PARLAMENTUL REPUBLICII MOLDOVA

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

L E G E
privind semnătura electronică şi documentul electronic

nr. 91 din 29.05.2014

Monitorul Oficial nr.174-177/397 din 04.07.2014

* * *

Parlamentul adoptă prezenta lege organică.

Prezenta lege creează cadrul necesar aplicării Directivei nr.1999/93/CE a Parlamentului European şi a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, publicată în Jurnalul Oficial al Comunităţilor Europene nr.L 13 din 19 ianuarie 2000.

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Scopul legii şi domeniul de aplicare

(1) Prezenta lege stabileşte regimul juridic al semnăturii electronice şi al documentului electronic, inclusiv cerinţele principale faţă de valabilitatea acestora şi cerinţele principale faţă de serviciile de certificare.

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

(3) Recunoaşterea semnăturii electronice şi a documentului electronic 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 decît cele prevăzute de prezenta lege, se aplică normele tratatelor internaţionale.

Articolul 2. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni semnifică:

acreditare voluntară – autorizaţie care prevede drepturi şi obligaţii specifice prestării de servicii de certificare, acordată, la cererea prestatorului de servicii de certificare, de către organul competent responsabil de stabilirea drepturilor şi obligaţiilor respective şi de supravegherea respectării acestora, în cazul în care prestatorul de servicii de certificare nu este împuternicit să exercite drepturile care decurg din autorizaţie pînă nu a primit decizia organului respectiv;

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;

autenticitate a documentului electronic – calitate a documentului electronic care constă în faptul că acesta este semnat de persoana care deţine o semnătură electronică autentică şi este abilitată cu drept de semnătură;

certificat al cheii publice – document electronic ce conţine cheia publică, este semnat cu semnătura electronică a prestatorului de servicii de certificare, atestă apartenenţa cheii respective titularului de certificat al cheii publice şi permite identificarea acestui titular;

certificat calificat al cheii publice – certificat al cheii publice care întruneşte cerinţele prevăzute la art.31 şi este eliberat de un prestator de servicii de certificare ce întruneşte cerinţele prevăzute la art.26;

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

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

circulaţie electronică a documentelor – totalitatea proceselor de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentelor electronice;

date de creare a semnăturii electronice – date unice, precum codurile sau cheile private, care sînt utilizate de semnatar pentru crearea unei semnături electronice;

date de verificare a semnăturii electronice – date, precum codurile sau cheile publice, care sînt utilizate în scopul verificării unei semnături electronice;

dispozitiv de creare a semnăturii electronice – mijloace tehnice şi/sau de program configurate, utilizate pentru punerea în aplicare a datelor de creare a semnăturii electronice;

dispozitiv securizat de creare a semnăturii electronice – dispozitiv de creare a semnăturii electronice care întruneşte cerinţele prevăzute la art.8 alin.(3) şi (4);

dispozitiv de verificare a semnăturii electronice – mijloace tehnice şi/sau de program configurate, utilizate pentru punerea în aplicare a datelor de verificare a semnăturii electronice;

destinatar al documentului electronic – persoană fizică sau juridică căreia îi este adresat documentul electronic sau altă persoană care, în condiţiile legii sau ale contractului, recepţionează documentul electronic;

document electronic – informaţie în formă electronică, creată, structurată, prelucrată, păstrată şi/sau transmisă prin intermediul computerului sau al altor dispozitive electronice, semnată cu semnătură electronică în conformitate cu prezenta lege;

intermediar în circulaţia electronică a documentelor – întreprinzător individual sau persoană juridică care, din însărcinarea semnatarului şi/sau a destinatarului documentului electronic, organizează şi administrează sistemul de circulaţie electronică a documentelor şi/sau prestează servicii legate de circulaţia electronică a documentelor;

marcă temporală – atribut al documentului electronic, care, prin intermediul semnăturii electronice, certifică faptul că informaţia a existat la un moment de timp determinat, cu păstrarea autenticităţii şi integrităţii documentului electronic;

prestator de servicii de certificare – întreprinzător individual sau persoană juridică care prestează servicii de certificare;

produs asociat semnăturii electronice – mijloace tehnice sau de program ori componente specifice ale acestora, destinate a fi utilizate de către un prestator de servicii de certificare la prestarea serviciilor de certificare sau destinate a fi utilizate pentru crearea ori verificarea semnăturilor electronice;

Registrul împuternicirilor de reprezentare în baza semnăturii electronice – registru ţinut în formă electronică în care sînt consemnate împuternicirile de reprezentare în baza semnăturii electronice acordate de către persoane fizice sau juridice unei alte persoane;

semnatar – persoană care deţine un dispozitiv de creare a semnăturii electronice şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care o reprezintă;

semnătură electronică – date în formă electronică, care sînt ataşate la sau logic asociate cu alte date în formă electronică şi care sînt utilizate ca metodă de autentificare;

servicii de certificare – servicii de certificare a cheilor publice, de aplicare a mărcii temporale, alte servicii conexe în domeniul semnăturii electronice;

sistemul de circulaţie electronică a documentelor – sistem tehnico-organizatoric ce asigură circulaţia documentelor electronice.

