

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. _____
din „__” _____ 2020
Chişinău

**Privind aprobarea proiectului de lege privind identificarea electronică şi
serviciile electronice de încredere**

Guvernul **HOTĂRĂŞTE:**

Se aprobă şi se prezintă Parlamentului proiectul de lege privind identificarea electronică şi serviciile electronice de încredere

Prim-ministru

Contrasemnează:

PARLAMENTUL REPUBLICII MOLDOVA

L E G E

privind identificarea electronică și serviciile electronice de încredere

Parlamentul adoptă prezenta lege organică.

Prezenta lege transpune prevederile Regulamentului (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.

Capitolul I

DISPOZIȚII GENERALE

Articolul 1. Scopul legii și domeniul de aplicare

(1) Prezenta lege stabilește cadrul juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unei pagini web.

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

(3) Prezenta lege nu aduce atingere prevederilor legislației privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma.

Articolul 2. Noțiuni principale

(1) În sensul prezentei legi, următoarele noțiuni semnifică:

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

certificat al cheii publice – document electronic ce conține cheia publică, este semnat cu semnătura electronică sau sigilat cu sigiliul electronic al prestatorului de servicii de încredere, atestă apartenența cheii respective titularului de certificat al cheii publice și permite identificarea acestui titular;

certificat calificat al cheii publice – certificat al cheii publice care întrunește cerințele prevăzute la art. 11 și este eliberat de un prestator de servicii de încredere ce întrunește cerințele prevăzute la art. 6;

certificat pentru sigiliul electronic – document electronic ce conține cheia

publică, este semnat cu semnătura electronică sau sigilat cu sigiliul electronic al prestatorului de servicii de încredere, atestă apartenența datelor de validare a sigiliului electronic persoanei juridice și care confirmă numele persoanei respective;

certificat calificat pentru semnături sau sigilii electronice – înseamnă un certificat pentru o semnătură electronică sau un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în art. 24;

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

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

certificat calificat pentru autentificarea unei pagini web – certificat pentru autentificarea unei pagini web care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în art. 33;

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

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

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

dispozitiv de creare a semnăturii electronice sau a sigiliului electronic – mijloace tehnice și/sau de program configurate, utilizate pentru a crea o semnătură sau un sigiliu electronic;

dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate – dispozitiv de creare a semnăturii electronice sau a sigiliului electronic care îndeplinește cerințele prevăzute în art. 26;

document electronic – orice conținut în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;

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

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

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

mijloace de identificare electronică – produsul tehnic și/sau de program care conține date de identificare personală și care este folosită în scopul autentificării în

cadrul unui serviciu online;

marcă temporală electronică – atribut al documentului electronic care certifică faptul că informația a existat la un moment de timp determinat, cu păstrarea autenticității și integrității documentului electronic;

marcă temporală electronică calificată – reprezintă o marcă temporală electronică care îndeplinește cerințele prevăzute la art. 30;

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

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

produs asociat - mijloc tehnic sau de program ori componente specifice ale acestora, destinate a fi utilizate de către un prestator de servicii de încredere la prestarea serviciilor de încredere sau destinate a fi utilizate pentru crearea ori verificarea semnăturilor sau sigiliilor electronice;

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

semnatar – persoana fizică sau persoană fizică care reprezintă o persoană juridică, care creează o semnătură electronică;

serviciu de încredere – serviciu electronic prestat în schimbul unei remunerații, care constă în:

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

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

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

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

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

sigiliu electronic avansat - sigiliu electronic care îndeplinește cerințele prevăzute la art. 22;

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

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

serviciu de distribuție electronică înregistrată calificat - înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 32;

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

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

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

Articolul 3. Recunoașterea reciprocă

(1) Recunoașterea serviciilor electronice de încredere și a documentului electronic în afara 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 acreditat cu domiciliul sau cu sediul în Republica Moldova garantează recunoașterea certificatului;

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

(3) Serviciile electronice 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 unui stat străin.

Capitolul II

IDENTIFICAREA ELECTRONICĂ ȘI SERVICII DE ÎNCREDERE

Secțiunea 1

Identificarea electronică

Articolul 4. Identificarea persoanelor în cadrul sistemelor informaționale

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

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

Secțiunea a 2-a

Servicii de încredere

Articolul 5. Prestatorul de servicii de încredere

(1) Prestatorii de servicii de încredere necalificați beneficiază de dreptul de a trece procedura de acreditare. Prestatorii de servicii de încredere calificați se supun acreditării obligatorii în conformitate cu prevederile prezentei legi.

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

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

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

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

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

Articolul 6. Acreditarea prestatorului de servicii de încredere

(1) 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.

(2) Modul de solicitare, acordare, suspendare și retragere a certificatului de acreditare a prestatorului de servicii de încredere 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.

(3) Acreditarea în domeniul prestării serviciilor electronice de încredere calificate se acordă prestatorului de servicii de încredere, care întrunește următoarele cerințe:

a) dispune de resurse financiare (garanție bancară sau poliță de asigurare) în valoare de cel puțin 300 de mii de lei pentru recuperarea unor eventuale prejudicii aduse terților din cauza încrederii acestora în datele conținute în certificatul cheii publice eliberat de către prestatorul de servicii de încredere sau în informația din registrul certificatelor eliberate de către prestatorul de servicii de încredere;

b) dispune, pentru prestarea serviciilor de încredere, de personal cu studii superioare în domeniul tehnologiei informației și/sau al securității informaționale, cu nivel corespunzător de competențe și experiență de gestionare și expertizare în domeniul tehnologiei serviciilor electronice de încredere;

c) asigură securitatea, fiabilitatea și continuitatea activității de prestare a serviciilor de încredere;

d) asigură înregistrarea informației în registrul certificatelor cheilor publice, în special prestează operativ serviciul de suspendare a valabilității certificatului cheii publice și de revocare a acestuia;

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

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

g) utilizează sisteme și produse care sînt protejate împotriva modificărilor și garantează siguranța tehnică și criptografică a funcțiilor pe care și le asumă;

h) creează condiții de evitare a falsificării certificatelor și, în cazul în care prestatorul de servicii de încredere generează cheia privată și cheia publică, garantează confidențialitatea în procesul de generare a acestor;

i) utilizează sisteme care nu stochează sau nu copiază datele de creare a semnăturii electronice sau a sigiliului electronic ale persoanelor pentru care prestatorul de servicii de încredere 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 și modifica date;
- autenticitatea informației să poată fi controlată;
- certificatele să fie disponibile publicului pentru informare;
- toate modificările tehnice care compromit cerințele de siguranță să fie vizibile pentru operator.

(4) Prestatorii de servicii de încredere calificați prezintă, pe suport de hîrtie, în format electronic sau prin intermediul ghișeului unic de solicitare a actelor permissive, cererea de acreditare cu anexarea documentelor care confirmă întrunirea cerințelor specificate la alin.(2) și, în special, atestă:

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

b) existența unei reglementări interne privind asigurarea activității prestatorului de servicii de încredere în conformitate cu prevederile prezentei legi;

c) corespunderea sistemelor și a produselor utilizate cu cerințele prezentei legi;

d) studiile și calificările persoanelor cu funcții de răspundere, ale căror obligații funcționale țin nemijlocit de prestarea serviciilor de încredere;

e) numirea persoanelor responsabile de activitatea prestatorului de servicii de încredere și a persoanelor împuternicite să certifice cheile publice, precum și identitatea acestora;

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

g) dreptul de import, export, proiectare, producere și comercializare a mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației, precum

și dreptul de prestare a serviciilor în domeniul protecției criptografice și tehnice a informației, cu excepția activității desfășurate de autoritățile publice investite cu acest drept prin lege (licența).

(5) Documentele menționate la alin. (3) lit. a) se prezintă în original. Documentele menționate la alin. (3) lit. b)-g) se prezintă în original, însoțite de câte o copie, originalul fiind restituit după verificarea copiei la momentul prezentării.

(6) La depunerea cererii de acreditare, prestatorul de servicii de încredere necalificat este obligat să prezinte, în formatul stabilit de organul de supraveghere și control, informațiile referitoare la procedurile de securitate și de certificare utilizate, precum și datele sale de identificare.

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

(8) În cazul adoptării deciziei de acreditare, organul de supraveghere și control, în termen de 10 zile calendaristice din momentul luării deciziei, notifică prestatorul de servicii de încredere despre decizia luată și eliberează acestuia certificatul de acreditare de modelul stabilit și, în conformitate cu actele normative în domeniul serviciilor electronice de încredere, înregistrează prestatorul acreditat în Registrul de evidență a prestatorilor de servicii de încredere.

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

(10) Drept temei pentru refuzul de acreditare servește necorespunderea prestatorului de servicii de încredere cerințelor specificate la alin. (3) sau prezentarea informației neveridice în documentele ce se anexează la cererea de acreditare.

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

(12) Decizia privind refuzul de acreditare poate fi contestată în instanța de judecată în modul stabilit.

(13) Prestatorul de servicii de încredere se consideră acreditat din ziua emiterii certificatului de acreditare.

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

(15) Informația despre prestatorii de servicii de încredere acreditați, precum și despre cei cu acreditarea retrasă se publică de către organul de supraveghere și control pe pagina sa web oficială.

(16) După primirea certificatului de acreditare pentru prestarea serviciilor de încredere calificate, cheia publică a prestatorului de servicii de încredere este certificată

de către prestatorul de servicii de încredere de nivel superior, în conformitate cu regulamentul aprobat de organul de supraveghere și control.

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

(18) După expirarea termenului de acreditare și în lipsa unei notificări scrise din partea organului de supraveghere și control, acreditarea se consideră prelungită pentru același termen.

(19) Prestatorii de servicii de încredere necalificați acreditați sînt obligați să comunice organului de supraveghere și control, cu cel puțin 10 zile calendaristice înainte, orice intenție de modificare a procedurilor de securitate și de certificare, cu precizarea datei și orei la care modificarea intră în vigoare, precum și să confirme, în decurs de 24 de ore, modificarea efectuată.

(20) În cazurile de urgență în care securitatea serviciilor de încredere este afectată, prestatorii de servicii de încredere necalificate acreditați pot efectua modificări ale procedurilor de securitate și de certificare, urmînd să comunice, în termen de 24 de ore, organului de supraveghere și control modificările efectuate și justificarea deciziei luate.

(21) Prestatorii de servicii de încredere acreditați sunt obligați, pe parcursul întregului termen de acreditare, să asigure respectarea cerințelor în conformitate cu care a fost acreditat. În cazul apariției circumstanțelor care fac imposibilă asigurarea respectării acestor cerințe, prestatorul de servicii de încredere urmează să notifice organul de supraveghere și control despre acest fapt în decurs de 24 de ore.

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

Articolul 7. Activitatea prestatorului de servicii de încredere

(1) Prestatorul de servicii de încredere:

- a) creează și eliberează certificatele cheilor publice;
- b) suspendă și revocă certificatele cheilor publice, restabilește valabilitatea certificatelor suspendate;
- c) ține registrul certificatelor cheilor publice, asigură actualizarea acestuia și accesul public la registru; și/sau
- 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 8. 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 în cauză;

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;

d) să asigure accesul la registrul certificatelor cheilor publice, cu respectarea prevederilor art. 51;

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

f) să acopere prejudiciile aduse oricărei entități sau persoane fizice, care se încrede 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;

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

j) să îndeplinească alte obligații stabilite de legislația în vigoare.

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

a) să certifice, în modul stabilit de legislație, cheia publică a prestatorului de servicii de încredere calificat acreditat, destinată certificării cheilor publice;

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

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

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

– numai persoanele autorizate să poată introduce și/sau modifica datele stocate;

– autenticitatea datelor să poată fi controlată;

d) să verifice, prin mijloace corespunzătoare și în conformitate cu legislația în vigoare, 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:

- de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau
- 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;
- prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat;
- e) să ia măsuri adecvate împotriva falsificării și furtului de date;
- f) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art.11, 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;
- g) înainte să stabilească o relație contractuală cu o persoană care solicită un certificat în sprijinul serviciului său de încredere, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele 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 pe cale electronică, trebuie comunicate în scris, într-un limbaj accesibil. Elementele pertinente ale informațiilor trebuie puse, de asemenea, la cerere, la dispoziția părților terțe care beneficiază de certificat;
- h) să înregistreze și mențină accesibile pentru o perioadă de 15 ani, inclusiv ulterior încetării activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către prestatorul de servicii de încredere calificat, în special în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic.

Articolul 9. Cererea de certificare a cheii publice

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

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

- a) datele de identificare a solicitantului;
- b) alte date a solicitantului, în funcție de scopul pentru care se eliberează certificatul cheii publice, precum și informațiile necesare pentru comunicarea cu acesta.

Articolul 10. 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 de certificare a cheii publice se adoptă de către prestatorul de servicii de încredere în cazul:

- a) încălcării prevederilor prezentei legi;
- b) încălcării drepturilor unor terți în procesul de întocmire sau de depunere a cererii de certificare;
- c) prezentării în cererea de certificare a unor informații ce nu corespund realității.

(4) Decizia privind refuzul de certificare a cheii publice poate fi contestată în instanța 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 11. 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 acreditat și trebuie să conțină, suplimentar:

- a) mențiunea care să indice că certificatul este eliberat ca certificat calificat al cheii publice;
- b) informația, atunci când este cazul, privind o calitate specială a titularului, în funcție de utilizarea pe care urmează să o aibă certificatul;

c) datele de verificare a serviciului de încredere care corespund datelor de creare a serviciului de încredere controlate de titularul certificatului cheii publice.

(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) Certificatul cheii publice se semnează sau sigilează cu semnătura sau cu 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 și este autentificat cu ștampila prestatorului de servicii de încredere. Un exemplar al certificatului cheii publice se transmite titularului, iar celălalt se păstrează la prestatorul de servicii de încredere.

(7) Prestatorul de servicii de încredere, de comun acord cu titularul certificatului cheii publice, poate indica în certificatul cheii publice cazurile în care certificatul respectiv va putea fi utilizat, precum și unele restricții 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 acestea nu contravin legislației și nu pun în pericol securitatea națională sau ordinea publică, și numai după o prealabilă verificare a exactității informațiilor în cauză.

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

Articolul 12. 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 păstrată și utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea al altei persoane.

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

Articolul 13. 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 constituie 20 de ani, termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de încredere de nivelul II constituie 10 ani, termenul de valabilitate a certificatului cheii publice al utilizatorului se stabilește de către prestatorul de servicii de încredere, dar nu poate constitui mai mult 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.

Articolul 14. Suspendarea și revocarea certificatului cheii publice

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

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

- a) la cererea titularului certificatului cheii publice;
- b) la cererea conducătorului persoanei juridice în care activează titularul certificatului cheii publice, în cazul certificatelor eliberate pentru exercitarea atribuțiilor funcționale;
- 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 certificatului cheii publice;
- g) în cazul decesului titularului certificatului cheii publice sau al instituirii unei măsuri de ocrotire judiciară (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 ce impun revocarea certificatului cheii publice, acesta este obligat, în termen de 3 ore de lucru, să facă 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.

Articolul 15. Obligațiile titularului certificatului cheii publice

(1) Titularul certificatului cheii publice este obligat:

- a) să asigure condițiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;
- b) să nu utilizeze cheia privată pentru serviciile de încredere dacă are motive să presupună că este încălcată confidențialitatea cheii private;
- c) să solicite imediat suspendarea valabilității certificatului cheii publice sau revocarea acestuia în cazul în care:
 - a pierdut cheia privată;
 - are motive să creadă că a fost încălcată confidențialitatea cheii private;
 - informațiile cuprinse în certificatul cheii publice nu corespund realității;
- d) să înștiințeze, în decurs de 24 de ore, prestatorul de servicii de încredere despre orice modificare a informațiilor cuprinse în certificatul cheii publice;
- e) să îndeplinească alte obligații prevăzute de prezenta lege și de acordul încheiat cu prestatorul de servicii de încredere.

Articolul 16. Registrul certificatelor cheilor publice

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

(2) Registrul certificatelor cheilor publice va 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 vederea verificării autenticității serviciilor de încredere, prestatorul de servicii de încredere este obligat să asigure accesul la registrul certificatelor cheilor publice, inclusiv în regimul timpului real.

Secțiunea a 3-a

Semnătura electronică și sigiliul electronic

Articolul 17. Principiile de utilizare a semnăturii electronice și sigiliului electronic

Principiile de utilizare a semnăturii electronice și sigiliului electronic sînt:

- a) libertatea alegerii și utilizării oricărui tip de semnătură electronică sau sigiliului electronic, dacă actele normative sau acordul părților nu prevăd cerința de utilizare a unui tip concret de semnătură electronică sau sigiliului electronice, în corespundere cu obiectivele de utilizare a acestuia;
- b) posibilitatea alegerii oricăror tehnologii și/sau mijloace tehnice care permit utilizarea tipurilor concrete de semnături electronice sau sigiliului electronic în conformitate cu prevederile prezentei legi;

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice sau sigiliului electronic și/sau a documentului electronic semnat sau sigilat prin intermediul acestor doar în baza faptului că semnătura electronică sau sigiliul electronic a fost creat prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic și/sau al produsului asociat .

Articolul 18. Tipuri de semnături electronice și sigilii electronice

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

- a) simplă;
- b) avansată;
- c) calificată.

(2) Semnătura electronică simplă și sigiliul electronic simplu sunt semnăturile și sigiliile electronice care se utilizează ca metodă de autentificare, fără a face trimitere exclusiv la semnatar.

Articolul 19. Regimul juridic de utilizare a semnăturii electronice și sigiliului electronic

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

- a) se prezintă în formă electronică; sau
- b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau
- c) nu se bazează pe un certificat calificat al cheii publice; sau
- d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic.

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

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

(4) Modalitatea în care se asigură gradul de protecție a semnăturii electronice calificate pentru echivalarea acestora cu semnătura olografă aplicată pe hîrtie se stabilește de organul de supraveghere și control, conform atribuțiilor prevăzute la art. 34 alin.(2).

(5) Modalitatea de aplicare a semnăturilor electronice de către funcționarii persoanelor juridice de drept public se stabilește de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanții acestora.

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

Articolul 20. Utilizarea semnăturii sau sigiliului electronic simplu

(1) Documentul electronic se consideră semnat cu semnătura electronică simplă sau sigilat cu sigiliu electronic simplu dacă este întrunită una dintre următoarele condiții:

a) semnătura sau sigiliul electronic simplu se conține nemijlocit în documentul electronic sau este logic asociat cu documentul electronic;

b) datele de creare a semnăturii sau sigiliului electronic simplu se aplică în corespundere cu regulile stabilite de către operatorul sistemului informatic prin intermediul căruia se efectuează crearea și/sau expedierea documentului electronic și în documentul electronic se conține informația care identifică persoana în numele căreia a fost creat și expedit documentul electronic.

(2) Actele normative și/sau acordul părților, care stabilesc cazurile de recunoaștere a documentelor electronice semnate cu semnătura electronică simplă sau sigilate cu sigiliul electronic simplu, echivalente documentelor pe suport de hârtie semnate cu semnătura olografă, trebuie să prevadă următoarele:

a) modalitatea de identificare a persoanei în numele căreia este semnat sau sigilat documentul electronic în baza semnăturii sau sigiliului electronic simplu a acesteia;

b) obligația persoanei care creează și/sau utilizează date de creare a semnăturii sau sigiliului electronic simplu de a asigura confidențialitatea acestora.

Articolul 21. Limitele utilizării unor tipuri de semnături sau sigilii electronice

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

a) semnarea documentelor electronice ce conțin informație atribuită la secretul de stat;

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

(2) Nu se admite utilizarea sigiliului electronic pentru sigilarea documentelor electronice ce conțin informație atribuită la secretul de stat.

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

Articolul 22. Cerințele pentru semnăturile și sigiliile electronice avansate

Semnătura electronică sau sigiliul electronic avansat îndeplinește cumulativ următoarele cerințe:

- a) face trimitere exclusiv la titular;
- b) permite identificarea titularului;
- c) este creată prin mijloace controlate exclusiv de titular;
- d) este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.

Articolul 23. Cerințele pentru semnăturile și sigiliile electronice calificate

Semnătura electronică sau sigiliul electronic calificat îndeplinește toate cerințele semnăturii electronice sau sigiliului electronic avansat și, suplimentar:

- a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de încredere acreditat;
- b) se crează prin intermediul dispozitivului securizat de creare a semnăturii electronice sau sigiliului electronic și se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice sau sigiliului electronic și/sau al produsului asociat semnăturii electronice sau sigiliului electronic, care dispun de confirmarea corespunderii cu cerințele prevăzute de prezenta lege.

Articolul 24. Cerințe pentru certificatele calificate pentru semnături sau sigilii electronice

Certificatele pentru semnături sau sigilii electronice calificate conțin:

- a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice;
- b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;
- c) datele de identificare și alte date ale semnatarului sau creatorului de sigiliu electronic;
- d) datele de validare a semnăturilor sau 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) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent;
- h) date de verificare a certificatului calificat pentru semnătura sau sigiliul electronic care corespund datelor de creare a acestora.

Articolul 25. Crearea semnăturii sau sigiliului electronic

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

(2) La crearea semnăturii și sigiliului electronic simple, părțile se bazează pe prevederile acordului încheiat.

Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice

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

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

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

d) să ofere posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura sau sigiliului electronic sau să facă referința irevocabilă la documentul dat;

e) să creeze o semnătură sau un sigiliu electronic numai după confirmarea de către semnatar sau creatorul unui sigiliu a operațiunii de creare a semnăturii sau a sigiliului electronic;

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

(2) Dispozitivele de creare a semnăturii sau sigiliului electronic avansate sau calificate nu trebuie să modifice datele care urmează a fi semnate sau sigilate, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.

Articolul 27. Verificarea autenticității semnăturii sau sigiliului electronic

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

(2) La verificarea semnăturii sau sigiliului electronic simple, părțile se bazează pe prevederile acordului încheiat, care trebuie să prevadă modalitatea de confirmare a integrității documentului electronic semnat sau sigilat.

(3) La verificarea semnăturii sau sigiliului electronic avansate și semnăturii sau sigiliului electronic calificate, dispozitivul de verificare a semnăturii sau sigiliului electronic și/sau produsul asociat trebuie:

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

b) să afișeze faptul modificării documentului electronic semnat sau sigilat electronic;

c) să facă referință la semnatar sau creator al sigiliului electronic.

(4) La verificarea semnăturii sau sigiliului electronic avansat și a semnăturii și sigiliului electronic calificate trebuie să se garanteze, cu o siguranță suficientă, că:

- a) datele de verificare a semnăturii sau sigiliului electronic corespund datelor afișate persoanei care verifică semnătura sau sigiliul electronic;
- b) semnătura sau sigiliul electronic este verificat cu certitudine, iar rezultatul verificării și identitatea semnatarului sau creatorului sigiliului sînt corect afișate;
- c) autenticitatea și valabilitatea certificatului cheii publice solicitat în momentul verificării semnăturii sau sigiliului electronic sînt verificate cu certitudine;
- d) conținutul certificatului cheii publice este redat clar;
- e) orice modificări care pot influența securitatea semnăturii sau sigiliului electronic pot fi detectate.

