Cerințe pentru semnăturile electronice

avansate și sigiliile electronice avansate

Semnăturile electronice avansate și sigiliile electronice avansate întrunesc cumulativ următoarele cerințe:

a) fac trimitere exclusiv la titular;

b) permit identificarea titularului;

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

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 electronice

calificate și sigiliile electronice calificate

Semnăturile electronice calificate și sigiliile electronice calificate întrunesc toate cerințele semnăturilor electronice sau, respectiv, a sigiliilor electronice avansate, precum și, 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 semnăturilor electronice sau a sigiliilor electronice și se verifică cu ajutorul dispozitivului de verificare a semnăturilor electronice sau a sigiliilor electronice și/sau al produsului, care dispun de confirmarea corespunderii cu cerințele prevăzute de prezenta lege.

Articolul 25. Cerințe pentru certificatele calificate

pentru semnături electronice sau pentru

sigilii electronice

(1) Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conțin:

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

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

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

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

e) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și 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.

(2) Suplimentar cerințelor de la alin. (1), certificatele calificate pentru semnături electronice sau pentru sigilii electronice conțin:

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

b) 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

c) 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 a sigiliului

electronic

(1) Crearea semnăturii electronice sau a sigiliului electronic se efectuează prin intermediul

dispozitivului de creare a semnăturilor electronice sau a sigiliilor electronice și/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 a sigiliilor electronice calificate, în numele semnatarului sau creatorului sigiliului electronic, 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 electronice sau a sigiliilor

electronice

(1) Dispozitivele de creare a semnăturilor electronice sau a sigiliilor electronice avansate sau calificate trebuie să asigure, prin intermediul mijloacelor tehnice și procedurilor corespunzătoare, că cel puțin:

a) datele de creare a semnăturii electronice sau a sigiliului electronic nu pot apărea decât o singură dată, iar confidențialitatea 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, iar semnătura electronică sau sigiliul electronic sunt protejate împotriva posibilelor falsificări prin mijloacele tehnice disponibile la data respectivă;

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

d) oferă posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura electronică sau sigiliul electronic ori face referința irevocabilă la documentul respectiv;

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

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

(2) Generarea sau gestionarea datelor de creare a semnăturilor electronice sau a sigiliului electronic, în numele semnatarului ori al creatorului sigiliului electronic, pot fi realizate numai de către un prestator de servicii de încredere calificat.

(3) Dispozitivele de creare a semnăturilor electronice sau a sigiliilor electronice avansate ori calificate nu trebuie să modifice datele cărora li se aplică semnătura electronică sau sigiliul electronic avansat sau calificat, ori să împiedice prezentarea datelor respective semnatarului sau creatorului sigiliului electronic înainte de semnare ori de aplicare a sigiliului electronic.

Articolul 28. Verificarea autenticității semnăturii

electronice sau a sigiliului electronic

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

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

a) să ofere posibilitatea afișării conținutului documentului electronic sau să facă referință irevocabilă la documentul respectiv;

b) să afișeze faptul modificării documentului electronic;

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

(3) La verificarea semnăturii electronice avansate sau a sigiliului electronic avansat, precum și a semnăturii electronice calificate sau a sigiliului electronic calificat trebuie să se garanteze, cu o siguranță suficientă, că:

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

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

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

d) conținutul certificatului cheii publice este redat clar;

e) modificările care pot influența securitatea semnăturii electronice sau a sigiliului electronic pot fi detectate.

Articolul 29. Cerințe pentru validarea semnăturii electronice

calificate și a sigiliului electronic calificat

Procesul de validare a semnăturii electronice calificate sau a sigiliului electronic calificat confirmă validitatea acestora cu următoarele condiții:

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

c) datele de validare a semnăturilor electronice sau a 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 pseudonimului 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 electronice sau a sigiliilor electronice calificate;

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

h) cerințele prevăzute la art. 24 erau întrunite 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 are formă electronică sau că nu întrunește cerințele pentru marca temporală electronică calificată.