Capitolul II
REGIMUL JURIDIC AL SEMNĂTURII ELECTRONICE

Articolul 3. Principiile de utilizare a semnăturii electronice

Principiile de utilizare a semnăturii electronice sînt următoarele:

a) libertatea alegerii şi utilizării oricărui tip de semnătură electronică, dacă actele normative sau acordul părţilor nu prevăd cerinţa de utilizare a unui tip concret de semnătură electronică, 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 în conformitate cu prevederile prezentei legi;

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice şi/sau a documentului electronic semnat prin intermediul acesteia doar în baza faptului că semnătura electronică nu a fost creată manual, dar prin intermediul dispozitivului de creare a semnăturii şi/sau al produsului asociat semnăturii electronice.

Articolul 4. Tipuri de semnături electronice

(1) Tipurile de semnături electronice, ale căror principii şi mecanisme de utilizare sînt reglementate de prezenta lege, sînt următoarele:

a) semnătura electronică simplă;

b) semnătura electronică avansată necalificată;

c) semnătura electronică avansată calificată.

(2) Semnătura electronică simplă este semnătura electronică utilizată ca metodă de autentificare, fără a face trimitere exclusiv la semnatar.

(3) Semnătura electronică avansată necalificată este o semnătură electronică ce îndeplineşte următoarele cerinţe:

a) face trimitere exclusiv la semnatar;

b) permite identificarea semnatarului;

c) este creată prin mijloace controlate exclusiv de semnatar; şi

d) este legată de datele la care se raportează, astfel încît orice modificare ulterioară a acestor date poate fi detectată.

(4) Semnătura electronică avansată calificată este o semnătură electronică care îndeplineşte toate cerinţele semnăturii electronice avansate necalificate şi, suplimentar:

a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate;

b) este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice şi se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice şi/sau al

produsului asociat semnăturii electronice, care dispun de confirmarea corespunderii cu cerinţele prevăzute de prezenta lege.

Articolul 5. Regimul juridic de utilizare a semnăturii electronice

(1) Semnătura electronică, 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 acreditat de servicii de certificare; sau

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

d) nu este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice.

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

(3) Modalitatea în care se va asigura gradul de protecţie a semnăturii electronice avansate calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hîrtie se stabileşte de organul competent, conform atribuţiilor prevăzute la art.36 alin.(1).

(4) 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.

(5) Semnătura electronică nu constituie un mijloc de criptare a informaţiei.

Articolul 6. Recunoaşterea semnăturilor electronice străine

(1) Certificatul cheii publice eliberat de către un prestator de servicii de certificare 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 certificare cu domiciliul sau cu sediul în Republica Moldova dacă este întrunită una dintre următoarele condiţii:

a) prestatorul de servicii de certificare 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 certificare acreditat cu domiciliul sau cu sediul în Republica Moldova garantează recunoaşterea certificatului;

c) certificatul sau prestatorul de servicii de certificare 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.

(2) Semnătura electronică şi documentul electronic semnat cu semnătură electronică 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.

Articolul 7. Cheia privată şi cheia publică

(1) Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate necalificate se creează de către persoana fizică. Acestea pot fi create de persoane terţe, prin acordul expres al persoanei fizice respective, cu condiţia asigurării imposibilităţii de copiere a acestor chei.

(2) Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate calificate se creează de către prestatorul de servicii de certificare prin intermediul dispozitivului

securizat de creare a semnăturii. În cazul utilizării dispozitivului securizat de creare a semnăturii în baza cartelei SIM, prestatorul de servicii de certificare asigură persoanei fizice iniţierea procedurii de creare a cheii private şi a cheii publice.

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

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

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

(6) Cheia publică este certificată de către prestatorul de servicii de certificare şi este accesibilă tuturor.

Articolul 8. Crearea semnăturii electronice

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

(2) La crearea semnăturii electronice simple, părţile se bazează pe prevederile acordului încheiat.

(3) La crearea semnăturii electronice avansate necalificate şi a semnăturii electronice avansate calificate, dispozitivul de creare a semnăturii electronice şi/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic semnat cu semnătura electronică sau să facă referinţa irevocabilă la documentul dat;

b) să creeze o semnătură electronică numai după confirmarea de către semnatar a operaţiunii de creare a semnăturii electronice;

c) să confirme în mod univoc crearea semnăturii electronice.

(4) Dispozitivele securizate de creare a semnăturii electronice trebuie să asigure, prin mijloace tehnice şi proceduri corespunzătoare, cel puţin că:

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

b) datele de creare a semnăturii electronice nu pot fi deduse prin calcul şi semnătura este protejată împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată;

c) datele de creare a semnăturii electronice sînt protejate în mod fiabil de semnatarul legitim împotriva utilizării de către alte persoane.