Articolul 28. Cerințe pentru validarea semnăturii și sigiliului electronic calificate

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

- a) certificatul care stă la baza semnăturii sau sigiliului a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 24;
- b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării sau sigilării;
- c) datele de validare a semnăturilor sau sigiliilor corespund datelor furnizate de titularul certificatului cheii publice;
- d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice;
- e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim;
- f) semnătura sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificat;
- g) integritatea datelor semnate sau sigilate nu a fost compromisă;
- h) cerințele prevăzute la articolul 22 au fost îndeplinite la momentul semnării.

Secțiunea a 4-a

Mărcile temporale electronice

Articolul 29. Efectul juridic al mărcilor temporale electronice

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

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

Articolul 30. 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 acreditat și îndeplinește următoarele cerințe:

- a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;
- b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată;
- c) este semnată utilizând o semnătură electronică calificată sau sigilată cu un sigiliu electronic calificat al prestatorului de servicii de încredere calificat.

Secțiunea a 5-a

Serviciul de distribuție electronică înregistrată

Articolul 31. Efectul juridic al unui serviciu de distribuție electronică înregistrată

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

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

Articolul 32. Cerințe pentru serviciile de distribuție electronică înregistrată calificate

Serviciile de distribuție electronică înregistrată calificate îndeplinesc următoarele cerințe:

- a) sunt prestate de către unul sau mai mulți prestatori de servicii de încredere calificați;
- b) asigură identificarea expeditorului;
- c) asigură identificarea destinatarului înainte de furnizarea datelor;
- d) trimiterea și primirea datelor este securizată printr-o semnătură electronică calificată sau un sigiliu electronic calificat al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea că datele să fie schimbate fără ca acest lucru să fie detectat;
- e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului și destinatarului datelor;
- f) data și ora trimiterii, primirii și ale oricărei modificări a datelor este indicată printr-o marcă temporală electronică calificată.

Secțiunea a 6-a

Autentificarea unei pagini web

Articolul 33. Cerințe pentru certificatele calificate pentru autentificarea unei pagini web

Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină:

- a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web;
- b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;
- c) datele de identificare și alte date ale titularului certificatului cheii publice, precum și informațiile necesare pentru comunicarea cu acesta;
- d) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează;
- e) numele domeniului (domeniilor) gestionate de titularului 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.

Capitolul IV

Supravegherea și controlul

Articolul 34. Organul de supraveghere și control

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

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

- a) este responsabil de elaborarea și promovarea politicii de stat și de exercitarea controlului în domeniul serviciilor de încredere;
- b) efectuează acreditarea, inclusiv voluntară, a 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 acreditați;
- d) asigură ținerea, actualizarea și accesul public la datele Registrului de evidență a prestatorilor de servicii de încredere;
- e) elaborează și aprobă, prin acte normative, cerințele în domeniul serviciilor de încredere;
- f) monitorizează și controlează respectarea cerințelor la prestarea serviciilor de încredere;
- g) participă la elaborarea și aprobarea reglementărilor tehnice și a standardelor în domeniul serviciilor de încredere;

h) acordă, la solicitare, asistență metodică și practică la utilizarea serviciilor de încredere;

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

j) aplică măsuri, după caz, în legătură cu prestatorii de servicii de încredere, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezenta lege;

k) cooperează cu autoritățile de protecție a datelor, în special prin informarea acestora, 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;

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

m) realizează colaborarea internațională în domeniul serviciilor de încredere.

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

Articolul 35. Controlul în domeniul serviciilor de încredere

(1) Controlul privind respectarea cerințelor stabilite de prezenta lege la prestarea serviciilor de încredere de către prestatorii acreditați și la acordarea sau prelungirea 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 – Comisia*) în baza regulamentului aprobat de organul de supraveghere și control.

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

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

(5) Comisia are dreptul:

a) să beneficieze de acces liber la materialele documentare, pe suport de hârtie și în format electronic, necesare pentru desfășurarea lucrărilor ce țin de prestarea serviciilor de încredere, precum și la sistemele de distribuție de aplicații soft, la aplicațiile soft și mijloacele tehnice instalate;

b) să obțină informații complete despre condițiile și modul de exploatare a mijloacelor tehnice și de program;

c) să obțină de la persoanele responsabile și de la personalul prestatorului de servicii de încredere informațiile privind prestarea serviciilor de încredere ce țin 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 condițiilor prevăzute de prezenta lege, Comisia va ține cont de următoarele principii:

- a) legalitatea și respectarea competenței stabilite de lege;
- b) neadmiterea aplicării sancțiunilor care nu sînt 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 a 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 începerea acestor controale.

(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 faptelor de încălcare a prezentei legi; și/sau
- b) recepționării cererilor și reclamațiilor argumentate adresate în formă scrisă organului 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 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 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 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 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 întocmește un act în 2 exemplare, unul dintre care se expediază/înmânează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de încredere, iar al doilea se păstrează la organul de supraveghere și control. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de încredere, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexînd documentele de rigoare.

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

(18) Termenul minim stabilit de organul de supraveghere și control pentru lichidarea încălcărilor depistate constituie 10 zile lucrătoare, iar cel maxim – 30 de zile lucrătoare după primirea prescripției expediate/înmânate împreună cu actul de control.

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

(20) Prestatorul de servicii de încredere acreditat care a primit prescripția privind lichidarea încălcărilor obligațiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripție, să comunice organului de supraveghere și control informația privind lichidarea încălcărilor.

(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de încredere acreditat, în cazul încălcării obligațiilor prevăzute de prezenta lege, precum și în cazul neînălăturării, în termenul stabilit, a datelor eronate din certificatele cheilor publice, organul de supraveghere și control poate aplica măsuri de suspendare sau retragere a acreditării prestatorului de servicii de încredere în conformitate cu prezenta lege.

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

(23) 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 judecătorească.

Articolul 36. Suspendarea și reluarea valabilității acreditării

(1) Acreditarea poate fi 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 privind suspendarea acreditării;

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

c) nevalabilitatea garanției bancare sau a poliței de asigurare pentru prestatorul de servicii de încredere acreditat;

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

(3) Decizia privind suspendarea acreditării se aduce la cunoștință prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăși 2 luni, dacă actele normative în domeniul serviciilor de încredere nu prevăd altfel.

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

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

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

Articolul 37. Retragera acreditării

(1) Acreditarea poate fi 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 privind încetarea activității, 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 încredere;

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

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

e) neînălțurarea, în termenul stabilit, a circumstanțelor care au dus la suspendarea acreditării;

f) nerespectarea repetată a prescripțiilor privind lichidarea încălțărilor obligațiilor stabilite de prezenta lege.

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

(4) Toate certificatele cheilor publice emise de către prestatorul de servicii de încredere calificat care 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 cheltuiala prestatorului de servicii de încredere care își încetează activitatea.

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

Articolul 38. 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 imediat, dar nu mai târziu de 24 de ore de la momentul constatării, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice în cauză încălcarea securității sau pierderea integrității fără întârzieri nejustificate.

(3) Organul de supraveghere 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 V

REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC ȘI CIRCULAȚIA ELECTRONICĂ A DOCUMENTELOR

Articolul 39. Regimul juridic de utilizare a documentului electronic

(1) Documentul electronic semnat cu semnătură electronică calificată sau sigilat cu sigiliu electronic calificat 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 avansată, sau sigilat cu sigiliu electronic simplu sau avansat, 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 părților privind aplicarea semnăturilor sau sigiliilor electronice, cu respectarea condițiilor stipulate la art. 42 alin. (1).

(3) Actele normative sau acordul părților privind aplicarea semnăturilor electronice sau sigiliilor electronice care stabilesc cazurile de recunoaștere a documentelor electronice, semnate cu semnătură electronică avansată sau sigilate cu sigiliu electronic avansat, asimilate, după efectele lor, cu documente analoage pe suport de hîrtie, semnate cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii sau sigiliului electronic, 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 hîrtie și semnat cu semnătură olografă, documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliu electronic se consideră a fi corespunzător acestei cerințe.

(5) În cazul în care, conform legislației, se cere ca documentul pe suport de hîrtie să fie autentificat cu ștampilă, documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic se consideră a fi corespunzător acestei cerințe.

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

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

(8) Documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic este echivalat, după valoarea sa probantă, cu probele scrise sau mijloacele materiale de probă. Documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic nu poate fi respins în calitate de probă pentru motivul că are o 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 semnat cu semnătura electronică sau sigilat cu sigiliul electronic sînt considerate originale și produc aceleași efecte juridice.

(11) În cazul în care o persoană creează un document electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic și un document pe suport de hîrtie, identice după conținut, ambele se consideră documente de sine stătătoare și

originale.

(12) Copia documentului electronic semnată cu semnătura electronică sau sigilată cu sigiliul electronic se consideră reprezentarea (redarea) acestuia pe suport de hârtie, într-o formă perceptibilă. Copia documentului electronic semnată cu semnătura electronică sau sigilată cu sigiliul electronic se autentifică în modul prevăzut de legislație pentru autentificarea copiilor documentelor pe suport de hârtie și conține mențiunea despre faptul că este copie a documentului electronic.

Articolul 40. Domeniile și scopul de utilizare a documentului electronic

(1) Documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic poate fi utilizat de către persoanele fizice și juridice în toate domeniile de activitate în care este posibilă utilizarea mijloacelor tehnice și de program ce permit crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea și/sau nimicirea informației în formă electronică.

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

Articolul 41. Cerințele față de documentul electronic

Documentul electronic trebuie să corespundă următoarelor cerințe principale:

- a) să fie creat, prelucrat, expedit, recepționat, păstrat, modificat și/sau nimicir cu ajutorul mijloacelor tehnice și/sau de program;
- b) să conțină, pentru confirmarea autenticității acestuia, una sau mai multe semnături sau sigilii electronice ce 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 sa repetată.

Articolul 42. Autenticitatea documentului electronic

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

- a) este semnat sau sigilat de persoana abilitată, în modul stabilit, să semneze cu semnătură olografă documentul echivalent pe suport de hârtie;
- b) este semnat sau sigilat cu semnătura sau sigiliul electronic autentic a semnatarului sau creatorului sigiliului indicat în document.

(2) Verificarea autenticității documentului electronic se efectuează prin verificarea, cu ajutorul dispozitivelor de verificare a semnăturii sau sigiliului electronic și/sau al produsului asociat, a autenticității acestei semnături sau sigiliu.

Articolul 43. 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 documentului electronic cu aplicarea semnăturii electronice sau sigiliului electronic;
- b) expedierea și recepționarea documentului electronic;
- c) verificarea autenticității documentului electronic;
- d) confirmarea recepționării documentului electronic;
- e) evidența documentelor electronice;
- f) păstrarea, modificarea și/sau nimicirea documentului electronic;
- g) crearea exemplarelor suplimentare ale documentului electronic;
- h) crearea și autentificarea copiilor documentului electronic pe suport de hârtie;
- i) aplicarea mărcii temporale.

(3) Modul de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentului electronic 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 44. 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 utilaje și mijloace tehnice și/sau de program 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 45. Crearea documentului electronic

(1) Documentul electronic conține informația ce constituie conținutul documentului electronic și semnătura sau sigiliul electronic al semnatarului sau

creatorului sigiliului electronic.

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

Articolul 46. 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-o formă ce permite păstrarea și utilizarea lui de către destinatar.

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

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

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

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

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

(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 document ca semnatar nu este semnatarul adevărat al 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 47. Momentul expedierii și recepționării documentului electronic

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

(2) Dacă semnatarul sau creatorul sigiliului și destinatarul documentului electronic nu au convenit altfel, moment al 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, la necesitate, prin aplicarea mărcii temporale pe documentul electronic respectiv.

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

Articolul 48. Evidența documentelor electronice

(1) Evidența documentelor electronice ale persoanelor fizice și/sau juridice se efectuează în conformitate cu legislația, prin ținerea registrelor electronice și/sau pe suport de hârtie.

(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 49. Păstrarea documentelor electronice

(1) Subiecții circulației electronice a documentelor sînt obligați să păstreze originalele documentelor electronice pe suport material într-o formă 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 utilizînd 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 a căror

păstrare se utilizează arhiva electronică securizată.

Articolul 50. Protecția documentului electronic

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

(2) Informația ce 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 sînt 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 ce permite stabilirea originii, apartenenței și destinației documentului electronic, precum și a datei creării, expedierii și recepționării acestuia.

Capitolul VI PROTECȚIA DATELOR CU CARACTER PERSONAL

Articolul 51. Protecția datelor cu caracter personal

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

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

Capitolul VII RĂSPUNDEREA

Articolul 52. Răspunderea persoanelor fizice și juridice care cad sub incidența prezentei legi

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

(2) Intermediarul în circulația electronică a documentelor poartă răspundere, 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 aceste acțiuni și/sau inacțiuni.

(3) Pentru acces ilegal la informația cuprinsă în documentele electronice, persoanele poartă răspundere civilă, contravențională sau penală, după caz, conform legislației.

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

Articolul 53. Răspunderea și sarcina probei

(1) Prestatorul de servicii de încredere poartă răspundere civilă, contravențională sau penală, după caz, conform legislației.

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

(3) 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.

(4) Intenția sau neglijența prestatorului de servicii de încredere calificat se prezumă, pînă la proba contrară.

(5) 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 în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează.

Articolul 54. Răspunderea titularului certificatului cheii publice

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

(2) 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 pînă la înscrierea, în termenul stabilit, a mențiunii respective în registrul certificatelor cheilor publice, cu excepția cazurilor în care titularul certificatului va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.

Capitolul VIII DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 55. Dispoziții 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.91 din 29.05.2014 privind semnătura electronică și documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr.174-177, art/710), cu modificările ulterioare.

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

a) va prezenta propuneri 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.

(4) Certificatele cheilor publice eliberate în baza Legii nr.91 din 29.05.2014 privind semnătura electronică și documentul electronic rămân valabile până la expirarea termenului de valabilitate a acestora.

(5) În termen de 18 luni de la data publicării prezentei legi, prestatorii de servicii de certificare a cheilor publice instituite în baza Legii nr.91 din 29.05.2014 privind semnătura electronică și documentul electronic sunt obligați să treacă procedura de acreditare în conformitate cu prevederile prezentei legi.

PREȘEDINTELE PARLAMENTULUI

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

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

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

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

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

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

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

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

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

Proiectul Legii a fost elaborat în vederea realizării angajamentelor asumate de Republica Moldova în cadrul Acordului de Asociere cu Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, ratificat

de Parlamentul Republicii Moldova prin Legea nr. 112 din 02.07.2014.

Proiectul urmărește realizarea armonizării legislației naționale cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Tabelul de concordanță a fost elaborat și remis împreună cu proiectul actului normativ.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

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

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

Principalele elemente noi propuse de proiect sunt:

- definirea noțiunilor noi pentru legislația națională: *serviciu de încredere, sigiliu electronic, serviciu de distribuție electronică înregistrată, certificat pentru autentificarea unei pagini web, creator al sigiliului electronic;*

- Instituirea și reglementarea serviciilor electronice de încredere noi:

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

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

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

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

emis certificatul.

- Stabilirea unui nou temei pentru revocarea certificatelor cheilor publice – *la cererea conducătorului persoanei juridice în care activează titularul certificatului cheii publice, în cazul certificatelor eliberate pentru exercitarea atribuțiilor funcționale*. Legislația în vigoare stabilește temeiul de revocare menționat doar pentru persoanele juridice de drept public (Hotărîrea Guvernului nr.1141 din 20.12.2017 pentru aprobarea Regulamentului privind modalitatea de aplicarea semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora (Monitorul Oficial nr.451-463/1269 din 29.12.2017), fapt care provoacă o delimitare nejustificată a condițiilor de revocare a certificatelor cheilor publice emise pentru persoanele juridice de drept public și cele de drept privat.

Totodată, menționăm că, la finele anului 2018, Ministerul Finanțelor a expediat spre avizare Serviciului proiectul hotărîrii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului Informațional Automatizat „Monitorizarea Electronică a Vânzărilor”, care descrie eliberarea cheilor publice pentru echipamentele de casă și de control, adică a sigiliilor electronice. Prin urmare, proiectul de lege propus, instituind sigiliul electronic, stabilește posibilitatea eliberării certificatelor cheilor publice pentru sisteme informaționale și va permite implementarea conceptului propus de Ministerul Finanțelor.

5. Fundamentarea economico-financiară

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

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

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

Totodată, proiectul prevede aducerea legislației în vigoare în concordanță cu noua lege, în termen de 12 luni de la data publicării acesteia. Printre acestea evidențiem:

- Hotărîrea Guvernului nr. 1140 din 20.12.2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.451-463/1268 din 29.12.2017);
- Hotărîrea Guvernului nr. 1141 din 20.12.2017 pentru aprobarea Regulamentului privind modalitatea de aplicarea semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora (Monitorul Oficial nr.451-463/1269 din 29.12.2017);

- Ordinul directorului Serviciului de Informații și Securitate nr. 69 din 15.07.2016 cu privire la aprobarea Normelor tehnice în domeniul semnăturii electronice avansate calificate (Monitorul Oficial nr.215-216/1201 din 19.07.2016);
- Ordinul directorului Serviciului de Informații și Securitate nr. 70 din 15.07.2016 cu privire la aprobarea unor acte normative în domeniul organizării funcționării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.215-216/1202 din 19.07.2016);
- Ordinul directorului Serviciului de Informații și Securitate nr. 25 din 17.03.2017 cu privire la aprobarea Regulamentului privind procedura de avizare a dispozitivelor de creare și/sau verificare a semnăturii electronice și a produselor asociate semnăturii electronice (Monitorul Oficial nr.322-328/1637 din 01.09.2017);
- Ordinul directorului Serviciului de Informații și Securitate nr. 29 din 16.04.2009 cu privire la aprobarea Regulamentului de soluționare a situațiilor litigioase în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.86-88/372 din 08.05.2009).

7. Avizarea și consultarea publică a proiectului

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

Alexandr ESAULENCO
Director



**Analiza impactului de Reglementare a proiectului de lege
privind identificarea electronică și serviciile electronice de încredere**

Titlul analizei impactului (poate conține titlul propunerii de act normativ):	Analiza impactului la proiectul de lege privind identificarea electronică și serviciile electronice de încredere
Data:	___ iunie 2020
Autoritatea administrației publice (autor):	Serviciul de Informații și Securitate al Republicii Moldova
Subdiviziunea:	Serviciul de Informații și Securitate al Republicii Moldova
Persoana responsabilă și datele de contact:	Serviciul de Informații și Securitate al Republicii Moldova, Tel: 022-239-402, 022-239-470

Compartimentele analizei impactului

1. Definirea problemei

a) Determinați clar și concis problema și/sau problemele care urmează să fie soluționate.

Proiectul urmează să soluționeze problema utilizării ineficiente a serviciilor de certificare a cheilor publice de către persoane. Astfel, la moment semnătura electronică este utilizată atât ca metodă de autentificare, identificare, cât și pentru semnarea diverselor acte juridice în unele persoanelor juridice, utilizatorii fiind nevoiți să semneze în numele persoanei juridice, prin aplicarea semnăturii sale personale, ne fiind posibilă aplicarea directă a unui instrument care va identifica necondiționat persoana juridică. Proiectul prevede crearea unor servicii electronice existente la moment în practica internațională, prin introducerea prevederilor privind funcționarea mărcilor temporale, serviciilor de distribuție electronică înregistrată și autentificare a unei pagini-web, și sigiliului electronic. Prin urmare, cadrul normativ actual nu permite utilizarea de către persoanele juridice a sigiliilor electronice sau utilizarea sigiliilor în cadrul echipamentelor de casă și control și în cadrul altor sisteme informaționale automatizate publice sau private, fapt care creează incomodități în activitatea acestora.

b) Descrieți problema, persoanele/entitățile afectate și cele care contribuie la apariția problemei, cu justificarea necesității schimbării situației curente și viitoare, în baza dovezilor și datelor colectate și examinate.

Odată cu dezvoltarea tehnologiilor informaționale și accesibilitatea acestora tot mai largă pentru public, serviciile electronice devin tot mai solicitate, în special cele publice. Astfel,

actualmente, în Republica Moldova există peste 70 de servicii electronice publice prestate prin intermediul Portalului serviciilor publice, și paginilor web oficiale ale instituțiilor publice (*datele obținute de pe pagina www.servicii.gov.md*). Utilizarea serviciilor electronice este posibilă datorită mijloacelor de identificare sigură a persoanelor, actualmente fiind utilizată în acest scop semnătura electronică.

La moment, semnătura electronică este utilizată, în mare parte, în raporturile dintre persoanele fizice și juridice de drept privat cu persoanele juridice de drept public, în special la depunerea declarațiilor și raporturilor fiscale, în alte cazuri fiind dată în continuare prioritate semnăturii olografe. Totodată, semnătura electronică presupune existența titularului acesteia – persoană fizică. Prin urmare, aceasta nu poate fi eliberată pentru persoane juridice sau pentru sisteme informaționale automatizate, fapt care restrânge sfera de extindere a serviciilor electronice. Or, potrivit art. 7 alin. (5) al Legii nr. 91/2014, cheia privată este păstrată și utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea al altei persoane. Aceeași problemă a fost identificată și de către Serviciul Fiscal de Stat al Republicii Moldova, la proiectarea și implementarea echipamentelor de casă și control care ar depune automatizat raporturi fiscale, nefiind posibilă la moment aplicarea unui instrument similar semnăturii electronice.

De menționat, că tehnologia infrastructurii cheilor publice permite realizarea pe baza acesteia a mai multor tipuri de servicii, menite să acopere majoritatea cererilor utilizatorilor. Astfel, există posibilitatea creării și utilizării, inclusiv de către sistemele automatizate a sigiliilor electronice, care se atribuie direct unei persoane juridice sau unui sistem informațional distinct.

Una din problemele de bază, este lipsa reglementărilor actualizate, care există la nivelul Uniunii Europene din anul 2014. În acest sens alinierea legislației naționale la cerințele europene, v-a permite ulterioara realizare a recunoașterii internaționale a semnăturilor electronice și sigiliilor electronice eliberate în Republica Moldova.

Deși numărul prestatorilor de servicii de certificare a scăzut, ca urmare a consolidării centrelor de date în sectorul public, efectuat prin Hotărârea Guvernului nr.414/2018, în prezent activând un singur prestator acreditat I.P. STISC, numărul persoanelor care solicită prestarea acestor servicii este în continuă creștere. Astfel, conform datelor prezentate de prestatori de servicii de certificare pe anul 2019, de către aceștia au fost încheiate 34976 de contracte și emise 160327 de certificate a cheilor publice, comparativ cu 23457 de contracte încheiate și 150565 de certificate emise în anul 2018, 30240 de contracte și 69745 de certificate în anul 2017, 23391 de contracte și 32361 de certificate în 2016, fapt care denotă creșterea încrederii utilizatorilor în servicii electronice și necesitatea extinderii mediului de utilizare a serviciilor de certificare. Prin urmare, situația existentă la moment afectează în mod negativ atât persoanele fizice care utilizează serviciile electronice guvernamentale, cât și persoanele juridice de drept privat, care la moment nu pot obține sigilii electronice pentru companii și certificate electronice pentru sistemele informaționale automatizate, cât

și entitățile publice care prestează servicii electronice guvernamentale, în special din domeniul fiscal.