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

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 întrunește următoarele cerințe:

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

b) se bazează pe o sursă de timp exactă, legată de ora universală coordonată;

c) acesteia îi este aplicată semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat ori 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 mărcilor temporale recunoscute conform art. 3.

Secțiunea a 4-a

Serviciul de distribuție electronică înregistrată

și autentificare a 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 probă în procedurile judiciare doar din motivul că acestea au formă electronică sau că nu întrunesc cerințele pentru serviciul de distribuție electronică înregistrată calificat.

(2) Datele transmise și primite prin utilizarea unui 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, precum și a exactității 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 întrunesc următoarele cerințe:

a) sunt prestate de 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 sunt securizate 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 modificate fără ca acest lucru să fie detectat;

e) modificarea datelor necesare în scopul de a transmite sau primi datele este clar indicată expeditorului și destinatarului datelor;

f) data și ora transmiterii, ale primirii și ale modificărilor datelor sunt indicate prin mărci temporale electronice calificate.

Articolul 34. Cerințe pentru certificatele calificate

pentru autentificarea unei pagini web

Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină:

a) mențiunea, 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) gestionat(e) 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 ori 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) datele 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) Organul 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 funcția prestatorului de servicii de încredere calificat de nivel superior pentru prestatorii de servicii de încredere calificați;

d) asigură ținerea, actualizarea și accesul public la datele Registrului de evidență a prestatorilor de servicii de încredere;

e) menține și publică, în mod securizat, liste sigure, cărora le 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 și aprobă, prin acte normative, cerințele în domeniul serviciilor de încredere;

g) supraveghează și controlează respectarea cerințelor cu privire 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 și 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 privind îndeplinirea cerințelor stabilite de prezenta lege;

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

l) cooperează cu autoritatea naţională pentru protecția 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 încălcările cerințelor prevăzute de prezenta lege;

n) realizează colaborarea internațională în domeniul serviciilor de încredere.

(3) Autoritatea sau instituția publică responsabilă de prestarea serviciului de sursă unică de sincronizare cu timpul universal coordonat (UTC) este stabilită de Guvern.

Articolul 36. Controlul în domeniul serviciilor de încredere

(1) Controlul privind respectarea cerințelor stabilite de prezenta lege cu privire la prestarea serviciilor de încredere și la acreditare sau prelungirea termenului acreditării este efectuat de către organul de supraveghere și 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 și control.

(3) Comisia se instituie în cadrul organului de supraveghere și control, în baza ordinului privind efectuarea controlului, emis de conducătorul organului respectiv.

(4) Componența nominală a Comisiei se stabilește pentru fiecare caz în parte.

(5) Comisia este în drept:

a) să beneficieze de acces liber la materialele documentare, pe suport de hârtie și în formă electronică, necesare pentru desfășurarea activităților ce ţin de prestarea serviciilor de încredere, precum și la sistemele de distribuție de aplicații software, la aplicațiile software și la mijloacele hardware instalate;

b) să obțină informații complete despre condițiile și modul de exploatare a mijloacelor software și hardware;

c) să obțină de la persoanele responsabile și de la personalul prestatorului de servicii de încredere informațiile 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 și fără prezentarea actelor de identitate ale membrilor Comisiei.

(7) La efectuarea controlului privind respectarea cerințelor prevăzute de prezenta lege, Comisia ține cont de:

a) legalitatea și respectarea competenței stabilite de lege;

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

c) tratarea dubiilor, apărute la aplicarea legislației, 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 acțiunile organului de supraveghere și control, inclusiv în instanța judecătorească.

(8) Controalele planificate privind respectarea de către prestatorul de servicii de încredere calificat a cerințelor și obligațiilor prevăzute de prezenta lege se efectuează de către organul de supraveghere și control cel mult o dată în decursul anului calendaristic, cu cooptarea, după caz, a reprezentanților instituțiilor cu funcții de reglementare și de control, conform competenței.