(5) Dispozitivele securizate de creare a semnăturii electronice nu trebuie să modifice datele care urmează a fi semnate sau să împiedice prezentarea lor semnatarului înainte de semnare.

Articolul 9. Verificarea autenticităţii semnăturii electronice

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

(2) La verificarea semnăturii electronice simple, părţile se bazează pe prevederile acordului încheiat, care trebuie să prevadă modalitatea de confirmare a integrităţii documentului electronic semnat.

(3) La verificarea semnăturii electronice avansate necalificate şi semnăturii electronice avansate calificate, dispozitivul de verificare a semnăturii electronice şi/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic semnat cu semnătura electronică sau să facă referinţa irevocabilă la documentul dat;

b) să afişeze faptul modificării documentului electronic semnat cu semnătura electronică;

c) să facă referinţă la semnatar.

(4) La verificarea securizată a semnăturii electronice avansate necalificate şi a semnăturii electronice avansate calificate trebuie să se garanteze, cu o siguranţă suficientă, că:

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

b) semnătura electronică este verificată cu certitudine, iar rezultatul verificării şi identitatea semnatarului sînt corect afişate;

c) autenticitatea şi valabilitatea certificatului cheii publice solicitat în momentul verificării semnăturii electronice sînt verificate cu certitudine;

d) conţinutul certificatului cheii publice este redat clar; şi

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

Articolul 10. Utilizarea semnăturii electronice simple

(1) Documentul electronic se consideră semnat cu semnătura electronică simplă dacă este întrunită una dintre următoarele condiţii:

a) semnătura electronică simplă se conţine nemijlocit în documentul electronic sau este logic asociată cu documentul electronic;

b) datele de creare a semnăturii electronice simple se aplică în corespundere cu regulile stabilite de către operatorul sistemului informatic prin intermediul căruia se efectuează crearea şi/sau expedierea documentului electronic şi în documentul electronic se conţine informaţia care identifică persoana în numele căreia a fost creat şi expediat documentul electronic.

(2) Actele normative şi/sau acordul părţilor, care stabilesc cazurile de recunoaştere a documentelor electronice semnate cu semnătura electronică simplă, echivalente documentelor pe suport de hîrtie semnate cu semnătura olografă, trebuie să prevadă următoarele:

a) modalitatea de identificare a persoanei în numele căreia este semnat documentul electronic în baza semnăturii electronice simple a acesteia;

b) obligaţia persoanei care creează şi/sau utilizează date de creare a semnăturii electronice simple de a asigura confidenţialitatea acestora.

Articolul 11. Limitele utilizării unor tipuri de semnături electronice

Nu se admite utilizarea semnăturii electronice simple şi a semnăturii electronice avansate necalificate pentru:

a) semnarea documentelor electronice ce conţin informaţie atribuită la secretul de stat;

b) semnarea documentelor electronice în raporturile juridice ale persoanelor juridice de drept public cu persoanele fizice şi cu persoanele juridice de drept privat.

Articolul 12. Registrul împuternicirilor de reprezentare în baza semnăturii electronice

(1) Registrul împuternicirilor de reprezentare în baza semnăturii electronice conţine date privind persoanele împuternicite, persoanele reprezentate, rolul şi scopul împuternicirilor, data acordării împuternicirilor, durata împuternicirilor, alte menţiuni privind acordarea, modificarea sau retragerea împuternicirilor. Împuternicirile pentru care este necesară forma autentică sînt înregistrate în Registrul împuternicirilor de reprezentare în baza semnăturii electronice cu respectarea legislaţiei notariale.

(2) Orice modificare în Registrul împuternicirilor de reprezentare în baza semnăturii electronice privind delegarea împuternicirilor poate fi realizată doar de către persoana care acordă împuternicirile respective.

(3) Posesorul şi deţinătorul Registrului împuternicirilor de reprezentare în baza semnăturii electronice, precum şi modul de creare şi actualizare a acestuia sînt stabilite de Guvern.

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

Articolul 13. Regimul juridic de utilizare a documentului electronic

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

(2) Documentul electronic semnat cu semnătură electronică simplă sau cu semnătură electronică avansată necalificată este asimilat, după efectele sale, cu documentul analog pe suport de hîrtie, semnat cu semnătură olografă, doar în cazurile stabilite expres de actele normative sau de acordul părţilor privind aplicarea semnăturilor electronice, cu respectarea condiţiilor stipulate la art.16 alin.(1).

(3) Actele normative sau acordul părţilor privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaştere a documentelor electronice, semnate cu semnătură electronică simplă sau cu semnătură electronică avansată necalificată, asimilate, după efectele lor, cu documente analoage pe suport de hîrtie, 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 hîrtie 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 hîrtie să fie autentificat cu ştampilă, documentul electronic se consideră a fi corespunzător acestei cerinţe.