Totodată, în cadrul programului european Eu4Digital, segmentul eSignature, de către reprezentanții SIS al RM, I.P., „STISC” și MEI al RM, se realizează acțiunile necesare implementării mecanismului de recunoaștere serviciilor de certificare între Republica Moldova și Ucraina, însă în scopul funcționării tuturor serviciilor electronice, este necesară reglementarea acestora, în conformitate cu actele normative și standardele europene.

c) Expuneți clar cauzele care au dus la apariția problemei

Apariția problemei a fost condiționată de dezvoltarea serviciilor electronice și implementarea acestora, pe de-o parte, și evoluția tehnologică și normativă internațională în domeniu, pe de altă parte. Astfel, a devenit posibilă utilizarea certificatelor cheilor publice nu doar în cadrul semnăturii electronice, dar și pentru prestarea altor servicii, cum ar fi sigiliul electronic, iar sistemele informaționale au obținut capacitatea de a le utiliza, în mod automatizat și comod pentru utilizatori. Ca urmare, Uniunea Europeană a aprobat în anul 2014 Regulamentul privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Până la moment, Republica Moldova nu a implementat Regulamentul menționat, obiectivul dat fiind trasat prin Planul național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioadă 2017-2019, aprobat prin Hotărârea Guvernului nr. 1472 din 30.12.2016. Totodată, la moment Legea nr.91/2014 privind semnătura electronică și documentul electronic a fost aprobată în baza Directivei 1999/93/CE, care este abrogată.

d) Descrieți cum a evoluat problema și cum va evolua fără o intervenție

În Republica Moldova, noțiunea de semnătura electronică (digitală) a fost introdusă prin Legea nr.264/2004 cu privire la documentul electronic și semnătura digitală, iar ulterior, în vederea creării cadrului necesar aplicării Directivei nr.1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, a fost aprobată Legea nr.91/2014 privind semnătura electronică și documentul electronic.

Utilizarea semnăturii electronice ca metodă de identificare și autentificare atât pentru persoanele fizice, cât și pentru persoanele fizice în interesul persoanelor juridice a reprezentat o soluție optimă pentru nivelul de dezvoltare tehnic și juridic al Republicii Moldova ce exista la momentul respectiv. Actualmente, cadrul normativ în domeniul semnăturii electronice nu acoperă toate cerințele utilizatorilor și nu permite aplicarea acestuia într-o scară mai largă.

Fără intervenția propusă, nu este posibilă reglementarea juridică a serviciilor electronice existente în spațiul UE și lipsă în Republica Moldova – sigiliul electronic, autentificarea unei pagini-web, deși realizarea tehnică a acestora este posibilă. Totodată, fără intervenție, va fi practic imposibilă realizarea recunoașterii bilaterale a serviciilor de certificare a cheilor publice, între Republica Moldova și alte state, în special cele din spațiul UE, fapt care va

duce inclusiv la reducerea numărului contractelor internaționale încheiate în format electronic.

e) Descrieți cadrul juridic actual aplicabil raporturilor analizate și identificați carențele prevederilor normative în vigoare, identificați documentele de politici și reglementările existente care condiționează intervenția statului

Actualmente domeniul semnăturii electronice este reglementat de Legea nr.91/2014 privind semnătura electronică și documentul electronic și alte acte normative subordonate. Reiterăm că aceasta din urmă a fost aprobată în scopul creării cadrului necesar aplicării Directivei nr.1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, care la moment este abrogată prin Regulamentul (UE) nr. 910/2014. În acest sens, Legea 91/2014 și-a îndeplinit scopul și este depășită, nefiind capabilă să răspundă cerințelor actuale, iar simpla modificare a acesteia se prezintă inutilă odată ce conform proiectului, semnătura electronică reprezintă doar o parte a serviciilor noi aferente acesteia. Neajustarea cadrului normativ intern la cerințele, standardele și practicile comunitare va duce la stagnarea dezvoltării atât a domeniului, cât și a relațiilor, inclusiv comerciale, electronice internaționale.

Intervenția statului în raporturile analizate este prevăzută de punctul 255 al Planului național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioadă 2017-2019, aprobat prin Hotărîrea Guvernului nr. 1472 din 30.12.2016 și articolul 255 din Acordul de Asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de altă parte, din 27.06.2014, ratificat prin Legea nr. 112/2014.

2. Stabilirea obiectivelor

a) Expuneți obiectivele (care trebuie să fie legate direct de problemă și cauzele acesteia, formulate cuantificat, măsurabil, fixat în timp și realist)

Prezentul proiect implică următoare obiective realizarea cărora va fi atinsă odată cu aprobarea proiectului:

1. Asigurarea posibilității realizării recunoașterii reciproce a certificatelor cheilor publice cu statele UE, ca urmare a alinierii cadrului normativ intern în domeniu la rigorile internaționale. Ca urmare a aprobării proiectului, organul de supraveghere și control (SIS al RM) va avea posibilitatea de elaborare a proiectelor privind recunoașterea bilaterală reciprocă a tuturor serviciilor electronice stabilite de Regulamentul (UE) nr. 910/2014, și nu doar pe segmentul semnăturii electronice după cum stabilește Legea 91/2014;

2. Asigurarea posibilității creării noilor servicii aferente semnăturii electronice necesare bunei funcționări a sistemelor informaționale atât din sectorul public, cât și privat, care la moment nu se regăsesc în legislația națională, cum ar fi: identificarea electronică, sigilii electronice, mărci temporale electronice, certificate de securitate pentru pagini web.

3. Identificarea opțiunilor
<p><i>a) Expuneți succint opțiunea „a nu face nimic”, care presupune lipsa de intervenție</i></p> <p>Opțiunea „a nu face nimic” presupune menținerea vidului legislativ creat, prin lipsa de reglementare a serviciilor aferente semnăturii electronice, necesare pentru dezvoltarea informațională a Republicii Moldova, inclusiv va face imposibilă realizarea recunoașterii reciproce a certificatelor cheilor publice, destinate pentru alte servicii electronice decât semnătura electronică, cu statele membre ale UE. Totodată, astfel Republica Moldova nu își va onora angajamentul asumat în cadrul Acordului de Asociere cu Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, ratificat de Parlamentul Republicii Moldova prin Legea nr. 112/2014.</p>
<p><i>b) Expuneți principalele prevederi ale proiectului, cu impact, explicând cum acestea ținesc cauzele problemei, cu indicarea noutăților și întregului spectru de soluții/drepturi/obligații ce se doresc să fie aprobate</i></p> <p>Proiectul de lege nu conține reglementări cu impact asupra bugetului public național, prevederi de reorganizare și reforme structurale sau instituționale ale autorităților sau instituțiilor publice.</p> <p>Proiectul de lege vine să reglementeze domeniul serviciilor electronice de încredere existente la moment în practica europeană, și anume semnătura electronică, sigiliul electronic, certificatele de securitate pentru pagini web, identificarea electronică și serviciul de distribuție electronică înregistrată. Proiectul stabilește organul de monitorizare și control în domeniul serviciilor electronice de încredere, drepturile și obligațiile acestuia, dar și drepturile și obligațiile prestatorilor de servicii de încredere. Totodată, proiectul stabilește cerințele pentru certificatele cheilor publice și dispozitivele de creare și verificare a semnăturilor sau sigiliilor electronice, ce corespund practicilor și standardelor Uniunii Europene.</p> <p>Nu în ultimul rând, intervenția propusă presupune instituirea și reglementarea serviciilor de încredere noi pentru Republica Moldova și anume:</p> <ol style="list-style-type: none"> 1. <i>Sigiliul electronic</i>, care permite aplicarea acestuia pe documente electronice de către persoanele juridice, fără necesitatea existenței intermediarilor (persoane fizice în interesul persoanei juridice), precum și va putea fi eliberat pentru utilizarea în cadrul sistemelor informaționale automatizate. Proiectul prevede principiile de utilizare a sigiliului electronic (art. 17, 20), tipurile de sigilii electronice ce pot fi utilizate (art. 18), stabilește regimul juridic de utilizare a acestora (art. 19), stabilește limitele de utilizare a diferitor tipuri de sigilii electronice (art. 21) și cerințele pentru acestea necesare a fi îndeplinite (art. 22, 23 și 24). Astfel, aprobarea prevederilor menționate va crea posibilitatea emiterii de către prestatori a sigiliilor electronice, iar utilizatorii le vor putea obține și utiliza în raporturile sale juridice;

2. *Identificarea electronică*, care reprezintă procesul de utilizare a datelor de identificare a persoanelor în format electronic, în scopul identificării persoanei în cadrul sistemelor informaționale;

3. *Serviciul de distribuție electronică înregistrată*, care reprezintă un serviciu ce permite transmiterea datelor între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind transmiterea și recepționarea datelor. Totodată, serviciul este menit să protejeze datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată.

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

c) Expuneți opțiunile alternative analizate sau explicați motivul de ce acestea nu au fost luate în considerare

Unica opțiune alternativă ar fi modificarea și completarea Legii nr.91/2014, însă aceasta nu a fost luată în considerație pe motiv că aceasta implică modificarea titlului și a clauzei de emitere a legii, deoarece aceasta a fost menită să creeze cadrul necesar aplicării Directivei nr.1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, publicată în Jurnalul Oficial al Comunităților Europene nr.L13 din 19 ianuarie 2000 (abrogată prin Regulamentul UE 910/2014). Totodată, va fi necesară modificarea fiecărui articol din legea menționată în vederea completării acestora cu prevederi noi care reglementează sigiliul electronic, care din punct de vedere tehnic este similar semnăturii electronice. Totodată, va fi necesară completarea legii cu servicii de încredere noi cum ar fi identificarea electronică, serviciul de distribuție electronică înregistrată, serviciul de autentificare a paginilor web, care anterior nu au fost reglementate în legislația națională, fapt care va duce la extinderea cercului de raporturi juridice reglementate, semnătura electronică ocupând doar o parte componentă din acestea. În acest sens, potrivit art. 63 alin. (1) din Legea 100/2017 cu privire la actele normative, *modificarea unui act normativ este admisă numai dacă nu afectează concepția generală ori caracterul unitar al actului respectiv. În caz contrar, actul normativ se înlocuiește cu un nou act, urmînd să fie abrogat în întregime.*

4. Analiza impacturilor opțiunilor

a) Expuneți efectele negative și pozitive ale stării actuale și evoluția acestora în viitor, care vor sta la baza calculării impacturilor opțiunii recomandate

Opțiunea I – a nu face nimic.

Efecte pozitive:

Semnătura electronică este reglementată în Republica Moldova, iar numărul de utilizatori ai acesteia este în continuă creștere.

Efecte negative:

1. Nu va fi aprobat un act care ar transpune 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, iar ca urmare, Republica Moldova nu î-și va onora angajamentul asumat în cadrul Acordului de Asociere cu Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora;

2. Republica Moldova va continua să aplice reglementări învechite de fapt și de drept, stabilite în baza reglementărilor comunitare deja abrogate;

3. Persoanele nu vor putea utiliza toate serviciile aferente semnăturii electronice, disponibile în alte țări, inclusiv statele UE;

4. Stagnarea în dezvoltarea digitală a Republicii Moldova și a serviciilor publice electronice, prin imposibilitatea eliberării certificatelor cheilor publice pentru sisteme informaționale automatizate.

Costuri.

Costuri în lipsa intervenției nu au fost identificate.

b¹) Pentru opțiunea recomandată, identificați impacturile completînd tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Opțiunea II – aprobarea proiectului de lege privind identificarea electronică și serviciile electronice de încredere.

Beneficii:

1. Asigurarea armonizării cadrului legislativ național la prevederile legislației UE;

2. Oferirea posibilității legale de prestare în Republica Moldova a tuturor serviciilor electronice aferente semnăturii electronice, existente la moment în practica internațională;

3. Dezvoltarea digitală a Republicii Moldova și a serviciilor publice electronice prestate, inclusiv prin eliberarea certificatelor cheilor publice pentru sisteme informaționale automatizate și persoane juridice;

4. Posibilitatea implementării fiscalității electronice automate, prin eliberarea certificatelor cheilor publice pentru echipamentele de casă și control, ce depun raporturi fiscale în mod automatizat;

5. Acordarea prestatorilor a posibilității de lărgire a spectrului de servicii electronice aferente semnăturii electronice prestate;

6. Posibilitatea încheierii acordurilor bilaterale în domeniu, cu statele membre ale UE în vederea recunoașterii reciproce nu doar a semnăturilor electronice ale persoanelor fizice, ci și a sigiliilor electronice ale persoanelor juridice, iar ca urmare dezvoltarea comerțului electronic transfrontalier.

Costuri.

Punerea în aplicare a legii nu va determina cheltuieli bugetare suplimentare, iar implementarea tehnică a noilor servicii electronice de încredere este posibilă în cadrul infrastructurii cheilor publice deja existente. Totodată, implementarea proiectului nu implică costuri din partea mediului privat (prestatori de servicii de certificare), acreditarea

prestatorilor fiind gratuită. Mai mult ca atât, prestatorul nu este obligat să presteze întregul spectru de servicii prevăzute de lege, având posibilitatea a selecta o parte din acestea, în dependență de capacitățile și specificul activității acestora.

Efecte negative:

În urma aprobării prezentului proiect, prestatorii care deja sunt acreditați vor fi nevoiți să solicite acreditarea repetată în condițiile noii legi pentru a continua activitate de prestare a serviciilor de certificare. Totodată, proiectul prevede un termen rezonabil de 18 luni pentru efectuarea acestei acțiuni, iar însăși procedura nu implică costuri financiare din partea prestatorilor.

b²) Pentru opțiunile alternative analizate, identificați impacturile completând tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Nu este cazul.

c) Pentru opțiunile analizate, expuneți cele mai relevante/iminente riscuri care pot duce la eșecul intervenției și/sau schimba substanțial valoarea beneficiilor și costurilor estimate și prezentați presupuneri privind gradul de conformare cu prevederile proiectului a celor vizați în acesta

Există riscul implementării în ritm lent a noilor prevederi pe motivul numărului redus de prestatori de servicii de certificare care la moment sunt acreditați, iar ca urmare, utilizatorii nu vor putea beneficia de noile servicii în scurt timp după aprobarea proiectului.

În vederea minimizării riscului, este prevăzută elaborarea proiectului hotărârii de Guvern care va stabili prestarea tuturor serviciilor de încredere de către centrul unic de certificare al Guvernului. Prin urmare, utilizatorilor le vor fi disponibile noile servicii în termen restrâns, iar prestatorii din mediul privat vor presta noile serviciile la decizia sa.

d) Dacă este cazul, pentru opțiunea recomandată expuneți costurile de conformare pentru întreprinderi, dacă există impact disproporționat care poate distorsiona concurența și ce impact are opțiunea asupra întreprinderilor mici și mijlocii. Se explică dacă sînt propuse măsuri de diminuare a acestor impacturi

Prevederile prezentului proiect de lege nu stabilește costuri suplimentare din partea prestatorilor. Mai mult ca atât, prestatorii nu sunt obligați să presteze toate serviciile electronice de încredere enumerate în proiect, fiind posibilă prestarea în continuare doar a unor servicii anumite, reieșind din specificul activității și voinței acestora.

Concluzie

e) Argumentați selectarea unei opțiuni, în baza atingerii obiectivelor, beneficiilor și costurilor, precum și a asigurării celui mai mic impact negativ asupra celor afectați

Autorii prezentei Analize optează pentru Opțiunea a II-a, care va asigura dezvoltarea digitală sigură a Republica Moldova, prin implementarea standardelor comunitare în domeniu, extinderea serviciilor electronice aferente semnăturii electronice, iar ca urmare,

oferirea pentru persoanelor a instrumentelor necesare pentru realizarea raporturilor juridice în mediul virtual. Totodată, aceasta va duce la facilitarea procedurilor de recunoaștere internațională a certificatelor cheilor publice eliberate în Republica Moldova.

5. Implementarea și monitorizarea

a) Descrieți cum va fi organizată implementarea opțiunii recomandate, ce cadru juridic necesită a fi modificat și/sau elaborat și aprobat, ce schimbări instituționale sînt necesare

Implementarea tehnică a proiectului de lege va avea loc pe baza componentelor tehnice și de program deja existente, fiind necesară ajustarea cadrului normativ subordonat legii, și anume:

- Hotărîrea Guvernului nr. 1140 din 20.12.2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.451-463/1268 din 29.12.2017);
- Hotărîrea Guvernului nr. 1141 din 20.12.2017 pentru aprobarea Regulamentului privind modalitatea de aplicarea semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora (Monitorul Oficial nr.451-463/1269 din 29.12.2017);
- Ordinul directorului Serviciului de Informații și Securitate nr. 69 din 15.07.2016 cu privire la aprobarea Normelor tehnice în domeniul semnăturii electronice avansate calificate (Monitorul Oficial nr.215-216/1201 din 19.07.2016);
- Ordinul directorului Serviciului de Informații și Securitate nr. 70 din 15.07.2016 cu privire la aprobarea unor acte normative în domeniul organizării funcționării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.215-216/1202 din 19.07.2016);
- Ordinul directorului Serviciului de Informații și Securitate nr. 25 din 17.03.2017 cu privire la aprobarea Regulamentului privind procedura de avizare a dispozitivelor de creare și/sau verificare a semnăturii electronice și a produselor asociate semnăturii electronice (Monitorul Oficial nr.322-328/1637 din 01.09.2017);
- Ordinul directorului Serviciului de Informații și Securitate nr. 29 din 16.04.2009 cu privire la aprobarea Regulamentului de soluționare a situațiilor litigioase în domeniul aplicării semnăturii electronice (Monitorul Oficial nr.86-88/372 din 08.05.2009).

Monitorizarea respectării prevederilor legii, aceasta va avea loc în baza Capitolului IV al proiectului, de către organul de supraveghere și control – Serviciul de Informații și Securitate al Republicii Moldova, prin efectuarea controalelor planificate și inopinate ale prestatorilor în condițiile legii.

b) Indicați clar indicatorii de performanță în baza cărora se va efectua monitorizarea

- Servicii electronice de încredere noi implementate și funcționale pentru cetățeni;
- Prestatori de servicii de încredere reacreditați în baza actului normativ nou aprobat;
- Acorduri internaționale de recunoaștere bilaterală a serviciilor electronice de încredere încheiate.

c) Identificați peste cât timp vor fi resimțite impacturile estimate și este necesară evaluarea performanței actului normativ propus. Explicați cum va fi monitorizată și evaluată opțiunea

Având în vedere faptul că, implementarea legii necesită modificarea unor acte normative subordonate, care se va efectua în termen de 12 luni de la data intrării în vigoare a proiectului, iar prestatorii existenți vor avea obligația de a trece procedura de acreditare în conformitate cu prevederile noii legi, impacturile estimate se vor resimți peste de 24 luni din momentul aprobării legii. Totodată, monitorizarea implementării va fi asigurată prin raportările anuale de activitate ale prestatorilor către organul de supraveghere și control, în care se va reflecta numărul utilizatorilor de servicii de încredere.

6. Consultarea

a) Identificați principalele părți (grupuri) interesate în intervenția propusă

Principalele părți interesate în promovarea prezentului proiect sunt:

1. persoanele fizice care utilizează serviciile electronice guvernamentale;
2. persoanele juridice de drept privat, care la moment nu pot obține sigilii electronice pentru companii, dar și certificate electronice pentru sistemele informaționale automatizate;
3. entitățile publice care prestează servicii electronice guvernamentale, în special din domeniul fiscal.

b) Explicați succint cum (prin ce metode) s-a asigurat consultarea adecvată a părților

Intervenția propusă a fost consultată și susținută în cadrul mai multor ședințe organizate de I.P. „Agenția de Guvernare Electronică” (ședința din 18.10.2018, 09.01.2019 și 12.02.2020), în cadrul grupului de lucru sectorial *eID* și *eSignature* din cadrul programului *EU4Digital: aducerea beneficiilor pieței digitale armonizate către țările Parteneriatului Estic* (ședința din 02.10.2019). De asemenea, intervenția a fost examinată în contextul avizării proiectului hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului Informațional Automatizat „Monitorizarea Electronică a Vânzărilor” (redacția din luna noiembrie, anul 2018) și solicitări din partea Ministerului Economiei și Infrastructurii (scrisoarea nr.08/1-8126 din 03.12.2019).

Suplimentar, proiectul de lege, nota informativă și AIR la aceasta au fost publicate pe pagina oficială a Serviciului de Informații și Securitate www.sis.md, compartimentul *Transparența*, subcompartimentul *Transparența decizională*.

c) Expuneți succint poziția fiecărei entități consultate față de documentul de analiză a impactului și/sau intervenția propusă (se expune poziția a cel puțin unui exponent din fiecare grup de interese identificat).

Atât entitățile publice consultate (I.P. Agenția de Guvernare Electronică, Ministerul Economiei și Infrastructurii), cât și prestatorii de servicii de certificare acreditați (I.P. Serviciul Tehnologia Informației și Securitate Cibernetică) și persoanele juridice de drept

(Orange Moldova SA și ÎM Moldcell SA) sau expus pozitiv asupra intervenției, înaintând unele obiecții și propuneri pe marginea proiectului, care vor fi examinate în procesul avizării acestuia.