(9) Planurile controalelor, elaborate de organul de supraveghere și control și aprobate în modul stabilit, se coordonează, în privința termenelor de efectuare, cu conducerea prestatorului de servicii de încredere cu cel puțin 5 zile lucrătoare înainte de demararea controalelor respective.

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

a) depistării și confirmării, de către organul supraveghere și control, a încălcărilor prezentei legi; și/sau

b) recepționării cererilor și reclamațiilor argumentate, adresate în formă scrisă organului de supraveghere și control, referitoare la încălcările sau la îndeplinirea necorespunzătoare a obligațiilor 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 prescripției privind înlăturarea 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 și a controlului inopinat nu poate depăși 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 de supraveghere și control în baza unei decizii motivate, adusă la cunoștința prestatorului de servicii de încredere supus controlului, care poate fi contestată de către prestatorul de servicii de încredere.

(15) La efectuarea controlului privind respectarea cerințelor și obligațiilor prevăzute de prezenta lege, prestatorul de servicii de încredere prezintă informația și documentele relevante scopului controlului și 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, prestatorului de servicii de încredere, iar cel de-al doilea se păstrează la organul de supraveghere și control. În cazul în care prestatorul de servicii de încredere nu este de acord cu rezultatele controlului efectuat, în termen de 10 zile lucrătoare de la data primirii actului de control, acesta poate prezenta în scris argumentele privind dezacordul, anexând documentele relevante.

(17) În cazul în care se depistează încălcări ale cerințelor prevăzute de prezenta lege, organul de supraveghere și control emite, în baza actului de control, prescripția privind înlăturarea acestor încălcări, ce cuprinde recomandările privind modul de remediere a tuturor încălcărilor constatate, precum și avertizarea despre posibila suspendare sau retragere a acreditării dacă acestea nu vor fi înlăturate în termenul stabilit.

(18) Termenul pentru înlăturarea încălcărilor constatate constituie 15 zile lucrătoare, calculat

din ziua următoare celei în care a fost primită prescripția expediată/înmânată împreună cu actul de control.

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

(20) Prestatorul de servicii de încredere calificat care a primit prescripţia privind înlăturarea încălcărilor cerințelor și obligațiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripţie, să comunice organului de supraveghere și control informația privind înlăturarea încălcărilor.

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

(22) Prestatorul de servicii de încredere are dreptul să depună la organul de supraveghere și control reclamații în scris privind încălcările prevederilor prezentei legi admise de Comisie sau să conteste acțiunile acesteia în instanța de judecată.

Articolul 37. Suspendarea și reluarea valabilității acreditării

(1) Acreditarea este suspendată în conformitate cu legislația în domeniul reglementării activității de întreprinzător.

(2) Drept temei pentru realizarea acțiunilor 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 cerințelor și obligațiilor stabilite de prezenta lege;

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

d) nevalabilitatea garanției bancare sau a poliței de asigurare;

e) nerespectarea de către prestatorul de servicii de încredere a prescripției privind înlăturarea încălcărilor prevăzute de prezenta lege, constatate în urma controlului efectuat de Comisie.

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

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

(5) Decizia privind reluarea valabilității acreditării se ia de către organul de supraveghere și control în temeiul hotărârii instanței de judecată care a emis hotărârea de suspendare a acreditării sau în temeiul hotărârii instanței de judecată ierarhic superioare, în termen de 3 zile lucrătoare de la data primirii înștiințării. Decizia se aduce la cunoștința prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data luării acesteia.

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

Articolul 38. Retragerea acreditării

(1) Acreditarea este retrasă în conformitate cu legislația în domeniul reglementării activității de întreprinzător.

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

a) cererea prestatorului de servicii de încredere calificat privind încetarea activității, 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 transmiterii certificatului de acreditare sau a copiei de pe acesta altei persoane în scopul desfășurării genului de activitate acreditat;

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

e) nerespectarea repetată a prescripţiilor privind înlăturarea încălcărilor cerințelor stabilite de prezenta lege.