(6) Cu o singură semnătură electronică pot fi semnate cîteva documente electronice legate între ele (setul de documente electronice). În cazul semnării cu semnătură electronică a setului de documente electronice, fiecare document inclus în acest set se consideră semnat cu acelaşi tip de semnătură electronică.

(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. Documentul electronic nu poate fi respins în calitate de probă 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 sînt considerate originale şi produc aceleaşi efecte juridice.

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

(12) Copie a documentului electronic se consideră reprezentarea (redarea) acestuia pe suport de hîrtie, într-o formă perceptibilă. Copia documentului electronic se autentifică în modul

prevăzut de legislaţie pentru autentificarea copiilor documentelor pe suport de hîrtie şi conţine menţiunea despre faptul că este copie a documentului electronic.

Articolul 14. 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 tehnice şi de program 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 15. 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 tehnice şi/sau de program;

b) să conţină, pentru confirmarea autenticităţii acestuia, una sau mai multe semnături 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;

d) să fie afişat într-o formă perceptibilă;

e) să permită utilizarea sa repetată.

Articolul 16. Autenticitatea documentului electronic

(1) Documentul electronic este considerat autentic dacă întruneşte cumulativ următoarele condiţii:

a) este semnat de persoana abilitată, în modul stabilit, să semneze cu semnătură olografă documentul echivalent pe suport de hîrtie;

b) este semnat cu semnătura electronică autentică a semnatarului indicat în document.

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

Articolul 17. 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;

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 hîrtie;

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 18. 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 de utilaje şi mijloace tehnice şi/sau de program 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 19. Crearea documentului electronic

(1) Documentul electronic este creat de semnatar şi conţine informaţia ce constituie conţinutul documentului electronic şi semnătura electronică a semnatarului.

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

Articolul 20. 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 şi destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră expediat dacă:

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

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 de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului.

(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 21. Momentul expedierii şi recepţionării documentului electronic

(1) Dacă semnatarul 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 de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului.

(2) Dacă semnatarul 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 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 22. Evidenţa documentelor electronice

(1) Evidenţa documentelor electronice ale persoanelor fizice şi/sau juridice se efectuează în conformitate cu legislaţia, prin ţinerea registrelor electronice şi/sau pe suport de hîrtie.

(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 23. Păstrarea documentelor electronice

(1) Subiecţii circulaţiei electronice a documentelor sînt obligaţi să păstreze originalele documentelor electronice pe suport material 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 hîrtie.

(3) Subiecţii circulaţiei electronice a documentelor pot asigura păstrarea acestora utilizînd 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 24. Protecţia documentului electronic

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

(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 sînt 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 IV
SERVICIILE DE CERTIFICARE

Articolul 25. Prestatorul de servicii de certificare

(1) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple şi a semnăturii electronice avansate necalificate beneficiază de dreptul de a trece procedura de acreditare. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate se supun acreditării obligatorii în conformitate cu prevederile prezentei legi.

(2) Prestatorii de servicii de certificare sînt organizaţi în mod ierarhic. În vîrful ierarhiei se află prestatorul de servicii de certificare de nivel superior.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple şi a semnăturii electronice avansate necalificate îşi organizează ierarhia de sine stătător.

(4) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple formează un singur nivel ierarhic. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate necalificate formează două niveluri ierarhice, inclusiv superior.

(5) Activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, inclusiv ierarhia acestora, se organizează în modul stabilit de Guvern, în conformitate cu prevederile prezentei legi.

(6) Evidenţa prestatorilor de servicii de certificare acreditaţi se ţine de către organul competent în cadrul Registrului de evidenţă a prestatorilor de servicii de certificare, care se actualizează permanent şi la care accesul este public.

(7) Înregistrarea în Registrul de evidenţă a prestatorilor de servicii de certificare se efectuează de către organul competent la data acreditării acestora.

Articolul 26. Acreditarea prestatorului de servicii de certificare

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

(2) Acreditarea în domeniul aplicării semnăturii electronice avansate calificate se acordă prestatorului de servicii de certificare, care întruneşte următoarele cerinţe:

a) dispune de resurse financiare (garanţie bancară sau poliţă de asigurare) în valoare de cel puţin 300 de mii de lei pentru recuperarea unor eventuale prejudicii aduse terţilor din cauza încrederii acestora în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare sau în informaţia din registrul certificatelor eliberate de către prestatorul de servicii de certificare;

b) dispune, pentru prestarea serviciilor de certificare, de personal cu studii superioare în domeniul tehnologiei informaţiei şi/sau al securităţii informaţionale, cu nivel corespunzător de competenţe şi experienţă de gestionare şi expertizare în domeniul tehnologiei semnăturilor electronice;

c) asigură securitatea, fiabilitatea şi continuitatea activităţii de prestare a serviciilor de certificare;

d) asigură înregistrarea informaţiei în registrul certificatelor cheilor publice, în special prestează operativ serviciul de suspendare a valabilităţii certificatului cheii publice şi de revocare a acestuia;