Tabel pentru identificarea impacturilor			
Categorii de impact	Punctaj atribuit		
	<i>Opțiunea a propusă</i>	<i>Opțiunea alterativ ă 1</i>	<i>Opțiunea alterativ ă 2</i>
Economic			
costurile desfășurării afacerilor	0		
povara administrativă	0		
fluxurile comerciale și investiționale	+2		
competitivitatea afacerilor	+2		
activitatea diferitor categorii de întreprinderi mici și mijlocii	+1		
concurența pe piață	+1		
activitatea de inovare și cercetare	+3		
veniturile și cheltuielile publice	+2		
cadrul instituțional al autorităților publice	0		
alegerea, calitatea și prețurile pentru consumatori	+3		
bunăstarea gospodăriilor casnice și a cetățenilor	0		
situația social-economică în anumite regiuni	0		
situația macroeconomică	0		
alte aspecte economice	0		
Social			
gradul de ocupare a forței de muncă	0		
nivelul de salarizare	0		
condițiile și organizarea muncii	0		
sănătatea și securitatea muncii	0		
formarea profesională	0		
inegalitatea și distribuția veniturilor	0		
nivelul veniturilor populației	0		
nivelul sărăciei	0		
accesul la bunuri și servicii de bază, în special pentru persoanele social-vulnerabile	0		

diversitatea culturală și lingvistică	0		
partidele politice și organizațiile civice	0		
sănătatea publică, inclusiv mortalitatea și morbiditatea	0		
modul sănătos de viață al populației	0		
nivelul criminalității și securității publice	0		
accesul și calitatea serviciilor de protecție socială	0		
accesul și calitatea serviciilor educaționale	0		
accesul și calitatea serviciilor medicale	0		
accesul și calitatea serviciilor publice administrative	0		
nivelul și calitatea educației populației	0		
conservarea patrimoniului cultural	0		
accesul populației la resurse culturale și participarea în manifestații culturale	0		
accesul și participarea populației în activități sportive	0		
discriminarea	0		
alte aspecte sociale	0		
De mediu			
clima, inclusiv emisiile gazelor cu efect de seră și celor care afectează stratul de ozon	0		
calitatea aerului	0		
calitatea și cantitatea apei și resurselor acvatice, inclusiv a apei potabile și de alt gen	0		
biodiversitatea	0		
flora	0		
fauna	0		
peisajele naturale	0		
starea și resursele solului	0		
producerea și reciclarea deșeurilor	0		
utilizarea eficientă a resurselor regenerabile și neregenerabile	0		
consumul și producția durabilă	0		
intensitatea energetică	0		
eficiența și performanța energetică	0		
bunăstarea animalelor	0		
riscuri majore pentru mediu (incendii, explozii, accidente etc.)	0		

utilizarea terenurilor	0		
alte aspecte de mediu	0		
<p><i>Tabelul se completează cu note de la -3 la +3, în drept cu fiecare categorie de impact, pentru fiecare opțiune analizată, unde variația între -3 și -1 reprezintă impacturi negative (costuri), iar variația între 1 și 3 – impacturi pozitive (beneficii) pentru categoriile de impact analizate. Nota 0 reprezintă lipsa impacturilor. Valoarea acordată corespunde cu intensitatea impactului (1 – minor, 2 – mediu, 3 – major) față de situația din opțiunea „a nu face nimic”, în comparație cu situația din alte opțiuni și alte categorii de impact. Impacturile identificate prin acest tabel se descriu pe larg, cu argumentarea punctajului acordat, inclusiv prin date cuantificate, în compartimentul 4 din Formular, lit.b¹) și, după caz, b²), privind analiza impacturilor opțiunilor.</i></p>			
Anexe			
1. Proiectul preliminar de act normativ, pe 34 de file.			

Tabel de concordanță
La proiectul de lege privind identificarea electronică și serviciile electronice de încredere

1. Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse 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					
2. Titlul proiectului de act normativ național Legea privind identificarea electronică și serviciile electronice de încredere					
3. Gradul de compatibilitate Compatibil					
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	Legea privind identificarea electronică și serviciile electronice de încredere	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/persoana responsabilă
4	5	6	7	8	9
CAPITOLUL I DISPOZIȚII GENERALE Articolul 1. Obiect. În vederea asigurării bunei funcționări a pieței interne, vizând în același timp un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere, prezentul regulament: (a) stabilește condițiile în care statele membre recunosc mijloacele de identificare electronică a persoanelor fizice și juridice care intră sub incidența unui sistem notificat de identificare electronică al unui alt stat membru;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
(b) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice; și (c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unui site internet.	Capitolul I DISPOZIȚII GENERALE Articolul 1. Scopul legii și domeniul de aplicare (1) Prezenta lege stabilește cadrul juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unei pagini web. (2) Prezenta lege nu limitează modul de utilizare a	Compatibil			Serviciul de Informații și Securitate al Republicii Moldova (SIS al RM)

	documentelor				
Articolul 2 Domeniul de aplicare (1) Prezentul regulament se aplică sistemelor de identificare electronică care au fost notificate de către un stat membru și prestatorilor de servicii de încredere cu sediul în Uniune. (2) Prezentul regulament nu se aplică prestării de servicii de încredere care sunt utilizate exclusiv în sisteme închise care decurg din dreptul intern sau din acordurile încheiate între un set definit de participanți. (3) Prezentul regulament nu aduce atingere dreptului intern sau al Uniunii privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 3 Definiții În sensul prezentului regulament, se aplică următoarele definiții: 1. „identificare electronică” înseamnă procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;	Articolul 2. Noțiuni principale (1) În sensul prezentei legi, următoarele noțiuni semnifică: <i>identificare electronică</i> - procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;	Compatibil			SIS al RM
2. „mijloace de identificare electronică” înseamnă o unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării unui serviciu online;	<i>mijloace de identificare electronică</i> – produsul tehnic și/sau de program care conține date de identificare personală și care este folosită în scopul autentificării în cadrul unui serviciu online;	Compatibil			SIS al RM
3. „date de identificare personală” înseamnă un set de date care permit stabilirea identității unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;	<i>date de identificare personală</i> – set de date care permit stabilirea identității unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;	Compatibil			SIS al RM
4. „sistem de identificare electronică” înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice sau persoane fizice reprezentând persoane juridice;	Articolul 7. Activitatea prestatorului de servicii de încredere (1) Prestatorul de servicii de încredere: a) creează și eliberează certificatele cheilor publice; b) suspendă și revocă certificatele cheilor publice, restabilește valabilitatea certificatelor suspendate; c) ține registrul certificatelor cheilor publice, asigură actualizarea acestuia și accesul public la registru; și/sau	Compatibil			SIS al RM

	d) prestează, în bază de contract servicii de încredere.				
5.,„autentificare” înseamnă un proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii și integrității unor date în format electronic;	Articolul 2. Noțiuni principale <i>autentificare</i> – proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii și integrității unor date în format electronic;	Compatibil			SIS al RM
6.,„beneficiar” înseamnă o persoană fizică sau juridică care beneficiază de un serviciu de identificare electronică sau de un serviciu de încredere;	<i>titularul certificatului cheii publice</i> – persoana fizică sau juridică sau persoana fizică care reprezintă persoana juridică, care utilizează serviciile de încredere;	Compatibil			SIS al RM
7.,„organism din sectorul public” înseamnă un stat, o autoritate regională sau locală, un organism de drept public sau o asociație formată din una sau mai multe astfel de autorități sau din unul sau mai multe astfel de organisme de drept public; sau o entitate privată mandatată de cel puțin una dintre aceste autorități, organisme sau asociații să presteze servicii publice atunci când acționează în temeiul unui astfel de mandat;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE. Totodată, noțiunea este parțial definită în Codul administrativ al RM din 19.07.2018 Articolul 7. Autoritățile publice Autoritate publică se consideră orice structură organizatorică sau organ instituită/instituit prin lege sau printr-un alt act normativ, care acționează în regim de putere publică în scopul realizării unui interes public.		
8.,„organism de drept public” înseamnă un organism astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European și a Consiliului;	Legea nr.131/2015 privind achizițiile publice. Articolul 13. Calitatea de autoritate contractantă 2) Persoană juridică de drept public este orice entitate care întrunește cumulativ următoarele condiții: a) este constituită pentru a răspunde exclusiv unor necesități de interes general, fără caracter industrial sau comercial; b) dispune de personalitate juridică; c) activitatea acesteia este asigurată cu bani publici sau gestiunea acesteia constituie obiectul controlului din	Compatibil			

	partea autorităților publice ori a altor persoane juridice de drept public, sau consiliul ei de administrație, de conducere ori de supraveghere este format, în proporție de peste 50%, din membri numiți de către entitățile menționate.				
9. „semnatar” înseamnă o persoană fizică care creează o semnătură electronică;	Articolul 2. Noțiuni principale <i>semnatar</i> – persoana fizică sau persoană fizică care reprezintă o persoană juridică, care creează o semnătură electronică;	Compatibil			SIS al RM
10. „semnătură electronică” înseamnă date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;	<i>semnătură electronică</i> – date în formă electronică, care sunt atașate la sau logic asociate cu alte date în formă electronică și care sunt utilizate ca metodă de autentificare;	Compatibil			SIS al RM
11. „semnătură electronică avansată” înseamnă o semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26;	Articolul 22. Cerințele pentru semnăturile și sigiliile electronice avansate Semnătura electronică sau sigiliul electronic avansat îndeplinește cumulativ următoarele cerințe: a) face trimitere exclusiv la titular; b) permite identificarea titularului; c) este creată prin mijloace controlate exclusiv de titular; d) este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.	Compatibil			SIS al RM
12. „semnătură electronică calificată” înseamnă o semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificat și care se bazează pe un certificat calificat pentru semnăturile electronice;	Articolul 23. Cerințele pentru semnăturile și sigiliile electronice calificate Semnătura electronică sau sigiliul electronic calificat îndeplinește toate cerințele semnăturii electronice sau sigiliului electronic avansat și, suplimentar: a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de încredere acreditat; b) se creează prin intermediul dispozitivului securizat de creare a semnăturii electronice sau sigiliului electronic și se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice sau sigiliului electronic și/sau al produsului asociat semnăturii electronice sau sigiliului electronic, care dispun de confirmarea corespunderii cu cerințele prevăzute de prezenta lege.	Compatibil			SIS al RM

13. „date de creare a semnăturilor electronice” înseamnă date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;	Articolul 2. Noțiuni principale <i>date de creare a semnăturilor electronice sau sigiliilor electronice</i> – date unice care sunt utilizate de semnatar sau de creatorul sigiliului pentru a crea o semnătură electronică sau un sigiliu electronic;	Compatibil			SIS al RM
14. „certificat pentru semnătura electronică” înseamnă o atestare electronică care face legătura între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele sau pseudonimul persoanei respective;	<i>certificat al cheii publice</i> – document electronic ce conține cheia publică, este semnat cu semnătura electronică sau sigilat cu sigiliul electronic al prestatorului de servicii de încredere, atestă apartenența cheii respective titularului de certificat al cheii publice și permite identificarea acestui titular;	Compatibil			SIS al RM
15. „certificat calificat pentru semnătură electronică” înseamnă un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa I;	<i>certificat calificat pentru semnături sau sigilii electronice</i> – înseamnă un certificat pentru o semnătură electronică sau un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în art. 24;	Compatibil			SIS al RM
16. „serviciu de încredere” înseamnă un serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în: (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; sau (b) crearea, verificarea și validarea certificatelor pentru autentificarea unui site internet; sau (c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;	<i>serviciu de încredere</i> – serviciu electronic prestat în schimbul unei remunerații, care constă în: a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective; b) crearea, verificarea și validarea certificatelor pentru autentificarea unei pagini web; c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;	Compatibil			SIS al RM
17. „serviciu de încredere calificat” înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;	<i>serviciu de încredere calificat</i> – reprezintă un serviciu de încredere care îndeplinește cerințele aplicabile, prevăzute de prezenta lege;	Compatibil			SIS al RM
18. „organism de evaluare a conformității” înseamnă un organism definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul în cauză ca fiind competent să efectueze evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate pe care acesta le prestează;	<i>organul de supraveghere și control</i> – autoritate publică centrală stabilită de prezenta lege cu atribuții de supraveghere și control în domeniul identificării electronice și serviciilor electronice de încredere;	Compatibil			SIS al RM
19. „prestator de servicii de încredere” înseamnă o	<i>prestator de servicii de încredere</i> – întreprinzător	Compatibil			SIS al RM

persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;	individual sau persoană juridică care prestează unul sau mai multe servicii de încredere;				
20. „prestator de servicii de încredere calificat” înseamnă un prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;	Articolul 5. Prestatorul de servicii de încredere (1) Prestatorii de servicii de încredere necalificați beneficiază de dreptul de a trece procedura de acreditare. Prestatorii de servicii de încredere calificați se supun acreditării obligatorii în conformitate cu prevederile prezentei legi. (2) Prestatorii de servicii de încredere sunt organizați în mod ierarhic. În vârful ierarhiei se află prestatorul de servicii de încredere de nivel superior. (3) Prestatorii de servicii de încredere necalificați își organizează ierarhia de sine stătător. (4) Activitatea prestatorilor de servicii de încredere calificați, inclusiv ierarhia acestora, se organizează în modul stabilit de Guvern, în conformitate cu prevederile prezentei legi. (5) Evidenta prestatorilor de servicii de încredere acreditați se ține de către organul de supraveghere și control în cadrul Registrului de evidență a prestatorilor de servicii de încredere, care se actualizează permanent și la care accesul este public. (6) Introducerea în Registrul de evidență a prestatorilor de servicii de încredere se efectuează de către organul de supraveghere și control la data acreditării acestora.	Compatibil			SIS al RM
21. „produs” înseamnă hardware sau software sau componente relevante de hardware sau software, destinate să fie utilizate pentru prestarea de servicii de încredere;	<i>produs</i> – mijloc tehnic și/sau de program ori componente specifice ale acestora, destinate să fie utilizate pentru prestarea serviciilor de încredere;	Compatibil			SIS al RM
22. „dispozitiv de creare a semnăturilor electronice” înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;	<i>dispozitiv de creare a semnăturii electronice sau a sigiliului electronic</i> – mijloace tehnice și/sau de program configurate, utilizate pentru a crea o semnătură sau un sigiliu electronic;	Compatibil			SIS al RM
23. „dispozitiv de creare a semnăturilor electronice calificat” înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II;	<i>dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate</i> – dispozitiv de creare a semnăturii electronice sau a sigiliului electronic care îndeplinește cerințele prevăzute în art. 26;	Compatibil			SIS I RM
24. „creatorul unui sigiliu” înseamnă o persoană juridică care creează un sigiliu electronic;	<i>creatorul unui sigiliu</i> – persoană juridică care creează un sigiliu electronic;	Compatibil			SIS al RM

25. „sigiliu electronic” înseamnă date în format electronic atașate la sau asociate logic cu alte date în format electronic pentru asigurarea originii și integrității acestora din urmă;	<i>sigiliu electronic</i> - date în format electronic atașate la sau asociate logic cu alte date în format electronic pentru asigurarea originii și integrității acestora din urmă;	Compatibil			SIS al RM
26. „sigiliu electronic avansat” înseamnă un sigiliu electronic care îndeplinește cerințele prevăzute la articolul 36;	<i>sigiliu electronic avansat</i> - sigiliu electronic care îndeplinește cerințele prevăzute la art. 22;	Compatibil			SIS al RM
27. „sigiliu electronic calificat” înseamnă un sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat și care se bazează pe un certificat calificat pentru sigiliile electronice;	<i>sigiliu electronic calificat</i> - sigiliu electronic avansat care este creat prin intermediul dispozitivului de creare a sigiliilor electronice calificat și care se bazează pe un certificat calificat a sigiliilor electronice;	Compatibil			SIS al RM
28. „date de creare a sigiliilor electronice” înseamnă date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;	<i>date de creare a semnăturilor electronice sau sigiliilor electronice</i> – date unice care sunt utilizate de semnatar sau de creatorul sigiliului pentru a crea o semnătură electronică sau un sigiliu electronic;	Compatibil			SIS al RM
29. „certificat pentru sigiliul electronic” înseamnă o atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective;	<i>certificat pentru sigiliul electronic</i> – document electronic ce conține cheia publică, este semnat cu semnătura electronică sau sigilat cu sigiliul electronic al prestatorului de servicii de încredere, atestă apartenența datelor de validare a sigiliului electronic persoanei juridice și care confirmă numele persoanei respective;	Compatibil			SIS al RM
30. „certificat calificat pentru sigiliul electronic” înseamnă un certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa III;	<i>certificat calificat pentru semnături sau sigilii electronice</i> – înseamnă un certificat pentru o semnătură electronică sau un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în art. 24;	Compatibil			SIS al RM
31. „dispozitiv de creare a sigiliului electronic” înseamnă software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;	<i>dispozitiv de creare a semnăturii electronice sau a sigiliului electronic</i> – mijloace tehnice și/sau de program configurate, utilizate pentru a crea o semnătură sau un sigiliu electronic;	Compatibil			SIS al RM
32. „dispozitiv de creare a sigiliului electronic calificat” înseamnă un dispozitiv de creare a sigiliului electronic care îndeplinește mutatis mutandis cerințele prevăzute în anexa II;	<i>dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate</i> – dispozitiv de creare a semnăturii electronice sau a sigiliului electronic care îndeplinește cerințele prevăzute în art. 26;	Compatibil			SIS al RM
33. „marcă temporală electronică” înseamnă date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment;	<i>marcă temporală electronică</i> – atribut al documentului electronic care certifică faptul că informația a existat la un moment de timp determinat, cu păstrarea autenticității și integrității documentului electronic;	Compatibil			SIS al RM
34. „marcă temporală electronică calificată” înseamnă o	<i>marcă temporală electronică calificată</i> – reprezintă o	Compatibil			SIS al RM

marcă temporală electronică care îndeplinește cerințele prevăzute la articolul 42;	marcă temporală electronică care îndeplinește cerințele prevăzute la art. 30;				
35. „document electronic” înseamnă orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;	<i>document electronic</i> – orice conținut în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;	Compatibil			SIS al RM
36. „serviciu de distribuție electronică înregistrată” înseamnă un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;	<i>serviciu de distribuție electronică înregistrată</i> – reprezintă un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind transmiterea și recepționarea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;	Compatibil			SIS al RM
37. „serviciu de distribuție electronică înregistrată calificat” înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la articolul 44;	<i>serviciu de distribuție electronică înregistrată calificat</i> - înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 32;	Compatibil			SIS al RM
38. „certificat pentru autentificarea unui site internet” înseamnă o atestare care face posibilă autentificarea unui site internet și face legătura între site-ul internet și persoana fizică sau juridică căreia i s-a emis certificatul;	<i>certificat pentru autentificarea unei pagini web</i> - atestare care face posibilă autentificarea unei pagini web și face legătura între pagina web și persoana fizică sau juridică căreia i s-a emis certificatul;	Compatibil			SIS al RM
39. „certificat calificat pentru autentificarea unui site internet” înseamnă un certificat pentru autentificarea unui site internet care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa IV;	<i>certificat calificat pentru autentificarea unei pagini web</i> – certificat pentru autentificarea unei pagini web care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în art. 33;	Compatibil			SIS al RM
40. „date de validare” înseamnă date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;	<i>date de validare</i> – date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;	Compatibil			SIS al RM
41. „validare” înseamnă procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.	<i>validare</i> - procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.	Compatibil			SIS al RM
Articolul 4 Principiul pieței interne (1) Nu există nicio restricție privind prestarea de servicii de încredere pe teritoriul unui stat membru de către un prestator de servicii de încredere stabilit în alt stat membru, din motive care se încadrează în domeniile reglementate de prezentul regulament. (2) Produsele și serviciile de încredere care sunt conforme		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

cu prezentul regulament sunt autorizate pentru a circula liber pe piața internă					
Articolul 5 Prelucrarea și protecția datelor (1) Prelucrarea datelor cu caracter personal se efectuează în conformitate cu Directiva 95/46/CE. (2) Fără a aduce atingere efectului juridic aferent pseudonimelor în temeiul dreptului intern, utilizarea pseudonimelor în cadrul tranzacțiilor electronice nu este interzisă.	Articolul 51. Protecția datelor cu caracter personal (1) Prestatorii de servicii de încredere vor asigura respectarea legislației în domeniul protecției datelor cu caracter personal în procesul de prestare a serviciilor de încredere. (2) Datele cu caracter personal se colectează de către prestatorul de servicii de încredere numai în măsura în care acestea sunt necesare pentru eliberarea și menținerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimțământul expres al persoanei interesate. Directiva 95/46/CE a fost transpusă prin Legea nr.133/2011 privind protecția datelor cu caracter personal.	Compatibil			Centrul Național pentru Protecția Datelor cu Caracter Personal
CAPITOLUL III IDENTIFICARE ELECTRONICĂ Articolul 6 Recunoașterea reciprocă (1) Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică și o autentificare în temeiul dreptului intern sau al practicii administrative naționale pentru a accesa un serviciu prestat online de un organism din sectorul public într-un stat membru, mijloacele de identificare electronică emise într-un alt stat membru sunt recunoscute în primul stat membru în scopul autentificării transfrontaliere a respectivului serviciu online, cu condiția să fie îndeplinite următoarele condiții: (a) mijloacele de identificare electronică să fie emise în cadrul unui sistem de identificare electronică inclus în lista publicată de Comisie în temeiul articolului 9; (b) nivelul de asigurare al respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare egal sau mai ridicat decât nivelul de asigurare impus de organismul din sectorul public relevant pentru a accesa respectivul serviciu online în primul stat membru, cu condiția ca nivelul de asigurare al mijloacelor de		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

<p>identificare electronică respective să corespundă nivelului de asigurare substanțial sau ridicat;</p> <p>(c) organismul din sectorul public relevant utilizează nivelul de asigurare „substanțial” sau „ridicat” în legătură cu accesarea online a serviciului respectiv.</p> <p>Această recunoaștere trebuie să aibă loc în termen de cel mult 12 luni de la publicarea de către Comisie a listei menționate la primul paragraf litera (a).</p> <p>(2) Mijloacele de identificare electronică eliberate în temeiul unui sistem de identificare electronică inclus în lista publicată de Comisie în conformitate cu articolul 9 și care corespund nivelului de asigurare scăzut pot fi recunoscute de către organismele din sectorul public în scopul autentificării transfrontaliere pentru serviciul furnizat online de către organismele respective.</p>					
<p>Articolul 7 Eligibilitatea pentru notificarea sistemelor de identificare electronică</p> <p>Un sistem de identificare electronică este eligibil pentru notificare în temeiul articolului 9 alineatul (1) în cazul în care sunt îndeplinite toate condițiile de mai jos:</p> <p>(a) mijloacele de identificare electronică din cadrul sistemului de identificare electronică sunt emise:</p> <p>(i) de statul membru care notifică;</p> <p>(ii) pe baza unui mandat din partea statului membru care notifică; sau</p> <p>(iii) independent de statul membru care notifică și sunt recunoscute de respectivul stat membru;</p> <p>(b) mijloacele de identificare electronică din cadrul sistemului de identificare electronică pot fi utilizate pentru a accesa cel puțin un serviciu care este prestat de un organism din sectorul public și care necesită identificarea electronică în statul membru care notifică;</p> <p>(c) sistemul de identificare electronică și mijloacele de identificare electronică emise în temeiul acestuia îndeplinesc cerințele aferente cel puțin unuia dintre nivelurile de asigurare prevăzute în actul de punere în aplicare menționat la articolul 8 alineatul (3);</p> <p>(d) statul membru care notifică se asigură că datele de identificare personală, reprezentând în mod unic persoana</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		