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

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

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

Articolul 39. Cerințe de securitate aplicabile prestatorilor

de servicii de încredere

(1) Prestatorii de servicii de încredere calificați și necalificați aplică măsurile tehnice și organizaționale 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, nu mai târziu de 24 de ore din momentul constatării, încălcarea securității sau pierderea integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de aceștia. 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 și persoanei fizice sau juridice respective încălcarea securității sau pierderea integrității, fără întârzieri nejustificate.

(3) Organul de supraveghere și 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

ȘI CIRCULAȚIA ELECTRONICĂ A DOCUMENTELOR

Articolul 40. Regimul juridic de utilizare a documentului

electronic

(1) Documentul electronic semnat cu semnătură electronică calificată este asimilat, după efectele acestuia, cu documentul similar 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 similar pe suport de hârtie, semnat cu semnătură olografă, doar în cazurile stabilite expres de actele normative sau de acordul părților privind aplicarea semnăturilor sau sigiliilor electronice, cu respectarea condițiilor stipulate la art. 43 alin. (1).

(3) Actele normative sau acordul părților privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaștere a documentelor electronice, semnate cu alt tip de semnătură electronică decât cea calificată, asimilate, după efectele lor, cu documente similare pe suport de hârtie, semnate cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum și obligațiile părților privind confidențialitatea și răspunderea materială.

(4) În cazul în care, conform legislației, se cere ca documentul să fie perfectat sau prezentat pe suport de hârtie și semnat cu semnătură olografă, documentul electronic se consideră corespunzător cerințelor respective.

(5) În cazul în care, conform legislației, se cere ca documentul pe suport de hârtie să fie autentificat cu ștampilă, documentul electronic se consideră a fi corespunzător cerinței respective.

(6) Pe mai multe documente electronice legate între acestea (set de documente electronice) se aplică o singură semnătură electronică sau un singur sigiliu electronic.

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

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

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

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

(11) În cazul în care o persoană creează un document electronic și un document pe suport de

hârtie semnat cu semnătură olografă, identice după conținut, ambele se consideră documente de sine stătătoare și originale.

(12) Copia de pe documentul electronic se consideră reprezentarea (redarea) acestuia pe suport de hârtie, într-o formă perceptibilă. Copia de pe documentul electronic se autentifică în modul prevăzut de legislație pentru autentificarea copiilor de pe documentele pe suport de hârtie și conține mențiunea despre faptul că este copie de pe documentul electronic.

Articolul 41. Domeniile și scopul utilizării documentului

electronic

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

(2) Documentul electronic poate fi utilizat în scopul expedierii informației, ținerii corespondenței, întocmirii actelor juridice, precum și în calitate de document care reflectă fapte economice.

Articolul 42. Cerințele față de documentul electronic

Documentul electronic trebuie să corespundă următoarelor cerințe principale:

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

b) să conțină, pentru confirmarea autenticității acestuia, una sau mai multe semnături electronice sau sigilii electronice care corespund condițiilor și cerințelor stabilite de prezenta lege;

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

d) să fie afișat într-o formă perceptibilă;

e) să permită utilizarea repetată a acestuia.

Articolul 43. Autenticitatea documentului electronic

(1) Documentul electronic este considerat autentic dacă întrunește cumulativ următoarele condiții:

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 documentul electronic este aplicată semnătura electronică autentică sau sigiliul electronic autentic al semnatarului sau al creatorului sigiliului electronic indicat în document.

(2) Verificarea autenticității documentului electronic se efectuează prin verificarea, cu ajutorul dispozitivelor de verificare a semnăturilor electronice sau a sigiliilor electronice și/sau al produsului, a autenticității semnăturii electronice sau a sigiliului electronic.

Articolul 44. Organizarea circulației electronice

a documentelor

(1) Circulația electronică a documentelor este organizată conform prevederilor prezentei legi și regulilor stabilite de către proprietarul sistemului de circulație electronică a documentelor, precum și conform contractelor încheiate între subiecții circulației electronice a documentelor.