e) asigură posibilitatea de stabilire cu exactitate a datei şi a orei eliberării, suspendării valabilităţii certificatului cheii publice sau revocării acestuia;

f) verifică, în conformitate cu legislaţia, identitatea persoanei pentru care se eliberează un certificat calificat al cheii publice;

g) utilizează sisteme şi produse care sînt protejate împotriva modificărilor şi garantează siguranţa tehnică şi criptografică a funcţiilor pe care şi le asumă;

h) creează condiţii de evitare a falsificării certificatelor şi, în cazul în care prestatorul de servicii de certificare generează date de creare de semnături electronice, garantează confidenţialitatea în procesul de generare a acestor date;

i) utilizează sisteme care nu stochează sau nu copiază datele de creare a semnăturii electronice ale persoanelor pentru care prestatorul de servicii de certificare a prestat servicii de gestionare a cheilor;

j) utilizează sisteme fiabile pentru stocarea certificatelor într-o formă care poate fi verificată, astfel încît:

– numai persoanele autorizate să poată introduce şi modifica date;

– autenticitatea informaţiei să poată fi controlată;

– certificatele să fie disponibile publicului pentru informare;

– toate modificările tehnice care compromit cerinţele de siguranţă să fie vizibile pentru operator.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate anexează la cererea de acreditare documente care confirmă întrunirea cerinţelor specificate la alin.(2) şi, în special, atestă:

a) dispunerea de resurse financiare pentru recuperarea unor eventuale prejudicii;

b) existenţa unei reglementări interne privind asigurarea activităţii prestatorului de servicii de certificare în conformitate cu prevederile prezentei legi;

c) corespunderea sistemelor şi a produselor utilizate cu cerinţele prezentei legi;

d) studiile şi calificările persoanelor cu funcţii de răspundere, ale căror obligaţii funcţionale ţin nemijlocit de prestarea serviciilor de certificare;

e) numirea persoanelor responsabile de activitatea prestatorului de servicii de certificare şi a persoanelor împuternicite să semneze certificatele cheilor publice, precum şi identitatea acestora;

f) ordinea de sincronizare cu Timpul Mondial Coordonat (UTC);

g) dreptul de import, export, proiectare, producere şi comercializare a mijloacelor criptografice şi tehnice de protecţie a informaţiei, a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei, precum şi dreptul de prestare a serviciilor în domeniul protecţiei criptografice şi tehnice a informaţiei, cu excepţia activităţii desfăşurate de autorităţile publice învestite cu acest drept prin lege (licenţa eliberată de către Camera de Licenţiere).

(4) Documentele menţionate la alin.(3) lit.a) se prezintă în original. Documentele menţionate la alin.(3) lit.b)-g) se prezintă în original, însoţite de cîte o copie, originalul fiind restituit după verificarea copiei la momentul prezentării.

(5) La depunerea cererii de acreditare, prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate este obligat să prezinte, în formatul stabilit de organul competent, informaţiile referitoare la procedurile de securitate şi de certificare utilizate, precum şi datele sale de identificare.

(6) Organul competent, în baza documentelor prezentate şi în termen de 30 de zile calendaristice, adoptă decizia privind acreditarea prestatorului de servicii de certificare sau privind refuzul de acreditare.

(7) În cazul adoptării deciziei de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei, notifică prestatorul de servicii de certificare despre decizia luată şi eliberează acestuia certificatul de acreditare de modelul stabilit şi, în conformitate cu actele normative în domeniul semnăturii electronice, înregistrează prestatorul acreditat în Registrul de evidenţă a prestatorilor de servicii de certificare.

(8) În cazul adoptării deciziei privind refuzul de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei de refuz, notifică în scris prestatorul de servicii de certificare despre decizia luată, cu indicarea cauzelor refuzului.

(9) Drept temei pentru refuzul de acreditare serveşte necorespunderea prestatorului de servicii de certificare cerinţelor specificate la alin.(2) sau prezentarea informaţiei neveridice în documentele ce se anexează la cererea de acreditare.

(10) Refuzul de acreditare nu poate împiedica depunerea repetată a documentelor în vederea acreditării după înlăturarea cauzelor care au servit temei pentru refuzul de acreditare.

(11) Decizia privind refuzul de acreditare poate fi contestată în instanţa de judecată în modul stabilit.

(12) Prestatorul de servicii de certificare se consideră acreditat din ziua emiterii certificatului de acreditare.

(13) În caz de deteriorare sau pierdere a certificatului de acreditare, prestatorului de servicii de certificare i se eliberează un duplicat al certificatului în termen de 5 zile lucrătoare, în baza cererii depuse.

(14) Informaţia despre prestatorii de servicii de certificare acreditaţi, precum şi despre cei cu acreditarea retrasă se publică de către organul competent pe pagina sa web oficială.