<p>în cauză, sunt atribuite, în conformitate cu specificațiile, standardele și procedurile tehnice aferente nivelului de asigurare relevant prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3), persoanei fizice sau juridice menționate la articolul 3 punctul 1 la momentul emiterii mijloacelor de identificare electronică din cadrul sistemului respectiv;</p> <p>(e) partea care emite mijloacele de identificare electronică din cadrul respectivului sistem se asigură că mijloacele de identificare electronică sunt atribuite persoanelor menționate la litera (d) de la prezentul articol, în conformitate cu specificațiile tehnice, standardele și procedurile aferente nivelului de asigurare corespunzător prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3);</p> <p>(f) statul membru care notifică asigură disponibilitatea autentificării online, astfel încât orice beneficiar stabilit pe teritoriul altui stat membru să poată confirma datele de identificare personală primite în format electronic.</p> <p>În cazul altor beneficiari decât organismele din sectorul public, statul membru care notifică poate defini condițiile de acces la mijlocul respectiv de autentificare. Autentificarea transfrontalieră este furnizată gratuit atunci când este efectuată în legătură cu un serviciu online prestat de un organism din sectorul public. Statele membre nu impun nicio cerință tehnică specifică disproporționată beneficiarilor care intenționează să efectueze o astfel de autentificare, atunci când astfel de cerințe împiedică sau afectează semnificativ interoperabilitatea sistemelor de identificare electronică notificate;</p> <p>(g) cu cel puțin șase luni înaintea notificării în conformitate cu articolul 9 alineatul (1), statul membru care notifică furnizează celorlalte state membre, în scopul îndeplinirii obligației prevăzute la articolul 12 alineatul (5), o descriere a sistemului respectiv în conformitate cu modalitățile prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul (7);</p> <p>(h) sistemul de identificare electronică îndeplinește cerințele prevăzute în actul de punere în aplicare menționat la articolul 12 alineatul (8).</p>					
---	--	--	--	--	--

<p>Articolul 8 Niveluri de asigurare ale mijloacelor de identificare electronică</p> <p>(1) Un sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) specifică nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv.</p> <p>(2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv:</p> <p>(a) nivelul de asigurare scăzut se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității;</p> <p>(b) nivelul de asigurare substanțial se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității;</p> <p>(c) nivelul de asigurare ridicat se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad mai ridicat de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane decât mijloacele de identificare electronică cu nivel de asigurare substanțial și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a împiedica utilizarea frauduloasă sau modificarea</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		
--	--	-------------------------------------	--	--	--

<p>frauduloasă a identității.</p> <p>(3) Până la 18 septembrie 2015, ținând cont de standardele internaționale relevante și sub rezerva alineatului (2), Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificații tehnice, standarde și proceduri minime, în raport cu care sunt specificate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică în sensul alineatului (1).</p> <p>Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente:</p> <p>(a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică;</p> <p>(b) procedura pentru emiterea mijloacelor de identificare electronică solicitate;</p> <p>(c) mecanismul de autentificare, prin care persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar;</p> <p>(d) entitatea care emite mijloacele de identificare electronică;</p> <p>(e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și</p> <p>(f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise.</p> <p>Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>					
<p>Articolul 9</p> <p>Notificarea</p> <p>(1) Statul membru care notifică înaintează Comisiei următoarele informații și, fără întârzieri nejustificate, orice modificări ulterioare ale acestora:</p> <p>(a) o descriere a sistemului de identificare electronică notificat, incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului;</p> <p>(b) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la următoarele aspecte: (i)</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		

<p>partea care emite mijloacele de identificare electronică; și</p> <p>(ii) partea care desfășoară procedura de autentificare;</p> <p>(c) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică;</p> <p>(d) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală;</p> <p>(e) o descriere a modului în care sunt îndeplinite cerințele prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul(8);</p> <p>(f) o descriere a autentificării menționate la articolul 7 litera (f);</p> <p>(g) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză.</p> <p>(2) La un an de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8), Comisia publică în Jurnalul Oficial al Uniunii Europene o listă a sistemelor de identificare electronică care au fost notificate în temeiul alineatului (1) de la prezentul articol și informațiile de bază cu privire la acestea.</p> <p>(3) În cazul în care Comisia primește o notificare după expirarea perioadei menționate la alineatul (2), aceasta publică în Jurnalul Oficial al Uniunii Europene modificările la lista menționată la alineatul (2) în termen de două luni de la data primirii respectivei notificări.</p> <p>(4) Un stat membru poate înainta Comisiei o cerere de eliminare a unui sistem de identificare electronică notificat de respectivul stat membru din lista menționată la alineatul (2). Comisia publică în Jurnalul Oficial al Uniunii Europene modificările corespunzătoare aduse listei, în termen de o lună de la primirea cererii statului membru.</p> <p>(5) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească circumstanțele, formatele și procedurile pentru notificările în temeiul alineatului (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>					
--	--	--	--	--	--

<p>Articolul 10 Încălcarea securității</p> <p>(1) În cazul în care fie sistemul de identificare electronică notificat în conformitate cu articolul 9 alineatul (1), fie autentificarea menționată la articolul 7 litera (f) este încălcată sau parțial compromisă într-un mod care afectează fiabilitatea autentificării transfrontaliere a sistemului respectiv, statul membru care notifică suspendă sau revocă, fără întârziere, respectiva autentificare transfrontalieră sau părțile compromise în cauză și informează celelalte state membre și Comisia.</p> <p>(2) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) este remediată, statul membru care notifică reinstituie autentificarea transfrontalieră și informează celelalte state membre și Comisia fără întârzieri nejustificate.</p> <p>(3) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) nu este remediată în termen de trei luni de la suspendare sau revocare, statul membru care notifică comunică celorlalte state membre și Comisiei retragerea sistemului de identificare electronică. Comisia publică în Jurnalul Oficial al Uniunii Europene, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 9 alineatul (2).</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		
<p>Articolul 11 Răspunderea</p> <p>(1) Statul membru care notifică este răspunzător pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligațiilor care îi revin în temeiul articolului 7 litera (d) și (f).</p> <p>(2) Partea care emite mijloacele de identificare electronică este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligației menționate la articolul 7 litera (e).</p> <p>(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenționat</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		

<p>sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere pentru neasigurarea executării corecte a autentificării menționate la articolul 7 litera (f).</p> <p>(4) Alineatele (1), (2) și (3) se aplică în conformitate cu normele de drept intern privind răspunderea.</p> <p>(5) Alineatele (1), (2) și (3) nu aduc atingere răspunderii care revine, în conformitate cu dreptul intern, părților la o tranzacție în care sunt utilizate mijloace de identificare electronică care intră sub incidența sistemului de identificare electronică notificat în temeiul articolului 9 alineatul (1).</p>					
<p>Articolul 12 Cooperarea și interoperabilitatea</p> <p>(1) Sistemele naționale de identificare electronică notificate în temeiul articolului 9 alineatul (1) sunt interoperabile.</p> <p>(2) În sensul alineatului (1), se stabilește un cadru de interoperabilitate.</p> <p>(3) Cadru de interoperabilitate îndeplinește următoarele criterii: (a) urmărește să fie neutru din punctul de vedere al tehnologiei și nu acordă prioritate niciuneia dintre soluțiile tehnice naționale specifice pentru identificarea electronică pe teritoriul statului membru;</p> <p>(b) respectă standardele europene și internaționale, atunci când este posibil;</p> <p>(c) facilitează punerea în aplicare a principiului luării în considerare a vieții private începând cu momentul conceperii (privacy by design); și</p> <p>(d) garantează că datele cu caracter personal sunt prelucrate în conformitate cu Directiva 95/46/CE.</p> <p>(4) Cadru de interoperabilitate este alcătuit din următoarele elemente: (a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la articolul 8;</p> <p>(b) o clasificare a nivelurilor naționale de asigurare aferente sistemelor de identificare electronică notificate în funcție de nivelurile de asigurare menționate la articolul 8;</p> <p>(c) o trimitere la cerințele tehnice minime referitoare la interoperabilitate;</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		

<p>(d) o trimitere la un set minim de date de identificare personală, reprezentând în mod unic o persoană fizică sau juridică, care sunt disponibile din sistemele de identificare electronică;</p> <p>(e) regulamentul de procedură;</p> <p>(f) dispoziții referitoare la soluționarea litigiilor; și</p> <p>(g) standarde de securitate operaționale comune.</p> <p>(5) Statele membre cooperează cu privire la următoarele aspecte:</p> <p>(a) interoperabilitatea sistemelor de identificare electronică notificate în conformitate cu articolul 9 alineatul (1) și a sistemelor de identificare electronică pe care statele membre intenționează să le notifice; și</p> <p>(b) securitatea sistemelor de identificare electronică.</p> <p>(6) Cooperarea dintre statele membre constă în:</p> <p>(a) schimbul de informații, de experiență și de bune practici privind sistemele de identificare electronică și, în special, cerințele tehnice referitoare la interoperabilitate și la nivelurile de asigurare;</p> <p>(b) schimbul de informații, de experiență și de bune practici cu privire la modul de lucru cu nivelurile de asigurare ale sistemelor de identificare electronică menționate la articolul 8;</p> <p>(c) evaluarea inter pares privind sistemele de identificare electronică care fac obiectul prezentului regulament; și</p> <p>(d) analiza evoluțiilor relevante din domeniul identificării electronice.</p> <p>(7) Până la 18 martie 2015, Comisia stabilește, prin intermediul actelor de punere în aplicare, modalitățile procedurale necesare pentru a facilita cooperarea între statele membre menționate la alineatele (5) și (6), în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc.</p> <p>(8) Până la 18 septembrie 2015, în vederea stabilirii de condiții uniforme pentru punerea în aplicare a cerinței menționate la alineatul (1), sub rezerva criteriilor stabilite la alineatul (3) și luând în considerare rezultatele cooperării dintre statele membre, Comisia adoptă acte de punere în aplicare privind cadrul de interoperabilitate, astfel cum este prevăzut la alineatul (4).</p>					
---	--	--	--	--	--

(9) Actele de punere în aplicare menționate la alineatele (7) și (8) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
CAPITOLUL III SERVICII DE ÎNCREDERE SECȚIUNEA 1 Dispoziții generale Articolul 13 Răspunderea și sarcina probei (1) Fără a aduce atingere alineatului (2), prestatorii de servicii de încredere sunt răspunzători pentru prejudiciile cauzate în mod intenționat sau din neglijență oricărei persoane fizice sau juridice ca urmare a nerespectării obligațiilor prevăzute în prezentul regulament. Sarcina de a proba intenția sau neglijența unui prestator de servicii de încredere necalificat revine persoanei fizice sau juridice care introduce o acțiune în despăgubiri pentru prejudiciul menționat la primul paragraf. Prezumția de intenție sau de neglijență se aplică unui prestator de servicii de încredere calificat, cu excepția cazului în care acesta dovedește că prejudiciul menționat la primul paragraf nu a intervenit din intenția sau din neglijența prestatorului de servicii de încredere calificat. (2) În cazul în care prestatorii de servicii de încredere își informează clienții în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează și în cazul în care aceste restricții pot fi recunoscute de părțile terțe, prestatorii de servicii de încredere nu sunt răspunzători pentru prejudiciile rezultate din utilizarea serviciilor care depășesc restricțiile indicate. (3) Alineatele (1) și (2) se aplică în conformitate cu normele de drept intern privind răspunderea.	Articolul 53. Răspunderea și sarcina probei (1) Prestatorul de servicii de încredere poartă răspundere civilă, contravențională sau penală, după caz, conform legislației. (2) Prestatorul de servicii de încredere poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligațiilor prevăzute de prezenta lege, cu excepția cazurilor în care prestatorul de servicii de încredere aduce probe pertinente că nu a putut împiedica cauzarea prejudiciului. (3) 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. (4) Intenția sau neglijența prestatorului de servicii de încredere calificat se prezumă, până la proba contrară. (5) 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 în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează.	Compatibil			SIS al RM
Articolul 14 Aspecte internaționale (1) Serviciile de încredere prestate de prestatori de servicii de încredere stabiliți într-o țară terță sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile electronice de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune dacă	Articolul 3. Recunoașterea reciprocă (1) Recunoașterea serviciilor electronice de încredere și a documentului electronic în afara 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	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE		SIS al RM

<p>serviciile de încredere care provin din țara terță sunt recunoscute în temeiul unui acord încheiat între Uniune și țara terță în cauză sau o organizație internațională în conformitate cu articolul 218 din TFUE.</p> <p>(2) Acordurile menționate la alineatul (1) garantează, în special, că: (a) cerințele aplicabile prestatorilor de servicii de încredere calificați stabiliți în Uniune și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de servicii de încredere din țara terță sau de organizațiile internaționale cu care a fost încheiat acordul, precum și de serviciile de încredere pe care aceștia le prestează;</p> <p>(b) serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță sau de organizația internațională cu care a fost încheiat acordul.</p>	<p>stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaționale.</p> <p>(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:</p> <p>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;</p> <p>b) un prestator de servicii de încredere acreditat cu domiciliul sau cu sediul în Republica Moldova garantează recunoașterea certificatului;</p> <p>c) certificatul 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.</p> <p>(3) Serviciile electronice 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 unui stat străin.</p>				
<p>Articolul 15</p> <p>Accesibilitatea pentru persoanele cu handicap</p> <p>Dacă este posibil, serviciile de încredere prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu handicap.</p>		<p>Parțial compatibil</p>	<p>Legea nr.60/2012 privind incluziunea socială a persoanelor cu dizabilități deja conține norme similare, motiv din care dublarea reglementărilor este inoportună.</p> <p>Articolul 17.</p> <p>Politica de stat în domeniul accesibilității</p> <p>(1) În scopul asigurării unei vieți independente</p>		<p>Ministerul Sănătății, Muncii și Protecției Sociale, Ministerul Economiei și Infrastructurii, SIS al RM</p>

			<p>persoanelor cu dizabilități, autoritățile publice centrale și locale, organizațiile nonguvernamentale, agenții economici, indiferent de forma de organizare juridică, în funcție de competențele lor funcționale, evaluează situația în domeniu și întreprind măsuri concrete pentru a facilita accesul persoanelor cu dizabilități, în condiții de egalitate cu ceilalți, la mediul fizic, la transport, la informație și la mijloacele de comunicare, inclusiv la tehnologia informației și la comunicațiile electronice, la alte utilități și servicii deschise sau furnizate publicului, atât în localitățile urbane, cât și în localitățile rurale, în conformitate cu normativele în vigoare.</p> <p>(2) Identificarea și eliminarea obstacolelor/ barierelor față de accesul deplin al persoanelor cu dizabilități trebuie aplicate în special la clădiri, drumuri, mijloace de transport și alte utilități interioare și</p>		
--	--	--	---	--	--

			exterioare, inclusiv școli, case, instituții publice și locuri de muncă, la serviciile de informare și comunicare, inclusiv serviciile electronice și de urgență, de asemenea la alte utilități și servicii publice.		
Articolul 16 Sanctiuni Statele membre stabilesc normele referitoare la sancțiunile aplicabile în cazul încălcării prezentului regulament. Sancțiunile prevăzute sunt eficace, proporționale și disuasive.	Articolul 52. Răspunderea persoanelor fizice și juridice care cad sub incidența prezentei legi (1) Persoanele fizice și juridice poartă răspundere, conform legislației, pentru neîndeplinirea prevederilor prezentei legi. (2) Intermediarul în circulația electronică a documentelor poartă răspundere, 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 aceste acțiuni și/sau inacțiuni. (3) Pentru acces ilegal la informația cuprinsă în documentele electronice, persoanele poartă răspundere civilă, contravențională sau penală, după caz, conform legislației. (4) Litigiile apărute în cadrul circulației electronice a documentelor, precum și cele legate de utilizarea documentelor electronice și a serviciilor electronice de încredere se soluționează de către subiecții circulației electronice a documentelor în conformitate cu legislația și contractele încheiate. Articolul 54. Răspunderea titularului certificatului cheii publice (1) Titularul certificatului cheii publice poartă răspundere civilă, contravențională sau penală, după caz, conform legislației. (2) Titularul certificatului cheii publice poartă răspundere civilă pentru prejudiciul cauzat de:	Compatibil			SIS al RM

	<p>a) neîndeplinirea sau îndeplinirea defectuoasă a obligațiilor prevăzute de prezenta lege;</p> <p>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 va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.</p>				
SECȚIUNEA 2 Supravegherea Articolul 17 Organismul de supraveghere (1) Statele membre desemnează un organism de supraveghere stabilit pe teritoriul lor sau, de comun acord cu un alt stat membru, un organism de supraveghere stabilit în acel stat membru. Organismul respectiv este responsabil de sarcinile de supraveghere în statul membru care l-a desemnat. Organismelor de supraveghere li se conferă competențele necesare și resursele adecvate pentru exercitarea sarcinilor lor.	Articolul 34. Organul de supraveghere și control (1) Organ de supraveghere și control este Serviciul de Informații și Securitate al Republicii Moldova;	Compatibil			SIS al RM
(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
(3) Rolul organismului de supraveghere constă în: (a) supravegherea prestatorilor de servicii de încredere calificați stabiliți pe teritoriul statului membru care l-a desemnat pentru a se asigura, prin intermediul activităților de supraveghere ex ante și ex post, că respectivii prestatori de servicii de încredere calificați, precum și serviciile de încredere calificate pe care le prestează, îndeplinesc cerințele stabilite în prezentul regulament; (b) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați stabiliți pe teritoriul statului membru care l-a desemnat, prin intermediul activităților de supraveghere ex post, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere calificați sau serviciile de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezentul regulament.	(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, inclusiv voluntară, a prestatorilor de servicii de încredere și retrace statutul respectiv; c) exercită funcția prestatorului de servicii de încredere calificat de nivel superior pentru prestatorii de servicii de încredere calificați acreditați; d) asigură ținerea, actualizarea și accesul public la datele Registrului de evidență a prestatorilor de servicii de încredere; e) elaborează și aprobă, prin acte normative, cerințele în domeniul serviciilor de încredere;	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE		SIS al RM

<p>(4) În sensul alineatului (3) și sub rezerva restricțiilor prevăzute de acesta, sarcinile organismului de supraveghere includ, în special:</p> <p>(a) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolul 18;</p> <p>(b) să efectueze analiza rapoartelor de evaluare a conformității menționate la articolul 20 alineatul (1) și la articolul 21 alineatul (1);</p> <p>(c) să informeze celelalte organisme de supraveghere și publicul cu privire la încălcarea securității sau la pierderea integrității, în conformitate cu articolul 19 alineatul (2);</p> <p>(d) să raporteze Comisiei cu privire la activitățile sale principale, în conformitate cu alineatul (6) de la prezentul articol;</p> <p>(e) să realizeze audituri sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați, în conformitate cu articolul 20 alineatul (2);</p> <p>(f) să coopereze cu autoritățile de protecție a datelor, în special prin informarea acestora, fără întârzieri nejustificate, cu privire la rezultatele auditurilor prestatorilor de servicii de încredere calificați, în cazul în care se presupune că normele de protecție a datelor cu caracter personal au fost încălcate;</p> <p>(g) să acorde statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează și să retragă statutul respectiv, în conformitate cu articolele 20 și 21;</p> <p>(h) să informeze organismul responsabil cu lista sigură națională menționată la articolul 22 alineatul (3) cu privire la deciziile sale de acordare sau de retragere a statutului de calificat, cu excepția cazului în care respectivul organism este și organism de supraveghere;</p> <p>(i) să verifice existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului în cazurile în care prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate cu articolul 24 alineatul (2) litera (h);</p> <p>(j) să solicite prestatorilor de servicii de încredere să</p>	<p>f) monitorizează și controlează respectarea cerințelor la prestarea serviciilor de încredere;</p> <p>g) participă la elaborarea și aprobarea reglementărilor tehnice și a standardelor în domeniul serviciilor de încredere;</p> <p>h) acordă, la solicitare, asistență metodică și practică la utilizarea serviciilor de încredere;</p> <p>i) supraveghează prestatorii de servicii de încredere calificați privind calitatea și securitatea serviciilor de încredere calificate pe care le prestează precum și îndeplinirea cerințelor stabilite în prezenta lege;</p> <p>j) aplică măsuri, după caz, în legătură cu prestatorii de servicii de încredere, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezenta lege;</p> <p>k) cooperează cu autoritățile de protecție a datelor, în special prin informarea acestora, 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;</p> <p>l) solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezenta lege;m) realizează colaborarea internațională în domeniul serviciilor de încredere.</p>				
--	--	--	--	--	--

remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament.					
<p>(5) Statele membre pot să solicite organismului de supraveghere să stabilească, să mențină și să actualizeze o infrastructură de asigurare a încrederii în conformitate cu condițiile stabilite de dreptul intern.</p> <p>(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere înaintează Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior, însoțit de un rezumat al notificărilor încălcărilor primit de la prestatorii de servicii de încredere, în conformitate cu articolul 19 alineatul (2).</p> <p>(7) Comisia pune la dispoziția statelor membre raportul anual menționat la alineatul (6).</p> <p>(8) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile pentru raportul menționat la alineatul (6). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
<p>Articolul 18</p> <p>Asistență reciprocă</p> <p>(1) Organismele de supraveghere cooperează cu scopul de a face schimb de bune practici. Pe baza unei solicitări justificate din partea unui alt organism de supraveghere, un organism de supraveghere acordă respectivului organism asistență astfel încât activitățile organismelor de supraveghere să poată fi desfășurate în mod coerent. Asistența reciprocă poate viza, în special, solicitările de informații și măsurile de supraveghere, cum ar fi solicitările de a desfășura inspecții legate de rapoartele de evaluare a conformității menționate la articolele 20 și 21.</p> <p>(2) Un organism de supraveghere căruia i se adresează o solicitare de asistență poate respinge respectiva solicitare din oricare dintre următoarele motive: (a) organismul de supraveghere nu are competența de a acorda asistența solicitată; (b) asistența solicitată nu este proporțională cu activitățile de supraveghere ale organismului de supraveghere desfășurate în conformitate cu articolul 17; (c) acordarea asistenței solicitate ar contraveni prezentului regulament.</p>		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