(2) Circulația electronică a documentelor poate include:

a) crearea și prelucrarea documentelor electronice cu aplicarea semnăturii electronice sau a sigiliului electronic;

b) expedierea și recepționarea documentelor electronice;

c) verificarea autenticității documentelor electronice;

d) confirmarea recepționării documentelor electronice;

e) evidența documentelor electronice;

f) păstrarea, modificarea și/sau nimicirea documentelor electronice;

g) crearea exemplarelor suplimentare ale documentelor electronice;

h) crearea și autentificarea copiilor pe suport de hârtie de pe documentele electronice;

i) aplicarea mărcii temporale electronice.

(3) Modul de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentelor electronice pentru sistemele de circulație electronică a documentelor persoanelor juridice de drept public se stabilește de Guvern, iar pentru sistemele de circulație electronică a documentelor persoanelor juridice de drept privat – de către proprietarii acestora.

Articolul 45. Intermediarul în circulația electronică

a documentelor

(1) La organizarea și efectuarea circulației electronice a documentelor pot participa intermediari în condițiile prezentei legi și în conformitate cu regulile stabilite de proprietarul sistemului de circulație electronică a documentelor.

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

a) să dispună de mijloace software și/sau hardware ce asigură fiabilitatea și securitatea sistemelor informaționale utilizate;

b) să dispună de personal cu competență și experiență în domeniul tehnologiei informației și/sau al securității informaționale;

c) să asigure condițiile necesare pentru stabilirea exactă a timpului și a sursei de expediere a documentului electronic, precum și a timpului recepționării și a adresei electronice a destinatarului;

d) să asigure protecția și păstrarea documentelor electronice;

e) să păstreze documentele electronice conform contractului cu utilizatorii sistemului de

circulație electronică a documentelor.

Articolul 46. Crearea documentului electronic

(1) Documentul electronic include informația, care constituie conținutul documentului electronic, și semnătura electronică sau sigiliul electronic al semnatarului ori al creatorului sigiliului electronic.

(2) Crearea documentului electronic se finalizează prin aplicarea semnăturii electronice sau a sigiliului electronic de către semnatar sau de către creatorul sigiliului electronic și, după caz, prin aplicarea mărcii temporale electronice.

Articolul 47. Expedierea și recepționarea documentului

electronic

(1) Documentul electronic poate fi expediat și recepționat cu ajutorul sistemelor informaționale și de comunicații electronice și/sau al purtătorilor materiali.

(2) Documentul electronic se expediază într-un mod ce permite păstrarea și utilizarea acestuia de către destinatar.

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

a) este expediat de către semnatar sau creatorul sigiliului electronic ori de către un intermediar în circulația electronică a documentelor, care acționează în numele semnatarului sau al creatorul sigiliului electronic, sau prin sistemul informațional utilizat de către semnatar sau creatorul sigiliului electronic;

b) este adresat în mod corespunzător sau este direcționat în sistemul informațional indicat de destinatar;

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

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

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

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

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

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

a) persoana indicată în documentul electronic ca semnatar nu este semnatarul acestuia;

b) semnatarul nu este inițiatorul expedierii documentului electronic;

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

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

Articolul 48. Momentul expedierii și al recepționării

documentului electronic

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

(2) Dacă semnatarul sau creatorul sigiliului electronic și destinatarul documentului electronic nu au convenit altfel, momentul recepționării documentului electronic se consideră momentul intrării acestuia în sistemul informațional indicat de destinatar. În cazul în care destinatarul documentului electronic nu a indicat sistemul informațional respectiv, documentul electronic se consideră recepționat din momentul intrării acestuia în sistemul informațional 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 informațional prin care a fost transmis.

(3) Momentul expedierii documentului electronic în sistemele informaționale poate fi confirmat, în caz de necesitate, prin aplicarea mărcii temporale electronice pe documentul electronic respectiv.