(15) După primirea certificatului de acreditare pentru prestarea serviciilor de certificare în domeniul aplicării semnăturii electronice avansate calificate, cheia publică a prestatorului de servicii de certificare este certificată de către prestatorul de servicii de certificare de nivel superior în conformitate cu regulamentul aprobat de organul competent.

(16) Acreditarea se consideră acordată sau, după caz, prelungită dacă organul competent nu răspunde solicitantului în termenul prevăzut de lege pentru acordarea sau prelungirea acesteia.

(17) După expirarea termenului de acreditare şi în lipsa unei notificări scrise din partea organului competent, acreditarea se consideră prelungită pentru acelaşi termen.

(18) Prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate sînt obligaţi să comunice organului competent, cu cel puţin 10 zile calendaristice înainte, orice intenţie de modificare a procedurilor de securitate şi de certificare, cu precizarea datei şi orei la care modificarea intră în vigoare, precum şi să confirme, în decurs de 24 de ore, modificarea efectuată.

(19) În cazurile de urgenţă în care securitatea serviciilor de certificare este afectată, prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate pot efectua modificări ale procedurilor de securitate şi de certificare, urmînd să comunice, în termen de 24 de ore, organului competent modificările efectuate şi justificarea deciziei luate.

(20) Prestatorul de servicii de certificare acreditat este obligat, 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 certificare urmează să notifice organul competent despre acest fapt în decurs de 24 de ore.

(21) Prestatorul de servicii de certificare de nivel superior în domeniul aplicării semnăturii electronice avansate calificate nu este supus acreditării în conformitate cu prevederile prezentei legi.

Articolul 27. Activitatea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare:

a) creează şi eliberează certificatele cheilor publice;

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

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

d) prestează, în bază de contract, alte tipuri de servicii ce ţin de semnătura electronică.

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

Articolul 28. Obligaţiile prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare 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 tîrziu 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.43;

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 certificare, 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 certificare şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;

h) să prezinte informaţiile necesare pentru autentificarea semnăturii electronice;

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

j) să îndeplinească alte obligaţii stabilite de prezenta lege.

(2) Prestatorul de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate este obligat, suplimentar:

a) să certifice, în modul stabilit de legislaţie, cheia publică a prestatorului de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate, destinată certificării cheilor publice;

b) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art.31, 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;

c) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul semnăturii sale electronice, 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. Aceste informaţii, care pot fi 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;

d) să păstreze toată informaţia cu privire la certificatul cheii publice ataşat semnăturilor electronice avansate calificate cel puţin 15 ani de la data revocării sau expirării certificatului, în eventualitatea unor litigii.

Articolul 29. Cererea de certificare a cheii publice

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

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

a) numele şi prenumele solicitantului şi numărul actului de identitate;

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

Articolul 30. Examinarea cererii de certificare a cheii publice

(1) Cererea de certificare a cheii publice este examinată de către prestatorul de servicii de certificare în termen de 3 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 certificare creează şi eliberează certificatul cheii publice.

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

a) încălcării prevederilor prezentei legi;

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 31. Certificatul cheii publice

(1) La crearea certificatului cheii publice, prestatorul de servicii de certificare 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 certificare 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 al semnăturii electronice;

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 certificare acreditat şi trebuie să conţină, suplimentar:

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

b) informaţia, atunci cînd este cazul, privind o calitate specială a semnatarului, în funcţie de utilizarea pe care urmează să o aibă certificatul;

c) datele de verificare a semnăturii electronice care corespund datelor de creare a semnăturii electronice controlate de semnatar.

(4) Date de identificare ale titularului, în cazul certificatului cheii publice al utilizatorului, se consideră numele, prenumele şi numărul de identificare a persoanei fizice (IDNP) şi/sau

pseudonimul, dacă există, iar în cazul certificatului cheii publice al prestatorului de servicii de certificare – denumirea prestatorului şi numărul de identificare a persoanei juridice (IDNO).

(5) În cazul semnăturii electronice simple şi al semnăturii electronice avansate necalificate, structura certificatului cheii publice se stabileşte de către prestatorul de servicii de certificare, în conformitate cu prevederile prezentei legi. În cazul semnăturii electronice avansate calificate, structura certificatului cheii publice se stabileşte de către organul competent, în conformitate cu prevederile prezentei legi.

(6) Certificatul cheii publice se semnează cu semnătura electronică a prestatorului de servicii de certificare corespunzătoare tipului certificatului solicitat.

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

(8) Prestatorul de servicii de certificare, 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.

(9) La cererea titularului certificatului cheii publice, prestatorul de servicii de certificare poate indica în certificatul cheii publice şi alte informaţii decît 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.

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

Articolul 32. Termenul de valabilitate şi termenul de păstrare a certificatului cheii publice

(1) Termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de certificare de nivel superior constituie 20 de ani, termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de certificare de nivelul II constituie 10 ani, termenul de valabilitate a certificatului cheii publice al utilizatorului se stabileşte de către prestatorul de servicii de certificare, dar nu poate constitui mai mult de un an.