<p>(3) După caz, statele membre pot autoriza organismele lor de supraveghere să efectueze anchete comune în care este implicat personalul din organismele de supraveghere ale celorlalte state membre. Mecanismele și procedurile pentru astfel de acțiuni în comun sunt convenite și stabilite de către statele membre în cauză, în conformitate cu dreptul lor intern.</p>					
<p>Articolul 19 Cerințe de securitate aplicabile prestatorilor de servicii de încredere (1) Prestatorii de servicii de încredere calificați și necalificați iau măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. Ținând cont de cele mai recente evoluții tehnologice, aceste măsuri garantează că nivelul securității este proporțional cu gradul de risc. În special, se iau măsuri pentru a preveni și minimiza impactul incidentelor legate de securitate și pentru a informa părțile interesate cu privire la efectele negative ale oricăror incidente de acest tip. (2) Prestatorii de servicii de încredere calificați și necalificați notifică, fără întârzieri nejustificate, însă, în orice caz, în termen de 24 de ore după ce au aflat, organismului de supraveghere competent și, dacă este cazul, altor organisme relevante, cum sunt organismul național competent pentru securitatea informațiilor sau autoritatea pentru protecția datelor, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. Atunci când încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice încălcarea securității sau pierderea integrității fără întârzieri nejustificate. După caz, în special dacă o încălcare a securității sau o pierdere a integrității se referă la două sau mai multe state membre, organismul de supraveghere notificat informează</p>	<p>Articolul 38. 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 imediat, dar nu mai târziu de 24 de ore de la momentul constatării, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice în cauză încălcarea securității sau pierderea integrității fără întârzieri nejustificate. (3) Organul de supraveghere 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.</p>	<p>Compatibil</p>			<p>SIS al RM</p>

organismele de supraveghere vizate din alte state membre și ENISA. Organismul de supraveghere notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvoltarea încălcării securității sau pierderea integrității servește interesului public.					
(3) Organismul de supraveghere furnizează ENISA, o dată pe an, un rezumat al notificărilor privind încălcarea securității sau pierderea integrității primite de la prestatorii de servicii de încredere. (4) Prin intermediul unor acte de punere în aplicare, Comisia poate: (a) elabora specificații suplimentare referitoare la măsurile menționate la alineatul (1); și (b) defini formatele și procedurile, inclusiv termenele, aplicabile în sensul alineatului (2). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		SIS al RM
SECȚIUNEA 3 Servicii de încredere calificate Articolul 20 Supravegherea prestatorilor de servicii de încredere calificați (1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin o dată la 24 de luni, de către un organism de evaluare a conformității. Scopul auditului este de a confirma că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. Prestatorii de servicii de încredere calificați transmit raportul de evaluare a conformității care a rezultat organismului de supraveghere în termen de trei zile lucrătoare de la primirea lui. (2) Fără a aduce atingere alineatului (1), organismul de supraveghere poate, în orice moment, să efectueze un audit sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind prestatorii de servicii de încredere calificați, pe cheltuiala prestatorilor de servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere	Articolul 35. Controlul în domeniul serviciilor de încredere (1) Controlul privind respectarea cerințelor stabilite de prezenta lege la prestarea serviciilor de încredere de către prestatorii acreditați și la acordarea sau prelungirea 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 – Comisia) în baza regulamentului aprobat de organul de supraveghere și control. (3) Comisia se creează în cadrul organului de supraveghere și control în baza ordinului privind efectuarea controlului, emis de conducătorul acestui organ. (4) Componenta nominală a Comisiei se stabilește pentru fiecare caz în parte. (5) Comisia are dreptul: a) să beneficieze de acces liber la materialele documentare, pe suport de hârtie și în format electronic, necesare pentru desfășurarea lucrărilor ce țin de prestarea serviciilor de încredere, precum și la	Compatibil			SIS al RM

<p>calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează autoritățile pentru protecția datelor cu privire la rezultatele auditurilor sale.</p> <p>(3) În cazul în care organismul de supraveghere solicită prestatorului de servicii de încredere calificat să remedieze neîndeplinirea obligațiilor care îi revin în temeiul prezentului regulament, iar respectivul prestator nu acționează în consecință și, după caz, într-un termen stabilit de organismul de supraveghere, organismul de supraveghere, ținând seama în special de amploarea, de durata și de consecințele respectivei neîndepliniri, poate retrage statutul de calificat al respectivului prestator sau al serviciului prestat de acesta care este afectat și informează organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1). Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la retragerea statutului de calificat, al său sau al serviciului în cauză.</p>	<p>sistemele de distribuție de aplicații soft, la aplicațiile soft și mijloacele tehnice instalate;</p> <p>b) să obțină informații complete despre condițiile și modul de exploatare a mijloacelor tehnice și de program;</p> <p>c) să obțină de la persoanele responsabile și de la personalul prestatorului de servicii de încredere informațiile privind prestarea serviciilor de încredere ce țin de obiectul controlului;</p> <p>d) să beneficieze de acces, în decursul zilei lucrătoare (în perioada efectuării controlului), în încăperile prestatorului de servicii de încredere.</p> <p>(6) Comisia nu are dreptul să efectueze controlul fără prezentarea ordinului privind efectuarea controlului și fără prezentarea actelor de identitate ale membrilor Comisiei.</p> <p>(7) La efectuarea controlului privind respectarea condițiilor prevăzute de prezenta lege, Comisia va ține cont de următoarele principii:</p> <p>a) legalitatea și respectarea competenței stabilite de lege;</p> <p>b) neadmiterea aplicării sancțiunilor care nu sînt stabilite de lege;</p> <p>c) tratarea dubiilor, apărute la aplicarea legislației, în favoarea prestatorului de servicii de încredere;</p> <p>d) efectuarea controlului pe cheltuiala statului;</p> <p>e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului;</p> <p>f) dreptul prestatorului de servicii de încredere de a contesta acțiunile organului de supraveghere și control, inclusiv în instanța judecătorească.</p> <p>(8) Controalele planificate privind respectarea de către prestatorul de servicii de încredere a 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.</p> <p>(9) Planurile controalelor, elaborate de organul de supraveghere și control și aprobate în modul stabilit, se</p>				
---	---	--	--	--	--

	<p>coordonează, în privința termenelor de efectuare, cu conducerea prestatorului de servicii de încredere, cu cel puțin 5 zile lucrătoare înainte de începerea acestor controale.</p> <p>(10) Controalele inopinate se efectuează la decizia organului de supraveghere și control, numai în temeiul:</p> <p>a) depistării și confirmării, de către organul supraveghere și control, a faptelor de încălcare a prezentei legi; și/sau</p> <p>b) recepționării cererilor și reclamațiilor argumentate adresate în formă scrisă organului supraveghere și control referitoare la încălcările sau la îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către prestatorul de servicii de încredere.</p> <p>(11) Prestatorul de servicii de încredere este informat despre efectuarea controlului inopinat în ziua demarării controlului.</p> <p>(12) Controalele repetate se efectuează numai în scopul verificării executării prescripției privind lichidarea încălcărilor prezentei legi, indicate în actul de control precedent (planificat sau inopinat). Controlul repetat se consideră parte componentă a controlului precedent.</p> <p>(13) Controlul se efectuează strict în termenele stabilite în ordinul privind efectuarea controlului.</p> <p>(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 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.</p> <p>(15) La efectuarea controlului privind respectarea obligațiilor prevăzute de prezenta lege, prestatorul de servicii de încredere prezintă informația și documentele relevante scopului controlului și nu împiedică efectuarea acestuia.</p> <p>(16) În baza rezultatelor controlului se întocmește un act în 2 exemplare, unul dintre care se</p>				
--	--	--	--	--	--

	<p>expediază/înmânează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de încredere, iar al doilea se păstrează la organul de supraveghere și control. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de încredere, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexând documentele de rigoare.</p> <p>(17) În cazul în care se depistează încălcări ale obligațiilor prevăzute de prezenta lege, organul supraveghere și control emite, în baza actului de control, prescripția privind lichidarea acestor încălcări, ce cuprinde recomandările privind modul de remediere a tuturor încălcărilor depistate, precum și avertizarea despre posibila suspendare sau retragere a acreditării dacă acestea nu vor fi lichidate în termenul stabilit.</p> <p>(18) Termenul minim stabilit de organul de supraveghere și control pentru lichidarea încălcărilor depistate constituie 10 zile lucrătoare, iar cel maxim – 30 de zile lucrătoare după primirea prescripției expediate/înmânate împreună cu actul de control.</p> <p>(19) În cazuri excepționale și la solicitarea oficială a prestatorului de servicii de încredere, termenul pentru lichidarea încălcărilor poate fi prelungit cu cel mult 20 de zile lucrătoare.</p> <p>(20) Prestatorul de servicii de încredere acreditat care a primit prescripția privind lichidarea încălcărilor obligațiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripție, să comunice organului de supraveghere și control informația privind lichidarea încălcărilor.</p> <p>(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de încredere acreditat, în cazul încălcării obligațiilor prevăzute de prezenta lege, precum și în cazul neînlăturării, în termenul stabilit, a datelor eronate din certificatele cheilor publice, organul de supraveghere și control poate aplica măsuri de suspendare sau retragere a acreditării prestatorului de servicii de încredere în</p>				
--	--	--	--	--	--

	<p>conformitate cu prezenta lege.</p> <p>(22) Informațiile despre rezultatele efectuării controlului se publică de către organul de supraveghere și control pe pagina sa web oficială.</p> <p>(23) 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 judecătorească.</p> <p>Articolul 36. Suspendarea și reluarea valabilității acreditării</p> <p>(1) Acreditarea poate fi suspendată în conformitate cu legislația în domeniul reglementării activității de întreprinzător.</p> <p>(2) Drept temei pentru realizarea acțiunilor prevăzute de lege pentru suspendarea acreditării servesc:</p> <p>a) cererea prestatorului de servicii de încredere privind suspendarea acreditării;</p> <p>b) încălcarea de către prestatorul de servicii de încredere a obligațiilor stabilite de prezenta lege;</p> <p>c) nevalabilitatea garanției bancare sau a poliței de asigurare pentru prestatorul de servicii de încredere acreditat;</p> <p>d) nerespectarea de către prestatorul de servicii de încredere a prescripției privind lichidarea încălcărilor obligațiilor prevăzute de prezenta lege, depistate în urma controlului efectuat de Comisie.</p> <p>(3) Decizia privind suspendarea acreditării se aduce la cunoștință prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăși 2 luni, dacă actele normative în domeniul serviciilor de încredere nu prevăd altfel.</p> <p>(4) Prestatorul de servicii de încredere este obligat să înștiințeze în scris organul de supraveghere și control despre înlăturarea circumstanțelor care au dus la suspendarea acreditării.</p> <p>(5) Decizia privind reluarea valabilității acreditării se adoptă de către organul de supraveghere și control în</p>				
--	--	--	--	--	--

	<p>temeiul hotărârii instanței de judecată care a emis hotărârea de suspendare a acreditării, în termen de 3 zile lucrătoare de la data primirii înștiințării. Decizia se aduce la cunoștință prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data adoptării acesteia.</p> <p>(6) Termenul de valabilitate a acreditării nu se prelungește pe perioada de suspendare a acesteia.</p> <p>Articolul 37. Retragerea acreditării</p> <p>(1) Acreditarea poate fi retrasă în conformitate cu legislația în domeniul reglementării activității de întreprinzător.</p> <p>(2) Drept temei pentru realizarea acțiunilor prevăzute de lege în vederea retragerii acreditării servesc:</p> <p>a) cererea prestatorului de servicii de încredere privind încetarea activității, depusă cu 30 de zile calendaristice înainte de încetarea planificată;</p> <p>b) decizia cu privire la anularea înregistrării de stat a persoanei juridice în cadrul căreia activează prestatorul de servicii de încredere;</p> <p>c) depistarea unor date neautentice în documentele prezentate organului de supraveghere și control;</p> <p>d) constatarea faptului de transmitere a certificatului de acreditare sau a copiei de pe acesta altei persoane în scopul desfășurării genului de activitate acreditat;</p> <p>e) neînlăturarea, în termenul stabilit, a circumstanțelor care au dus la suspendarea acreditării;</p> <p>f) nerespectarea repetată a prescripțiilor privind lichidarea încălcărilor obligațiilor stabilite de prezenta lege.</p> <p>(3) Mențiunea referitoare la data și numărul deciziei privind retragerea acreditării se înscrie în Registrul de evidență a prestatorilor de servicii de încredere nu mai târziu de ziua lucrătoare imediat următoare zilei adoptării deciziei.</p> <p>(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</p>				
--	---	--	--	--	--

	<p>altui prestator de servicii de încredere calificat, în modul stabilit de organul de supraveghere și control, pe cheltuiala prestatorului de servicii de încredere care își încetează activitatea.</p> <p>(5) Prestatorul de servicii de încredere este obligat, în decurs de 10 zile lucrătoare de la data adoptării deciziei de retragere a acreditării, să depună la organul de supraveghere și control certificatul de acreditare retras.</p>				
<p>(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale următoarelor standarde: (a) pentru acreditarea organismelor de evaluare a conformității și pentru raportul de evaluare a conformității menționat la alineatul (1); (b) privind normele de audit în temeiul cărora organismele de evaluare a conformității își vor desfășura evaluarea conformității prestatorilor de servicii de încredere calificați, astfel cum se menționează la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
<p>Articolul 21 Inițierea unui serviciu de încredere calificat (1) În cazul în care prestatorii de servicii de încredere care nu au statutul de calificat intenționează să înceapă să presteze servicii de încredere calificate, aceștia transmit organismului de supraveghere o notificare a intenției lor, împreună cu un raport de evaluare a conformității emis de un organism de evaluare a conformității. (2) Organismul de supraveghere verifică dacă prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezentul regulament și, în special, cerințele pentru prestatorii de servicii de încredere calificați și pentru serviciile de încredere calificate prestate de aceștia. În cazul în care organismul de supraveghere ajunge la concluzia că prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele menționate în primul paragraf, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de</p>	<p>Articolul 6. Acreditarea prestatorului de servicii de încredere (1) 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. (2) Modul de solicitare, acordare, suspendare și retragere a certificatului de acreditare a prestatorului de servicii de încredere 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. (3) Acreditarea în domeniul prestării serviciilor electronice de încredere calificate se acordă prestatorului de servicii de încredere, care întrunește următoarele cerințe: a) dispune de resurse financiare (garanție bancară sau poliță de asigurare) în valoare de cel puțin 300 de mii de lei pentru recuperarea unor</p>	Compatibil			SIS al RM

<p>acesta și informează organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1), în termen de maximum trei luni de la notificare în conformitate cu alineatul (1) de la prezentul articol.</p> <p>În cazul în care verificarea nu este încheiată în termen de trei luni de la notificare, organismul de supraveghere informează prestatorul de servicii de încredere, specificând motivele întârzierii și termenul în care se încheie verificarea.</p>	<p>eventuale prejudicii aduse terților din cauza încrederii acestora în datele conținute în certificatul cheii publice eliberat de către prestatorul de servicii de încredere sau în informația din registrul certificatelor eliberate de către prestatorul de servicii de încredere;</p> <p>b) dispune, pentru prestarea serviciilor de încredere, de personal cu studii superioare în domeniul tehnologiei informației și/sau al securității informaționale, cu nivel corespunzător de competențe și experiență de gestionare și expertizare în domeniul tehnologiei serviciilor electronice de încredere;</p> <p>c) asigură securitatea, fiabilitatea și continuitatea activității de prestare a serviciilor de încredere;</p> <p>d) asigură înregistrarea informației în registrul certificatelor cheilor publice, în special prestează operativ serviciul de suspendare a valabilității certificatului cheii publice și de revocare a acestuia;</p> <p>e) asigură posibilitatea de stabilire cu exactitate a datei și a orei eliberării, suspendării valabilității certificatului cheii publice sau revocării acestuia;</p> <p>f) verifică, în conformitate cu legislația, identitatea persoanei pentru care se eliberează un certificat calificat al cheii publice;</p> <p>g) utilizează sisteme și produse care sunt protejate împotriva modificărilor și garantează siguranța tehnică și criptografică a funcțiilor pe care și le asumă;</p> <p>h) creează condiții de evitare a falsificării certificatelor și, în cazul în care prestatorul de servicii de încredere generează cheia privată și cheia publică, garantează confidențialitatea în procesul de generare a acestor;</p> <p>i) utilizează sisteme care nu stochează sau nu copiază datele de creare a semnăturii electronice sau a sigiliului electronic ale persoanelor pentru care prestatorul de servicii de încredere a prestat servicii de gestionare a cheilor;</p> <p>j) utilizează sisteme fiabile pentru stocarea certificatelor într-o formă care poate fi verificată, astfel încât: – numai persoanele autorizate să poată introduce și modifica date; – autenticitatea informației să poată fi controlată; – certificatele să fie disponibile publicului</p>				
---	---	--	--	--	--

	<p>pentru informare; – toate modificările tehnice care compromit cerințele de siguranță să fie vizibile pentru operator.</p> <p>(4) Prestatorii de servicii de încredere calificați prezintă, pe suport de hârtie, în format electronic sau prin intermediul ghișeului unic de solicitare a actelor permissive, cererea de acreditare cu anexarea documentelor care confirmă întrunirea cerințelor specificate la alin.(2) și, în special, atestă:</p> <p>a) dispunerea de resurse financiare pentru recuperarea unor eventuale prejudicii;</p> <p>b) existența unei reglementări interne privind asigurarea activității prestatorului de servicii de încredere în conformitate cu prevederile prezentei legi;</p> <p>c) corespunderea sistemelor și a produselor utilizate cu cerințele prezentei legi;</p> <p>d) studiile și calificările persoanelor cu funcții de răspundere, ale căror obligații funcționale țin nemijlocit de prestarea serviciilor de încredere;</p> <p>e) numirea persoanelor responsabile de activitatea prestatorului de servicii de încredere și a persoanelor împuternicite să certifice cheile publice, precum și identitatea acestora;</p> <p>f) ordinea de sincronizare cu Timpul Mondial Coordonat (UTC);</p> <p>g) dreptul de import, export, proiectare, producere și comercializare a mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației, precum și dreptul de prestare a serviciilor în domeniul protecției criptografice și tehnice a informației, cu excepția activității desfășurate de autoritățile publice investite cu acest drept prin lege (licența).</p> <p>(5) Documentele menționate la alin. (3) lit. a) se prezintă în original. Documentele menționate la alin. (3) lit. b)-g) se prezintă în original, însoțite de câte o copie, originalul fiind restituit după verificarea copiei la momentul prezentării.</p> <p>(6) La depunerea cererii de acreditare, prestatorul de servicii de încredere necalificat este obligat să prezinte, în formatul stabilit de organul de supraveghere și</p>				
--	---	--	--	--	--

	<p>control, informațiile referitoare la procedurile de securitate și de certificare utilizate, precum și datele sale de identificare.</p> <p>(7) Organul de supraveghere și control, în baza documentelor prezentate, în termen de 30 de zile calendaristice, adoptă decizia privind acreditarea prestatorului de servicii de încredere sau privind refuzul de acreditare.</p> <p>(8) În cazul adoptării deciziei de acreditare, organul de supraveghere și control, în termen de 10 zile calendaristice din momentul luării deciziei, notifică prestatorul de servicii de încredere despre decizia luată și eliberează acestuia certificatul de acreditare de modelul stabilit și, în conformitate cu actele normative în domeniul serviciilor electronice de încredere, înregistrează prestatorul acreditat în Registrul de evidență a prestatorilor de servicii de încredere.</p> <p>(9) În cazul adoptării deciziei privind refuzul de acreditare, organul de supraveghere și control, în termen de 10 zile calendaristice din momentul luării deciziei de refuz, notifică în scris prestatorul de servicii de încredere despre decizia luată, cu indicarea cauzelor refuzului.</p> <p>(10) Drept temei pentru refuzul de acreditare servește necorespunderea prestatorului de servicii de încredere cerințelor specificate la alin. (3) sau prezentarea informației neveridice în documentele ce se anexează la cererea de acreditare.</p> <p>(11) Refuzul de acreditare nu împiedică depunerea repetată a documentelor în vederea acreditării după înlăturarea cauzelor care au servit temei pentru refuzul de acreditare.</p> <p>(12) Decizia privind refuzul de acreditare poate fi contestată în instanța de judecată în modul stabilit.</p> <p>(13) Prestatorul de servicii de încredere se consideră acreditat din ziua emiterii certificatului de acreditare.</p> <p>(14) În caz de deteriorare sau pierdere a certificatului de acreditare, prestatorul de servicii de încredere i se eliberează un duplicat al certificatului în termen de 5 zile lucrătoare, în baza cererii depuse.</p>				
--	---	--	--	--	--

	<p>(15) Informația despre prestatorii de servicii de încredere acreditați, precum și despre cei cu acreditarea retrasă se publică de către organul de supraveghere și control pe pagina sa web oficială.</p> <p>(16) După primirea certificatului de acreditare pentru prestarea serviciilor de încredere calificate, cheia publică a prestatorului de servicii încredere este certificată de către prestatorul de servicii de încredere de nivel superior, în conformitate cu regulamentul aprobat de organul de supraveghere și control.</p> <p>(17) Acreditarea se consideră acordată sau, după caz, prelungită dacă organul de supraveghere și control nu răspunde solicitantului în termenul prevăzut de lege pentru acordarea sau prelungirea acesteia.</p> <p>(18) După expirarea termenului de acreditare și în lipsa unei notificări scrise din partea organului de supraveghere și control, acreditarea se consideră prelungită pentru același termen.</p> <p>(19) Prestatorii de servicii de încredere necalificați acreditați sunt obligați să comunice organului de supraveghere și control, cu cel puțin 10 zile calendaristice înainte, orice intenție de modificare a procedurilor de securitate și de certificare, cu precizarea datei și orei la care modificarea intră în vigoare, precum și să confirme, în decurs de 24 de ore, modificarea efectuată.</p> <p>(20) În cazurile de urgență în care securitatea serviciilor de încredere este afectată, prestatorii de servicii de încredere necalificate acreditați pot efectua modificări ale procedurilor de securitate și de certificare, urmând să comunice, în termen de 24 de ore, organului de supraveghere și control modificările efectuate și justificarea deciziei luate.</p> <p>(21) Prestatorii de servicii de încredere acreditați sunt obligați, pe parcursul întregului termen de acreditare, să asigure respectarea cerințelor în conformitate cu care a fost acreditat. În cazul apariției circumstanțelor care fac imposibilă asigurarea respectării acestor cerințe, prestatorul de servicii de încredere urmează să notifice organul de supraveghere și control despre acest fapt în</p>				
--	---	--	--	--	--

	decurs de 24 de ore. (22) Prestatorul de servicii de încredere calificat de nivel superior nu este supus acreditării în conformitate cu prevederile prezentei legi.				
(3) Prestatorii de servicii de încredere calificați pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în listele sigure menționate la articolul 22 alineatul (1). (4) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile în sensul alineatelor (1) și (2). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 22 Listele sigure (1) Fiecare stat membru instituie, menține și publică liste care includ informații referitoare la prestatorii de servicii de încredere calificați pentru care este responsabil, împreună cu informații referitoare la serviciile de încredere calificate prestate de aceștia. (2) Statele membre instituie, mențin și publică, în mod securizat, listele sigure semnate sau sigilate electronic menționate la alineatul (1), într-o formă adecvată pentru prelucrarea automată. (3) Statele membre notifică Comisiei, fără întârzieri nejustificate, informații cu privire la organismul responsabil pentru instituirea, menținerea și publicarea listelor sigure naționale și detalii despre locul unde sunt publicate aceste liste, certificatele utilizate pentru semnarea sau sigilarea listelor sigure și orice modificări ale acestora. (4) Comisia pune la dispoziția publicului, printr-un canal sigur, informațiile menționate la alineatul (3) într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată. (5) Până la 18 septembrie 2015, Comisia specifică, prin intermediul unor acte de punere în aplicare, informațiile menționate la alineatul (1) și definește specificațiile tehnice și formatele pentru listele sigure aplicabile în sensul alineatelor (1)-(4). Respectivetele acte de punere în		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).RO 28.8.2014 Jurnalul Oficial al Uniunii Europene L 257/97					
Articolul 23 Marca de încredere a UE pentru serviciile de încredere calificate (1) După indicarea statutului de calificat menționat la articolul 21 alineatul (2) al doilea paragraf pe lista sigură menționată la articolul 22 alineatul (1), prestatorii de servicii de încredere calificați pot utiliza o marcă de încredere a UE pentru a indica într-un mod simplu, ușor de recunoscut și clar serviciile de încredere calificate pe care le prestează. (2) În cazul utilizării mărcii de încredere a UE pentru serviciile de încredere calificate menționate la alineatul (1), prestatorii de servicii de încredere calificați se asigură că pe site-ul lor internet este disponibil un link către lista sigură relevantă. (3) Până la 1 iulie 2015, Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificațiile referitoare la forma și, în special, prezentarea, componența, mărimea și designul mărcii de încredere a UE pentru serviciile de încredere calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 24 Cerințe pentru prestatorii de servicii de încredere calificați (1) Atunci când emite un certificat calificat pentru un serviciu de încredere, un prestator de servicii de încredere calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat. Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în conformitate cu dreptul intern: (a) de către persoana fizică sau de către un reprezentant	Articolul 8. 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 în cauză; 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; d) să asigure accesul la registrul certificatelor cheilor	Compatibil			SIS al RM