(4) Dacă semnatarul sau creatorul sigiliului electronic și destinatarul documentului electronic au convenit asupra confirmării recepționării documentului electronic, momentul recepționării acestuia se consideră momentul expedierii de către destinatar a confirmării privind recepționarea, cu aplicarea mărcii temporale electronice, după caz.

Articolul 49. Evidența documentelor electronice

(1) Evidența documentelor electronice ale persoanelor fizice și/sau juridice se efectuează în conformitate cu legislația cu privire la registre.

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

Articolul 50. Păstrarea documentelor electronice

(1) Subiecții circulației electronice a documentelor sunt obligați să păstreze originalele documentelor electronice într-un mod ce permite verificarea autenticității acestora.

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

(3) Subiecții circulației electronice a documentelor pot asigura păstrarea acestora utilizând serviciile intermediarului în circulația electronică a documentelor, cu condiția respectării prevederilor prezentei legi.

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

Articolul 51. Protecția documentului electronic

(1) Documentul electronic beneficiază de aceeași protecție juridică ca și documentul similar pe suport de hârtie.

(2) Informația care constituie conținutul documentului electronic este utilizată și protejată, conform legislației, în funcție de statutul și gradul de protecție a acesteia.

(3) Crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea și/sau nimicirea documentului electronic trebuie să corespundă cerințelor de securitate stabilite de Guvern pentru sistemele de circulație electronică a documentelor persoanelor juridice de drept public. Cerințele de securitate pentru sistemele de circulație electronică a documentelor persoanelor juridice de drept privat sunt stabilite de către proprietarii acestora.

(4) În procesul de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentului electronic se impune păstrarea informației care permite stabilirea originii, apartenenței și destinației documentului electronic, precum și a datei și orei creării, expedierii și recepționării acestuia.

Capitolul V

PROTECȚIA DATELOR CU CARACTER PERSONAL.

RĂSPUNDEREA JURIDICĂ

Articolul 52. Protecția datelor cu caracter personal

Prestatorii de servicii de încredere asigură respectarea legislației în domeniul protecției datelor cu caracter personal în procesul de prestare a serviciilor de încredere.

Articolul 53. Răspunderea persoanelor fizice și juridice

care cad sub incidența prezentei legi

(1) Persoanele fizice și juridice poartă răspundere juridică, conform legislației, pentru neîndeplinirea prevederilor prezentei legi.

(2) Intermediarul în circulația electronică a documentelor poartă răspundere juridică, conform legislației, pentru neîndeplinirea sau îndeplinirea defectuoasă a obligațiilor prevăzute de prezenta lege, pentru calitatea necorespunzătoare a serviciilor prestate, precum și pentru prejudiciul cauzat de acțiunile și/sau inacțiunile sale.

(3) Litigiile apărute în cadrul circulației electronice a documentelor, precum și cele legate de utilizarea documentelor electronice și a serviciilor de încredere se soluționează de către subiecții circulației electronice a documentelor în conformitate cu legislația și contractele încheiate.

Articolul 54. Răspunderea prestatorului de servicii

de încredere și sarcina probei

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

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

(3) Intenția sau neglijența 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 depășesc restricțiile stabilite în cazul în care prestatorii informează clienții prealabil și în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care 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 obligațiilor prevăzute de prezenta lege;

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

Capitolul VI

DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 56. Dispoziții finale

(1) Prezenta lege intră în vigoare peste 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 și documentul electronic.

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

a) va prezenta propuneri Parlamentului privind aducerea legislației în vigoare în concordanță cu prezenta lege;

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

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

Articolul 57. Dispoziții tranzitorii

(1) Certificatele cheilor publice eliberate în baza Legii nr. 91/2014 privind semnătura electronică și 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 acreditați în baza Legii nr. 91/2014 privind semnătura electronică și documentul electronic sunt obligați să treacă procedura de acreditare în conformitate cu prevederile prezentei legi.

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

PREȘEDINTELE PARLAMENTULUI Igor GROSU

Nr. 124. Chișinău, 19 mai 2022.