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

Articolul 33. Suspendarea şi revocarea certificatului cheii publice

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

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

a) la cererea titularului certificatului cheii publice;

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

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

d) 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;

e) la modificarea certificatului cheii publice;

f) în cazul decesului titularului certificatului cheii publice sau la recunoaşterea lui ca fiind incapabil;

g) la solicitarea organului competent, în cazul încălcării prezentei legi.

(3) În cazul în care prestatorul de servicii de certificare 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 certificare este obligat să înştiinţeze titularul certificatului cheii publice despre motivele revocării certificatului acestuia.

Articolul 34. Obligaţiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

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

b) să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă are motive să presupună că este încălcată confidenţialitatea cheii private;

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

– a pierdut cheia privată;

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

– informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

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

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

Articolul 35. Registrul certificatelor cheilor publice

(1) Prestatorul de servicii de certificare 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 semnăturii electronice.

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

Capitolul V
MONITORIZARE ŞI CONTROL

Articolul 36. Atribuţiile autorităţilor publice în domeniul aplicării semnăturii electronice

(1) Organul competent responsabil de elaborarea şi promovarea politicii de stat şi de exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice este Serviciul de Informaţii şi Securitate, care exercită următoarele atribuţii:

a) efectuează acreditarea, inclusiv voluntară, a prestatorilor de servicii de certificare;

b) exercită funcţia prestatorului de servicii de certificare de nivel superior pentru prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice avansate calificate;

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

d) elaborează şi aprobă, prin acte normative, cerinţele în domeniul aplicării tuturor tipurilor de semnături electronice;

e) monitorizează şi controlează respectarea cerinţelor la prestarea serviciilor de certificare în domeniul aplicării tuturor tipurilor de semnături electronice;

f) participă la elaborarea şi aprobarea reglementărilor tehnice şi a standardelor în domeniul semnăturii electronice;

g) acordă, la solicitare, asistenţă metodică şi practică la aplicarea mecanismelor semnăturii electronice;

h) realizează colaborarea internaţională în domeniul semnăturii electronice.

(2) Guvernul stabileşte autoritatea sau instituţia publică responsabilă de prestarea serviciului de sursă unică de sincronizare cu Timpul Mondial Coordonat (UTC).

Articolul 37. Controlul în domeniul aplicării semnăturii electronice

(1) Organul competent controlează respectarea cerinţelor stabilite de prezenta lege la prestarea serviciilor de certificare de către prestatorii acreditaţi şi la acordarea sau prelungirea acreditării.

(2) Controlul se efectuează de către comisia de control în domeniul semnăturii electronice (în continuare – Comisia) în baza regulamentului aprobat de organul competent.

(3) Comisia se creează în cadrul organului competent 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 hîrtie şi în format electronic, necesare pentru desfăşurarea lucrărilor ce ţin de prestarea serviciilor de certificare, precum şi la sistemele de distribuţie de aplicaţii soft, la aplicaţiile soft şi mijloacele tehnice instalate;

b) să obţină informaţii complete despre condiţiile şi modul de exploatare a mijloacelor tehnice şi de program;

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

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

(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 principii:

a) legalitatea şi respectarea competenţei stabilite de lege;

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

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

d) efectuarea controlului pe cheltuiala statului;

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

f) dreptul prestatorului de servicii de certificare de a contesta acţiunile organului competent, inclusiv în instanţa judecătorească.

(8) Controalele planificate privind respectarea de către prestatorul de servicii de certificare a obligaţiilor prevăzute de prezenta lege se efectuează de către organul competent 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 competent şi aprobate în modul stabilit, se coordonează, în privinţa termenelor de efectuare, cu conducerea prestatorului de servicii de certificare, cu cel puţin 5 zile lucrătoare înainte de începerea acestor controale.

(10) Controalele inopinate se efectuează la decizia organului competent, numai în temeiul:

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

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

(11) Prestatorul de servicii de certificare 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 competent în baza unei decizii motivate, adusă la cunoştinţa prestatorului de servicii de certificare supus controlului, care poate fi contestată de către prestatorul de servicii de certificare.

(15) La efectuarea controlului privind respectarea obligaţiilor prevăzute de prezenta lege, prestatorul de servicii de certificare 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/înmînează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de certificare, iar al doilea se păstrează la organul competent. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de certificare, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexînd documentele de rigoare.

(17) În cazul în care se depistează încălcări ale obligaţiilor prevăzute de prezenta lege, organul competent 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 minim stabilit de organul competent pentru lichidarea încălcărilor depistate constituie 10 zile lucrătoare, iar cel maxim – 30 de zile lucrătoare după primirea prescripţiei expediate/înmînate împreună cu actul de control.