<p>autorizat al persoanei juridice, în persoană; sau</p> <p>(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 și care îndeplinesc cerințele stabilite la articolul 8 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”; sau</p> <p>(c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu dispozițiile de la litera (a) sau (b); sau</p> <p>(d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică. Nivelul de asigurare echivalent este confirmat de un organism de evaluare a conformității.</p> <p>(2) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate:</p> <p>(a) informează organismul de supraveghere cu privire la orice schimbare survenită în prestarea sa de servicii de încredere calificate și cu privire la vreo intenție de a își înceta activitatea respectivă;</p> <p>(b) angajează personal și, după caz, subcontractanți care dețin cunoștințele, credibilitatea, experiența și calificările necesare și care au beneficiat de formare adecvată în ceea ce privește normele de siguranță și protecție a datelor cu caracter personal și aplică proceduri administrative și de gestiune care corespund standardelor europene sau internaționale;</p> <p>(c) în ceea ce privește riscul de răspundere pentru daune în conformitate cu articolul 13, menține suficiente resurse financiare și/sau obține o asigurare de răspundere adecvată, în conformitate cu dreptul intern;</p> <p>(d) înainte de stabilirea unei relații contractuale, informează, în mod clar și cuprinzător, orice persoană care dorește să utilizeze un serviciu de încredere calificat de clauzele și condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia;</p>	<p>publice, cu respectarea prevederilor art. 51;</p> <p>e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege și să facă mențiunea respectivă în registrul certificatelor cheilor publice în termenele stabilite;</p> <p>f) să acopere prejudiciile aduse oricărei entități sau persoane fizice, care se încrede 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;</p> <p>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;</p> <p>h) să prezinte informațiile necesare pentru autentificarea serviciilor de încredere;</p> <p>i) să solicite eliberarea duplicatului certificatului de acreditare în cazul pierderii sau deteriorării acestuia;</p> <p>j) să îndeplinească alte obligații stabilite de legislația în vigoare.</p> <p>(2) Prestatorul de servicii de încredere calificat acreditat este obligat, suplimentar celor stipulate la alin. (1):</p> <p>a) să certifice, în modul stabilit de legislație, cheia publică a prestatorului de servicii de încredere calificat acreditat, destinată certificării cheilor publice;</p> <p>b) să informeze organul de supraveghere și control cu privire la orice schimbare survenită în prestarea de servicii de încredere calificate și cu privire la intenția de a își înceta activitatea respectivă;</p> <p>c) să utilizeze sisteme sigure pentru stocarea datelor care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât:</p> <ul style="list-style-type: none"> – acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul subiectului la care se referă datele; – numai persoanele autorizate să poată introduce și/sau modifica datele stocate; – autenticitatea datelor să poată fi controlată; 				
--	---	--	--	--	--

<p>(e) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea;</p> <p>(f) utilizează sisteme demne de încredere pentru a stoca datele care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât: (i) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul persoanei la care se referă datele; (ii) numai persoanele autorizate să poată introduce și modifica datele stocate; (iii) autenticitatea datelor să poată fi controlată;</p> <p>(g) ia măsuri adecvate împotriva falsificării și furtului de date;</p> <p>(h) înregistrează și menține accesibile pentru o perioadă de timp corespunzătoare, inclusiv ulterior încetării activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către prestatorul de servicii de încredere calificat, în special în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic;</p> <p>(i) are un plan actualizat, în cazul încetării serviciului, pentru a asigura continuitatea serviciului conform dispozițiilor verificate de către organismul de supraveghere, în conformitate cu articolul 17 alineatul (4) litera (i);</p> <p>(j) asigură prelucrarea legală a datelor cu caracter personal în conformitate cu Directiva 95/46/CE; (k) în cazul prestatorilor de servicii de încredere calificați care eliberează certificate calificate, instituie și actualizează permanent o bază de date a certificatelor.</p> <p>(3) Dacă un prestator de servicii de încredere calificat care eliberează certificate calificate decide să revoce un certificat, acesta înregistrează respectiva revocare în baza sa de date privind certificatele și publică statutul de revocat al certificatului în timp util și în orice caz în termen de 24 de ore de la primirea cererii. Revocarea intră în vigoare imediat după publicare.</p> <p>(4) Cu privire la alineatul (3), prestatorii de servicii de încredere calificați care emit certificate calificate</p>	<p>d) să verifice, prin mijloace corespunzătoare și în conformitate cu legislația în vigoare, 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:</p> <ul style="list-style-type: none"> - de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau - 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; - prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat; <p>e) să ia măsuri adecvate împotriva falsificării și furtului de date;</p> <p>f) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art.11, 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;</p> <p>g) înainte să stabilească o relație contractuală cu o persoană care solicită un certificat în sprijinul serviciului său de încredere, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele 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 pe cale electronică, trebuie comunicate în scris, într-un limbaj accesibil. Elementele pertinente ale informațiilor trebuie puse, de asemenea, la cerere, la dispoziția părților terțe care beneficiază de certificat;</p> <p>h) să înregistreze și mențină accesibile pentru o perioadă de 15 ani, inclusiv ulterior încetării activității</p>				
--	--	--	--	--	--

furnizează oricărui beneficiar informații cu privire la valabilitatea sau revocarea statutului de certificate calificate emise de aceștia. Aceste informații sunt puse la dispoziție cel puțin pentru fiecare certificat în parte, în orice moment și după expirarea perioadei de valabilitate a certificatului, în mod automat, fiabil, gratuit și eficient.	prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către prestatorul de servicii de încredere calificat, în special în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic.				
(5) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numerele de referință ale standardelor pentru sisteme și produse demne de încredere, care respectă cerințele prevăzute la alineatul (2) literale (e) și (f) de la prezentul articol. În cazul în care sistemele și produsele demne de încredere respectă standardele respective, se presupune că acestea respectă cerințele prevăzute la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
SECȚIUNEA 4 Semnătura electronică Articolul 25 Efectele juridice ale semnăturilor electronice (1) Unei semnături electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnăturile electronice calificate. (2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe. (3) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru este recunoscută drept semnătură electronică calificată în toate celelalte state membre.	Articolul 17. Principiile de utilizare a semnăturii electronice și sigiliului electronic Principiile de utilizare a semnăturii electronice și sigiliului electronic sunt: a) libertatea alegerii și utilizării oricărui tip de semnătură electronică sau sigiliului electronic, dacă actele normative sau acordul părților nu prevăd cerința de utilizare a unui tip concret de semnătură electronică sau sigiliului electronic, în corespundere cu obiectivele de utilizare a acesteia; b) posibilitatea alegerii oricăror tehnologii și/sau mijloace tehnice care permit utilizarea tipurilor concrete de semnături electronice sau sigiliului electronic în conformitate cu prevederile prezentei legi; c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice sau sigiliului electronic și/sau a documentului electronic semnat sau sigilat prin intermediul acestor doar în baza faptului că semnătura electronică sau sigiliul electronic a fost creat prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic și/sau al produsului asociat .	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE		

	<p>Articolul 19. Regimul juridic de utilizare a semnăturii electronice și sigiliului electronic (1) Semnătura electronică și sigiliul electronic, indiferent de gradul de protecție de care dispune, produce efecte juridice și este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă: a) se prezintă în formă electronică; sau b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau c) nu se bazează pe un certificat calificat al cheii publice; sau d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic. (2) Semnătura electronică calificată are aceeași valoare juridică ca și semnătura olografă. (3) Semnătura electronică calificată și sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă semnătura sau sigiliul electronic calificat. (4) Modalitatea în care se asigură gradul de protecție a semnăturii electronice calificate pentru echivalarea acestora cu semnătura olografă aplicată pe hârtie se stabilește de organul de supraveghere și control, conform atribuțiilor prevăzute la art. 34 alin.(2). (5) Modalitatea de aplicare a semnăturilor electronice de către funcționarii persoanelor juridice de drept public se stabilește de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanții acestora. (6) Semnătura electronică și sigiliul electronic nu constituie mijloace de criptare a informației.</p>				
<p>Articolul 26 Cerințe pentru semnături electronice avansate O semnătura electronică avansată îndeplinește următoarele cerințe: (a) face trimitere exclusiv la semnatar; (b) permite identificarea semnatarului; (c) este creată utilizând date de creare a semnăturilor</p>	<p>Articolul 22. Cerințele pentru semnăturile și sigiliile electronice avansate Semnătura electronică sau sigiliul electronic avansat îndeplinește cumulativ următoarele cerințe: a) face trimitere exclusiv la titular; b) permite identificarea titularului; c) este creată prin mijloace controlate exclusiv de</p>	Compatibil			SIS al RM

electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său; și (d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.	titular; d) este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.				
Articolul 27 Semnăturile electronice în cadrul serviciilor publice (1) În cazul în care un stat membru solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște semnăturile electronice avansate, semnăturile electronice avansate bazate pe un certificat calificat pentru semnături electronice și semnăturile electronice calificate care întrebunțează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5). (2) În cazul în care un stat membru solicită o semnătură electronică avansată bazată pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște semnăturile electronice avansate bazate pe un certificat calificat și semnăturile electronice calificate care întrebunțează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5). (3) Statele membre nu solicită o semnătură electronică la un nivel de securitate mai ridicat decât cel al semnăturii electronice calificate pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public. (4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru semnături electronice avansate. În cazul în care o semnătură electronică avansată îndeplinește respectivele standarde, se presupune că aceasta respectă cerințele referitoare la semnăturile electronice avansate menționate în prezentul articol alineatele (1) și (2) și la articolul 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

<p>5) Până la 18 septembrie 2015 și ținând cont de practicile, standardele și actele juridice ale Uniunii existente, Comisia definește, prin intermediul unor acte de punere în aplicare, formate de referință ale semnăturilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative. Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>					
<p>Articolul 28 Certificate calificate pentru semnăturile electronice (1) Certificatele calificate pentru semnăturile electronice îndeplinesc cerințele prevăzute în anexa I. (2) Certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa I. (3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate. (4) În cazul în care un certificat calificat pentru semnăturile electronice a fost revocat după activarea inițială, acesta își pierde valabilitatea din momentul în care a fost revocat și nu se revine în niciun caz la statutul său anterior. (5) Sub rezerva următoarelor condiții, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a unui certificat calificat pentru semnătura electronică: (a) în cazul în care un certificat calificat pentru semnătura electronică a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare; (b) perioada de suspendare este clar indicată în baza de date privind certificatele și statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informații privind statutul certificatului. (6) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru semnătura electronică. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește</p>	<p>Articolul 24. Cerințe pentru certificatele calificate pentru semnături sau sigilii electronice Certificatele pentru semnături sau sigilii electronice calificate conțin: a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului de sigiliu electronic; d) datele de validare a semnăturilor sau 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) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent; h) date de verificare a certificatului calificat pentru semnătura sau sigiliul electronic care corespund datelor de creare a acestora.</p>	<p>Parțial compatibil</p>	<p>Transpunerea integrală este condiționată de aderarea RM la UE</p>		

standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa I. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
Articolul 29 Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate (1) Dispozitivele de creare a semnăturilor electronice calificate îndeplinesc cerințele prevăzute în anexa II. (2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru dispozitivele de creare a semnăturilor electronice calificate. În cazul în care un dispozitiv de creare a semnăturilor electronice calificat îndeplinește standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa II. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice (1) Dispozitivele de creare a semnăturilor sau sigiliilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice și proceduri corespunzătoare, cel puțin că: a) datele de creare a semnăturii 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 sau a sigiliului electronic nu pot fi deduse prin calcul și semnătura sau sigiliul sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane; d) să ofere posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura sau sigiliului electronic sau să facă referința irevocabilă la documentul dat; e) să creeze o semnătură sau un sigiliu electronic numai după confirmarea de către semnatar sau creatorul unui sigiliu a operațiunii de creare a semnăturii sau a sigiliului electronic; f) să confirme în mod univoc crearea semnăturii sau a sigiliului electronic. (2) Dispozitivele de creare a semnăturii sau sigiliului electronic avansate sau calificate nu trebuie să modifice datele care urmează a fi semnate sau sigilate, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE		
Articolul 30 Certificarea dispozitivelor de creare a semnăturilor		Parțial compatibil	Prevederile art. 30 alin.(1) nu sunt	În termen	SIS al RM

electronice calificate (1) Conformitatea dispozitivelor de creare a semnăturii electronice calificate cu cerințele prevăzute în anexa II este certificată de organisme publice sau private adecvate desemnate de statele membre.			fundamentale, respectiv vor fi expuse în actele normative subordonate legii.	de 12 luni de la data publicării legii	
(2) Statele membre notifică Comisiei denumirile și adresele organismului public sau privat menționat la alineatul (1). Comisia pune informațiile respective la dispoziția statelor membre. (3) Certificarea menționată la alineatul (1) se bazează pe unul dintre următoarele elemente: (a) un proces de evaluare de securitate efectuat în conformitate cu unul dintre standardele pentru evaluarea securității produselor din domeniul tehnologiei informației incluse în lista instituită în conformitate cu al doilea paragraf; sau (b) un alt proces decât procesul prevăzut la litera (a), cu condiția ca acest proces să utilizeze niveluri de securitate comparabile și ca organismul public sau privat menționat la alineatul (1) să notifice Comisiei respectivul proces. Procesul respectiv poate fi utilizat numai în absența standardelor menționate la litera (a) sau dacă un proces de evaluare de securitate menționat la litera (a) este în curs de desfășurare. Comisia stabilește, prin intermediul unor acte de punere în aplicare, lista standardelor pentru evaluarea de securitate a produselor din domeniul tehnologiei informației menționate la litera (a). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).(4) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47 privind stabilirea de criterii specifice care urmează să fie îndeplinite de către organismele desemnate menționate la alineatul (1) de la prezentul articol.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 31 Publicarea unei liste a dispozitivelor de creare a semnăturilor electronice certificate și calificate (1) Statele membre notifică Comisiei, fără întârzieri nejustificate și în termen de maximum o lună de la încheierea certificării, informații cu privire la dispozitivele de creare a semnăturilor electronice calificate care au fost		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

<p>certificate de către organismele menționate la articolul 30 alineatul (1). De asemenea, statele membre notifică Comisiei, fără întârziere și în termen de maximum o lună de la anularea certificării, informații cu privire la dispozitivele de creare a semnăturii electronice care nu mai sunt certificate.</p> <p>(2) Pe baza informațiilor primite, Comisia stabilește, publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate.</p> <p>(3) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile aplicabile în sensul alineatului (1). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>					
<p>Articolul 32 Cerințe pentru validarea semnăturilor electronice calificate</p> <p>(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:</p> <p>(a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu anexa I;</p> <p>(b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;</p> <p>(c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar;</p> <p>(d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului;</p> <p>(e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim;</p> <p>(f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;</p> <p>(g) integritatea datelor semnate nu a fost compromisă; (h) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării.</p> <p>(2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul</p>	<p>Articolul 28. Cerințe pentru validarea semnăturii și sigiliului electronic calificate</p> <p>Procesul de validare a unei semnături sau sigiliu electronic calificat confirmă validitatea acestora cu următoarele condiții:</p> <p>a) certificatul care stă la baza semnăturii sau sigiliului a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 24;</p> <p>b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării sau sigilării;</p> <p>c) datele de validare a semnăturilor sau sigiliilor corespund datelor furnizate de titularul certificatului cheii publice;</p> <p>d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice;</p> <p>e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim;</p> <p>f) semnătura sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificat;</p> <p>g) integritatea datelor semnate sau sigilate nu a fost compromisă;</p>	<p>Compatibil</p>			<p>SIS al RM</p>

corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.	h) cerințele prevăzute la articolul 22 au fost îndeplinite la momentul semnării.				
(3) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru validarea semnăturilor electronice calificate. În cazul în care validarea semnăturilor electronice calificate îndeplinește standardele respective, se presupune că aceasta respectă cerințele prevăzute la alineatul (1). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 33 Serviciul calificat de păstrare a semnăturilor electronice calificate (1) Un serviciu de validare calificat pentru semnături electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care: (a) realizează validarea în conformitate cu articolul 32 alineatul (1); și (b) permite beneficiarilor să primească rezultatul procesului de validare în mod automat, fiabil, eficient și care poartă semnătura electronică avansată sau sigiliul electronic avansat al prestatorului care oferă serviciul de validare calificat.		Parțial compatibil	Prevederile art. 33 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		SIS al RM
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință pentru standardele referitoare la serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare a semnăturilor electronice calificate îndeplinește standardele respective, se prezumă că acesta respectă cerințele prevăzute la alineatul (1). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 34 Serviciul calificat de păstrare a semnăturilor electronice calificate (1) Un serviciu calificat de păstrare a semnăturilor electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care utilizează proceduri și tehnologii capabile să extindă fiabilitatea		Parțial compatibil	Prevederile art. 34 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		SIS al RM

semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.					
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru serviciul calificat de păstrare a semnăturilor electronice calificate. În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele respective, se presupune că acestea respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
SECȚIUNEA 5 Sigiliile electronice Articolul 35 Efectele juridice ale sigiliilor electronice (1) Unui sigiliu electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca probă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru sigiliile electronice calificate. (2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.	Articolul 19. Regimul juridic de utilizare a semnăturii electronice și sigiliului electronic (1) Semnătura electronică și sigiliul electronic, indiferent de gradul de protecție de care dispune, produce efecte juridice și este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă: a) se prezintă în formă electronică; sau b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau c) nu se bazează pe un certificat calificat al cheii publice; sau d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic. (2) Semnătura electronică calificată are aceeași valoare juridică ca și semnătura olografă. (3) Semnătura electronică calificată și sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă semnătura sau sigiliul electronic calificat. (4) Modalitatea în care se asigură gradul de protecție a semnăturii electronice calificate pentru echivalarea acestora cu semnătura olografă aplicată pe hârtie se stabilește de organul de supraveghere și control, conform atribuțiilor prevăzute la art. 34 alin.(2). (5) Modalitatea de aplicare a semnăturilor electronice de către funcționarii persoanelor juridice de drept public se stabilește de Guvern. Persoanele juridice de	Compatibil			SIS al RM

	drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanții acestora. (6) Semnătura electronică și sigiliul electronic nu constituie mijloace de criptare a informației.				
(3) Un sigiliu electronic calificat bazat pe un certificat calificat eliberat de un stat membru este recunoscut drept sigiliu electronic calificat în toate celelalte state membre.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 36 Cerințele pentru sigiliile electronice avansate Un sigiliu electronic avansat îndeplinește următoarele cerințe: (a) face trimitere exclusiv la creatorul sigiliului; (b) permite identificarea creatorului sigiliului; (c) este creat cu ajutorul datelor de creare a sigiliilor electronice pe care creatorul sigiliului le poate utiliza sub controlul său, cu un nivel ridicat de încredere, pentru crearea sigiliilor electronice; și (d) este legat de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată.	Articolul 22. Cerințele pentru semnăturile și sigiliile electronice avansate Semnătura electronică sau sigiliul electronic avansat îndeplinește cumulativ următoarele cerințe: a) face trimitere exclusiv la titular; b) permite identificarea titularului; c) este creată prin mijloace controlate exclusiv de titular; d) este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.	Compatibil			SIS al RM
Articolul 37 Sigiliile electronice în cadrul serviciilor publice (1) În cazul în care un stat membru solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate, sigiliile electronice avansate bazate pe un certificat calificat pentru sigilii electronice și sigiliile electronice calificate care întrebuițează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5). (2) În cazul în care un stat membru solicită un sigiliu electronic bazat pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate bazate pe un certificat calificat și sigiliile electronice calificate care întrebuițează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5). (3) Statele membre nu solicită un sigiliu electronic la un		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

<p>nivel de securitate mai ridicat decât cel al sigiliului electronic calificat pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public.</p> <p>(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru sigilii electronice avansate. În cazul în care un sigiliu electronic avansat îndeplinește standardele respective, se presupune că acesta respectă cerințele referitoare la sigiliile electronice avansate menționate la alineatele (1) și (2) de la prezentul articol și la articolul 36. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p> <p>(5) Până la 18 septembrie 2015 și ținând cont de practicile, standardele și actele juridice ale Uniunii existente, Comisia definește, prin intermediul unor acte de punere în aplicare, formate de referință ale sigiliilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>					
<p>Articolul 38 Certificate calificate pentru sigiliul electronic (1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III. (2) Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa III. (3) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate. (4) În cazul în care un certificat calificat pentru un sigiliu electronic a fost revocat după activarea inițială, acesta își pierde valabilitatea din momentul în care a fost revocat și nu se revine în niciun caz la statutul său anterior. (5) Sub rezerva următoarelor condiții, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a certificatelor calificate pentru sigiliile electronice:</p>	<p>Articolul 24. Cerințe pentru certificatele calificate pentru semnături sau sigilii electronice Certificatele pentru semnături sau sigilii electronice calificate conțin:</p> <p>a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice;</p> <p>b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;</p> <p>c) datele de identificare și alte date ale semnatarului sau creatorului de sigiliu electronic;</p> <p>d) datele de validare a semnăturilor sau sigiliilor electronice care corespund datelor de creare a acestora;</p> <p>e) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează;</p> <p>f) numărul unic de înregistrare a certificatului;</p>	<p>Parțial compatibil</p>	<p>Transpunerea integrală este condiționată de aderarea RM la UE</p>		<p>SIS al RM</p>