(19) În cazuri excepţionale şi la solicitarea oficială a prestatorului de servicii de certificare, termenul pentru lichidarea încălcărilor poate fi prelungit cu cel mult 20 de zile lucrătoare.

(20) Prestatorul de servicii de certificare acreditat care a primit prescripţia privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripţie, să comunice organului competent informaţia privind lichidarea încălcărilor.

(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de certificare acreditat, în cazul încălcării obligaţiilor prevăzute de prezenta lege, precum şi în cazul neînlăturării, în termenul stabilit, a datelor eronate din certificatele cheilor publice, organul competent poate aplica măsuri de suspendare sau retragere a acreditării prestatorului de servicii de certificare în conformitate cu prezenta lege.

(22) Informaţiile despre rezultatele efectuării controlului se publică de către organul competent pe pagina sa web oficială.

(23) Prestatorul de servicii de certificare are dreptul să depună la organul competent reclamaţii în scris privind încălcările prevederilor prezentei legi admise de Comisie sau să conteste acţiunile acesteia în instanţa judecătorească.

Articolul 38. Suspendarea şi reluarea valabilităţii acreditării

(1) Acreditarea poate fi 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 certificare privind suspendarea acreditării;

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

c) nevalabilitatea garanţiei bancare sau a poliţei de asigurare pentru prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, prevăzută la art.26 alin.(2) lit.a);

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

(3) Decizia privind suspendarea acreditării se aduce la cunoştinţă prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăşi 2 luni, dacă actele normative în domeniul semnăturii electronice nu prevăd altfel.

(4) Prestatorul de servicii de certificare este obligat să înştiinţeze în scris organul competent despre înlăturarea circumstanţelor care au dus la suspendarea acreditării.

(5) Decizia privind reluarea valabilităţii acreditării se adoptă de către organul competent în temeiul hotărîrii instanţei de judecată care a emis hotărîrea de suspendare a acreditării, în termen de 3 zile lucrătoare de la data primirii înştiinţării. Decizia se aduce la cunoştinţă prestatorului de servicii de certificare 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 39. Retragerea acreditării

(1) Acreditarea poate fi 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 certificare privind încetarea activităţii, depusă cu 30 de zile calendaristice înainte de încetarea planificată;

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

c) depistarea unor date neautentice în documentele prezentate organului competent;

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

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

f) 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 certificare nu mai tîrziu de ziua lucrătoare imediat următoare zilei adoptării deciziei.

(4) Toate certificatele cheilor publice emise de către prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate care şi-a încetat activitatea se revocă şi se transmit spre păstrare altui prestator de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, în modul stabilit de organul competent, pe cheltuiala prestatorului de servicii de certificare care îşi încetează activitatea.

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

Capitolul VI
RĂSPUNDEREA

Articolul 40. 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) Pentru acces ilegal la informaţia cuprinsă în documentele electronice, persoanele poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

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

Articolul 41. Răspunderea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

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

(3) Prestatorul de servicii de certificare nu poartă răspundere civilă pentru prejudiciul cauzat urmare a utilizării certificatului cheii publice cu încălcarea restricţiilor de utilizare a acestuia sau a restricţiilor privind limitele valorii operaţiunilor în care acesta poate fi utilizat.

Articolul 42. Răspunderea titularului certificatului cheii publice

(1) Titularul certificatului cheii publice poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

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

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

b) semnarea documentelor electronice cu utilizarea cheii private, inclusiv în perioada de la solicitarea suspendării valabilităţii sau revocării certificatului cheii publice pînă 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 VII
PROTECŢIA DATELOR CU CARACTER PERSONAL

Articolul 43. Protecţia datelor cu caracter personal

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

(2) Datele cu caracter personal se colectează de către prestatorul de servicii de certificare numai cu acordul prealabil al persoanei care solicită certificatul şi numai în măsura în care acestea sînt necesare pentru eliberarea şi menţinerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimţămîntul expres al persoanei interesate.

Capitolul VIII
DISPOZIŢII FINALE

Articolul 44. Dispoziţii finale

(1) Prezenta lege intră în vigoare la 6 luni de la data publicării.

(2) La data intrării în vigoare a prezentei legi se abrogă Legea nr.264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr.132-137, art.710).

(3) Prevederile art.5 alin.(1) în partea ce ţine de procedurile judiciare intră în vigoare la 1 ianuarie 2016.

(4) Guvernul, în termen de 12 luni de la data publicării prezentei legi:

a) va prezenta propuneri 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.

(5) Certificatele cheilor publice eliberate în baza Legii nr.264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală rămîn valabile pînă la expirarea termenului de valabilitate a acestora.

(6) În termen de 18 luni de la data publicării prezentei legi, centrele de certificare a cheilor publice instituite în baza Legii nr.264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală sînt obligate să treacă procedura de acreditare în conformitate cu prevederile prezentei legi.

PREŞEDINTELE PARLAMENTULUI **Igor CORMAN**

Chişinău, 29 mai 2014.
Nr.91.