<p>(a) în cazul în care un certificat calificat pentru sigilii electronice a fost suspendat temporar, respectivul certificat își pierde valabilitatea pe parcursul perioadei de suspendare;</p> <p>(b) perioada de suspendare este clar indicată în baza de date privind certificatele și statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informații privind statutul certificatului.</p> <p>(6) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru sigiliile electronice. În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa III. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>	<p>g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent;</p> <p>h) date de verificare a certificatului calificat pentru semnătura sau sigiliul electronic care corespund datelor de creare a acestora.</p>				
<p>Articolul 39 Dispozitive de creare a sigiliilor electronice calificate (1) Articolul 29 se aplică mutatis mutandis cerințelor pentru dispozitivele de creare a sigiliilor electronice calificate. (2) Articolul 30 se aplică mutatis mutandis certificării dispozitivelor de creare a sigiliilor electronice calificate. (3) Articolul 31 se aplică mutatis mutandis publicării unei liste a dispozitivelor de creare a sigiliilor electronice certificate și calificate.</p>	<p>Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice (1) Dispozitivele de creare a semnăturilor sau sigiliilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice și proceduri corespunzătoare, cel puțin că: a) datele de creare a semnăturii 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 sau a sigiliului electronic nu pot fi deduse prin calcul și semnătura sau sigiliul sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane; d) să ofere posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura sau sigiliului electronic sau să facă referința irevocabilă la documentul dat;</p>	<p>Parțial compatibil</p>	<p>Transpunerea integrală este condiționată de aderarea RM la UE. Totodată, prevederile art.30 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.</p>		<p>SIS al RM</p>

	<p>e) să creeze o semnătură sau un sigiliu electronic numai după confirmarea de către semnatar sau creatorul unui sigiliu a operațiunii de creare a semnăturii sau a sigiliului electronic;</p> <p>f) să confirme în mod univoc crearea semnăturii sau a sigiliului electronic.</p> <p>(2) Dispozitivele de creare a semnăturii sau sigiliului electronic avansate sau calificate nu trebuie să modifice datele care urmează a fi semnate sau sigilate, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.</p>				
<p>Articolul 40</p> <p>Validarea și păstrarea sigiliilor electronice calificate</p> <p>Articolele 32, 33 și 34 se aplică mutatis mutandis validării și păstrării sigiliilor electronice calificate.</p>	<p>Articolul 28. Cerințe pentru validarea semnăturii și sigiliului electronic calificate</p> <p>Procesul de validare a unei semnături sau sigiliu electronic calificat confirmă validitatea acestora cu următoarele condiții:</p> <p>a) certificatul care stă la baza semnăturii sau sigiliului a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 24;</p> <p>b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării sau sigilării;</p> <p>c) datele de validare a semnăturilor sau sigiliilor corespund datelor furnizate de titularul certificatului cheii publice;</p> <p>d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice;</p> <p>e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim;</p> <p>f) semnătura sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificat;</p> <p>g) integritatea datelor semnate sau sigilate nu a fost compromisă;</p> <p>h) cerințele prevăzute la articolul 22 au fost îndeplinite la momentul semnării.</p>	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE Totodată, prevederile art.33 alin.(1) și 34 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		SIS al RM
SECȚIUNEA 6	Secțiunea a 4-a	Compatibil			SIS al RM

Mărcile temporale electronice Articolul 41 Efectul juridic al mărcilor temporale electronice (1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată. (2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate.	Mărcile temporale electronice Articolul 29. Efectul juridic al mărcilor temporale electronice (1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată. (2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate.				
(3) O marcă temporală electronică calificată emisă într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate statele membre.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 42 Cerințe pentru mărcile temporale electronice calificate (1) O marcă temporală electronică calificată îndeplinește următoarele cerințe: (a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat; (b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; și (c) este semnată utilizând o semnătură electronică avansată sau sigilată cu un sigiliu electronic avansat al prestatorului de servicii de încredere calificat sau printr-o metodă echivalentă.	Articolul 30. 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 acreditat și îndeplinește următoarele cerințe: a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat; b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; c) este semnată utilizând o semnătură electronică calificată sau sigilată cu un sigiliu electronic calificat al prestatorului de servicii de încredere calificat.	Compatibil			SIS al RM
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru legătura între dată și oră și date și pentru exactitatea surselor orei indicate. În cazul în care legătura între dată și oră și date și exactitatea surselor orei indicate îndeplinesc standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Respectivile acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

articolul 48 alineatul (2).					
SECȚIUNEA 7 Serviciul de distribuție electronică înregistrată Articolul 43 Efectul juridic al unui serviciu de distribuție electronică înregistrată (1) Datelor trimise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca dovadă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru serviciul de distribuție electronică înregistrată. (2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de către destinatarul identificat și a preciziei datei și orei trimiterii și primirii datelor indicate de serviciul de distribuție electronică înregistrată.	Secțiunea a 5-a Serviciul de distribuție electronică înregistrată Articolul 31. Efectul juridic al unui serviciu de distribuție electronică înregistrată (1) Datelor transmise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca dovadă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru serviciul de distribuție electronică înregistrată. (2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de către destinatarul identificat și a preciziei datei și orei trimiterii și primirii datelor indicate de serviciul de distribuție electronică înregistrată.	Compatibil			SIS al RM
Articolul 44 Cerințe pentru serviciile de distribuție electronică înregistrată calificate (1) Serviciile de distribuție electronică înregistrată calificate îndeplinesc următoarele cerințe: (a) sunt prestate de către unul sau mai mulți prestatori de servicii de încredere calificați; (b) asigură identificarea expeditorului cu un nivel de încredere ridicat; (c) asigură identificarea destinatarului înainte de furnizarea datelor; (d) trimiterea și primirea datelor este securizată printr-o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat; (e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului și destinatarului datelor; (f) data și ora trimiterii, primirii și ale oricărei modificări a	Articolul 32. Cerințe pentru serviciile de distribuție electronică înregistrată calificate Serviciile de distribuție electronică înregistrată calificate îndeplinesc următoarele cerințe: a) sunt prestate de către unul sau mai mulți prestatori de servicii de încredere calificați; b) asigură identificarea expeditorului; c) asigură identificarea destinatarului înainte de furnizarea datelor; d) trimiterea și primirea datelor este securizată printr-o semnătură electronică calificată sau un sigiliu electronic calificat astfel încât să se excludă posibilitatea că datele să fie schimbate fără ca acest lucru să fie detectat; e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului și destinatarului datelor; f) data și ora trimiterii, primirii și ale oricărei modificări a datelor este indicată printr-o marcă	Compatibil			SIS al RM

datelor este indicată printr-o marcă temporală electronică calificată. În cazul datelor transferate între doi sau mai mulți prestatori de servicii de încredere, cerințele de la literale (a)-(f) se aplică tuturor prestatorilor de servicii de încredere calificați.	temporală electronică calificată.				
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru procesele de trimitere și primire de date. În cazul în care procesul de trimitere și primire de date îndeplinește standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
SECȚIUNEA 8 Autentificarea unui site internet Articolul 45 Cerințe pentru certificatele calificate pentru autentificarea unui site internet(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute în anexa IV.	Secțiunea a 6-a Autentificarea unei pagini web Articolul 33. Cerințe pentru certificatele calificate pentru autentificarea unei pagini web Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină: a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale titularului certificatului cheii publice, precum și informațiile necesare pentru comunicarea cu acesta; d) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează; e) numele domeniului (domeniilor) gestionate de titularului 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.	Compatibil			SIS al RM

<p>(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru autentificarea unui site internet. În cazul în care un certificat calificat pentru autentificarea unui site internet îndeplinește standardele respective, se presupune că respectă cerințele prevăzute în anexa IV. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		
<p>CAPITOLUL IV DOCUMENTE ELECTRONICE Articolul 46 Efectele juridice ale documentelor electronice Unui document electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.</p>	<p>Capitolul V REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC ȘI CIRCULAȚIA ELECTRONICĂ A DOCUMENTELOR Articolul 39. Regimul juridic de utilizare a documentului electronic (8) Documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic este echivalat, după valoarea sa probantă, cu probele scrise sau mijloacele materiale de probă. Documentul electronic semnat cu semnătura electronică sau sigilat cu sigiliul electronic nu poate fi respins în calitate de probă pentru motivul că are o formă electronică.</p>	<p>Compatibil</p>			<p>SIS al RM</p>
<p>CAPITOLUL V DELEGAREA DE COMPETENȚE ȘI MĂSURI DE PUNERE ÎN APLICARE Articolul 47 Exercitarea delegării (1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol. (2) Se conferă Comisiei, pentru o perioadă de timp nedeterminată de la 17 septembrie 2014, competența de a adopta actele delegate menționate la articolul 30 alineatul (4). (3) Delegarea competențelor menționată la articolul 30 alineatul (4) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. Decizia de revocare pune capăt delegării competenței menționate în decizia respectivă. Aceasta produce efecte începând cu</p>		<p>Norme UE neaplicabile</p>	<p>Transpunerea este condiționată de aderarea RM la UE</p>		

<p>ziua următoare datei publicării în Jurnalul Oficial al Uniunii Europene sau la o dată ulterioară specificată în decizie. Aceasta nu aduce atingere valabilității actelor delegate aflate deja în vigoare.</p> <p>(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.</p> <p>(5) Un act delegat adoptat în conformitate cu articolul 30 alineatul (4) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea actului respectiv Parlamentului European și Consiliului sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European și Consiliul au informat Comisia cu privire la faptul că nu vor formula obiecții. La inițiativa Parlamentului European sau a Consiliului, termenul respectiv se prelungește cu două luni.</p>					
<p>Articolul 48 Procedura comitetului</p> <p>(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.</p> <p>(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.</p>		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
<p>CAPITOLUL VI DISPOZIȚII FINALE Articolul 49 Revizuire</p> <p>Comisia evaluează modul de aplicare a prezentului regulament și prezintă un raport în acest sens Parlamentului European și Consiliului cel mai târziu la 1 iulie 2020. Comisia evaluează, în special, dacă este oportun să se modifice domeniul de aplicare al prezentului regulament sau dispozițiile sale specifice, inclusiv articolul 6, articolul 7 litera (f), articolele 34, 43, 44 și 45, ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, ale pieței și juridice. Raportul menționat la primul paragraf este însoțit, după caz, de propuneri legislative. În plus, Comisia prezintă un raport Parlamentului European și Consiliului, o dată la patru ani,</p>		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		

ulterior raportului menționat la primul paragraf, cu privire la progresele realizate în vederea atingerii obiectivelor prezentului regulament.					
Articolul 50 Abrogare (1) Directiva 1999/93/CE se abrogă cu efect de la 1 iulie 2016. (2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea RM la UE		
Articolul 51 Măsurile tranzitorii (1) Dispozitivele sigure de creare a semnăturilor a căror conformitate a fost determinată în conformitate cu articolul 3 alineatul (4) din Directiva 1999/93/CE sunt considerate dispozitive de creare a semnăturilor electronice calificate în temeiul prezentului regulament. (2) Certificatele calificate emise pentru persoane fizice în conformitate cu Directiva 1999/93/CE sunt considerate drept certificate calificate pentru semnături electronice în temeiul prezentului regulament, până la expirarea lor. (3) Un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE prezintă un raport de evaluare a conformității către organismul de supraveghere cât mai curând posibil, dar nu mai târziu de 1 iulie 2017. Până la prezentarea unui astfel de raport de evaluare a conformității și până la finalizarea de către organismul de supraveghere a evaluării sale, prestatorul de servicii de certificare respectiv este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament. (4) În cazul în care un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE nu prezintă un raport de evaluare a conformității către organismul de supraveghere în termenul prevăzut la alineatul (3), respectivul prestator de servicii de certificare nu este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament începând cu data de 2 iulie 2017.	Capitolul VIII DISPOZIȚII FINALE ȘI TRANZITORII Articolul 55. Dispoziții finale (2) La data intrării în vigoare a prezentei legi se abrogă Legea nr.91 din 29.05.2014 privind semnătura electronică și documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr.174-177, art./710), cu modificările ulterioare. (4) Certificatele cheilor publice eliberate în baza Legii nr.91 din 29.05.2014 privind semnătura electronică și documentul electronic rămân valabile până la expirarea termenului de valabilitate a acestora. (5) În termen de 18 luni de la data publicării prezentei legi, prestatorii de servicii de certificare a cheilor publice înstitute în baza Legii nr.91 din 29.05.2014 privind semnătura electronică și documentul electronic sunt obligați să treacă procedura de acreditare în conformitate cu prevederile prezentei legi.	Parțial compatibil	Transpunerea integrală este condiționată de aderarea RM la UE		SIS al RM
Articolul 52 Intrarea în vigoare		Norme UE neaplicabile	Transpunerea este condiționată de aderarea		

<p>(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.</p> <p>(2) Prezentul regulament se aplică de la 1 iulie 2016, cu excepția următoarelor dispoziții:</p> <p>(a) articolul 8 alineatul (3), articolul 9 alineatul (5), articolul 12 alineatele (2)-(9), articolul 17 alineatul (8), articolul 19 alineatul (4), articolul 20 alineatul (4), articolul 21 alineatul (4), articolul 22 alineatul (5), articolul 23 alineatul (3), articolul 24 alineatul (5), articolul 27 alineatele (4) și (5), articolul 28 alineatul (6), articolul 29 alineatul (2), articolul 30 alineatele (3) și (4), articolul 31 alineatul (3), articolul 32 alineatul (3), articolul 33 alineatul (2), articolul 34 alineatul (2), articolul 37 alineatele (4) și (5), articolul 38 alineatul (6), articolul 42 alineatul (2), articolul 44 alineatul (2), articolul 45 alineatul (2) și articolele 47 și 48 se aplică de la 17 septembrie 2014;</p> <p>(b) articolul 7, articolul 8 alineatele (1) și (2), articolele 9, 10, 11 și articolul 12 alineatul (1) se aplică de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8);</p> <p>(c) articolul 6 se aplică după trei ani de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8).</p> <p>(3) În cazul în care sistemul de identificare electronică notificat este inclus în lista publicată de Comisie în conformitate cu articolul 9 înainte de data menționată la alineatul (2) litera (c) de la prezentul articol, recunoașterea mijloacelor de identificare electronică din cadrul sistemului respectiv în temeiul articolului 6 are loc cel târziu în termen de 12 luni de la publicarea respectivului sistem, dar nu înainte de data menționată la alineatul (2) litera (c) de la prezentul articol.</p> <p>(4) Fără a aduce atingere alineatului (2) litera (c) de la prezentul articol, un stat membru poate decide ca mijloacele de identificare electronică din cadrul unui sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) de către un alt stat membru să fie recunoscute de primul stat membru de la data aplicării</p>			RM la UE		
---	--	--	----------	--	--

<p>actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8). Statele membre vizate informează Comisia. Comisia publică aceste informații. Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.</p>					
<p>ANEXA I CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SEMNĂTURI ELECTRONICE Certificatele calificate pentru semnături electronice conțin: (a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice; (b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;— în cazul unei persoane fizice: numele persoanei; (c) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (d) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (f) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (h) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit; (i) localizarea serviciilor care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat; (j) în cazul în care datele de creare a semnăturilor electronice legate de datele de validare a semnăturilor electronice sunt situate într-un dispozitiv de creare a semnăturilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.</p>	<p>Articolul 24. Cerințe pentru certificatele calificate pentru semnături sau sigilii electronice Certificatele pentru semnături sau sigilii electronice calificate conțin: a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului de sigiliu electronic; d) datele de validare a semnăturilor sau 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) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent; h) date de verificare a certificatului calificat pentru semnătura sau sigiliul electronic care corespund datelor de creare a acestora.</p>	<p>Compatibil</p>			<p>SIS al RM</p>

<p>ANEXA II CERINȚE PENTRU DISPOZITIVELE DE CREARE A SEMNĂTURILOR ELECTRONICE CALIFICATE</p> <p>1. Dispozitivele de creare a semnăturilor electronice calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că:</p> <p>(a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil;</p> <p>(b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată;</p> <p>(c) există suficiente asigurări că datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice nu pot să fie descoperite prin deducție și că semnătura electronică este protejată în mod fiabil împotriva falsificării utilizând tehnologia disponibilă în prezent;</p> <p>(d) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice pot să fie protejate în mod fiabil de către semnatarul legitim împotriva utilizării de către alte persoane.</p> <p>2. Dispozitivele de creare a semnăturilor electronice calificate nu modifică datele care urmează să fie semnate sau nu împiedică prezentarea lor semnatarului înainte de a semna.</p> <p>3. Generarea sau gestionarea datelor de creare a semnăturilor electronice în numele semnatarului se pot realiza numai de către un prestator de servicii de încredere calificat.</p> <p>4. Fără a aduce atingere punctului 1 litera (d), prestatorii de servicii de încredere calificați care gestionează datele de creare a semnăturilor electronice în numele semnatarului pot duplica datele de creare a semnăturilor electronice numai în scopul de a le avea de rezervă, cu condiția ca următoarele cerințe să fie îndeplinite:</p> <p>(a) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale;</p> <p>(b) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului.</p>	<p>Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice</p> <p>(1) Dispozitivele de creare a semnăturilor sau sigiliilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice și proceduri corespunzătoare, cel puțin că:</p> <p>a) datele de creare a semnăturii sau a sigiliului electronic nu pot apărea decât o singură dată, iar confidențialitatea acestora este asigurată în conformitate cu prezenta lege;</p> <p>b) datele de creare a semnăturii sau a sigiliului electronic nu pot fi deduse prin calcul și semnătura sau sigiliul sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată;</p> <p>c) datele de creare a semnăturii sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane;</p> <p>d) să ofere posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura sau sigiliului electronic sau să facă referința irevocabilă la documentul dat;</p> <p>e) să creeze o semnătură sau un sigiliu electronic numai după confirmarea de către semnatar sau creatorul unui sigiliu a operațiunii de creare a semnăturii sau a sigiliului electronic;</p> <p>f) să confirme în mod univoc crearea semnăturii sau a sigiliului electronic.</p> <p>(2) Dispozitivele de creare a semnăturii sau sigiliului electronic avansate sau calificate nu trebuie să modifice datele care urmează a fi semnate sau sigilate, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.</p>	<p>Parțial compatibil</p>	<p>Prevederile pct.3 și pct.4 nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.</p>		<p>SIS al RM</p>
--	--	----------------------------------	--	--	-------------------------

<p>ANEXA III CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SIGILIILE ELECTRONICE Certificatele calificate pentru sigiliile electronice conțin: (a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru sigilii electronice; (b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;— în cazul unei persoane fizice: numele persoanei; (c) cel puțin numele creatorului sigiliului și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale; (d) datele de validare a sigiliilor electronice, care corespund datelor de creare a sigiliilor electronice; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (f) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (h) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit; (i) localizarea serviciilor care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat; (j) în cazul în care datele de creare a sigiliilor electronice legate de datele de validare a sigiliilor electronice sunt situate într-un dispozitiv de creare a sigiliilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.</p>	<p>Articolul 24. Cerințe pentru certificatele calificate pentru semnături sau sigilii electronice Certificatele pentru semnături sau sigilii electronice calificate conțin: a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului de sigiliu electronic; d) datele de validare a semnăturilor sau 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) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent; h) date de verificare a certificatului calificat pentru semnătura sau sigiliul electronic care corespund datelor de creare a acestora.</p>	Compatibil			SIS al RM
<p>ANEXA IV CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU AUTENTIFICAREA UNUI SITE INTERNET Certificatele calificate pentru autentificarea unui site internet conțin: (a) o indicație, cel puțin într-o formă</p>	<p>Secțiunea a 6-a Autentificarea unei pagini web Articolul 33 Cerințe pentru certificatele calificate pentru autentificarea unei pagini web Certificatele calificate pentru autentificarea unei pagini</p>	Compatibil			SIS al RM

<p>adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unui site internet; (b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale,— în cazul unei persoane fizice: numele persoanei; (c) în cazul persoanelor fizice: cel puțin numele persoanei căreia i s-a eliberat certificatul sau un pseudonim. În cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; în cazul persoanelor juridice: cel puțin denumirea persoanei juridice căreia i se eliberează certificatul și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale; (d) elemente ale adresei persoanei fizice sau juridice căreia i s-a eliberat certificatul, incluzând cel puțin orașul și statul, și, dacă este cazul, în forma în care sunt înscrise în registrele oficiale; (e) numele domeniului (domeniilor) gestionat(e) de persoana fizică sau juridică căreia i s-a emis certificatul; (f) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (g) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (h) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (i) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (h) este disponibil gratuit; (j) localizarea serviciilor privind statutul valabilității certificatului care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat.</p>	<p>web trebuie să conțină:</p> <p>a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web;</p> <p>b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;</p> <p>c) datele de identificare și alte date ale titularului certificatului cheii publice, precum și informațiile necesare pentru comunicarea cu acesta;</p> <p>d) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează;</p> <p>e) numele domeniului (domeniilor) gestionate de titularul certificatului cheii publice căruia i s-a emis certificatul;</p> <p>f) numărul unic de înregistrare a certificatului;</p> <p>g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent.</p>				
--	--	--	--	--	--



**SERVICIUL DE INFORMAȚII ȘI SECURITATE
AL REPUBLICII MOLDOVA**

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 166 tel. 022-239-625, fax 022-234-068, e-mail: sis@sis.md

16 iunie 2020

Nr. 44 - 1730

Cancelariei de Stat

Cerere

privind înregistrarea de către Cancelaria de Stat a proiectelor de acte ce urmează
a fi anunțate în cadrul ședinței secretarilor generali de stat

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul legii „Privind identificarea electronică și serviciile electronice de încredere”.
2.	Autoritatea care a elaborat proiectul	Serviciul de Informații și Securitate al Republicii Moldova
3.	Justificarea depunerii cererii	Proiectul a fost elaborat în temeiul art. 255 al Planului național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioada 2017 – 2019, aprobat prin Hotărârea Guvernului nr. 1472 din 30 decembrie 2016.
4.	Lista autorităților și instituțiilor a căror avizare este necesară	Ministerul Economiei și Infrastructurii Ministerul Finanțelor Ministerul Justiției Centrul Național Anticorupție Centrul de Armonizare a Legislației Agenția Servicii Publice I.P. „Serviciul Tehnologii Informaționale și Securitate Cibernetică” I.P. „Agenția de Guvernare Electronică”
5.	Termenul-limită pentru depunerea avizelor/expertizelor	30 zile lucrătoare
6.	Persoana responsabilă de promovarea proiectului	Valentin Ghețiu, Serviciul de Informații și Securitate, Tel: 022-239-470
7.	Anexe	1. Proiectul hotărârii Guvernului „privind aprobarea proiectului de lege privind identificarea electronică și serviciile electronice de încredere”, pe 1 filă; 2. Proiectul legii „Privind identificarea electronică și serviciile electronice de încredere”, pe 34 file; 3. Nota informativă la proiect, pe 4 file; 4. Tabelul de concordanță, pe 64 file; 5. Analiza impactului de reglementare, pe 13 file; 6. Procesul-verbal nr.19 al ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător din 16 iunie 2020, pe 8 file.
8.	Data și ora depunerii cererii	
9.	Semnătura	

Alexandr ESAULENCO
Director

