UE

Proiect

LEGE

privind identificarea electronică și serviciile de încredere

Parlamentul adoptă prezenta lege organică.

Prezenta lege 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. CELEX: 02014R0910-20241018.

Capitolul I

DISPOZIȚII GENERALE

Articolul 1. Obiect

Prezenta lege urmărește să asigure buna funcționare a pieței interne și să asigure un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere utilizate în Republica Moldova, pentru a permite și a facilita exercitarea de către persoanele fizice și juridice a dreptului de a participa la societatea digitală în condiții de siguranță și de a accesa servicii publice și private online. În acest scop, prezenta lege:

a) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice;

b) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate, serviciile de certificare pentru autentificarea unui site internet, arhivarea electronică, atestarea electronică a atributelor, dispozitivele de creare a semnăturilor, dispozitivele de creare a sigiliilor electronice, precum și pentru registrele electronice;

c) stabilește modul în care Republica Moldova recunoaște prestatorii de servicii de încredere calificați cu sediul în state membre ale Uniunii Europene, precum și serviciile de încredere calificate furnizate de către aceștia.

Articolul 2. Domeniul de aplicare

(1) Prezenta lege se aplică sistemelor de identificare electronică, portofelelor pentru identitatea digitală și prestatorilor de servicii de încredere cu sediul în Republica Moldova.

(2) Prezenta lege 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) Prezenta lege nu aduce atingere cadrului normativ privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma, ori cerințelor sectoriale privind forma.

(4) Prezenta lege nu aduce atingere prevederilor Legii nr. 195/2024 privind protecția datelor cu caracter personal.

Articolul 3. Definiții

În sensul prezentei legi, se aplică următoarele definiții:

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

2. *autentificarea strictă a utilizatorilor* – procedură de autentificare bazată pe utilizarea a cel puțin doi factori de autentificare din categorii diferite, și anume: cunoștințe (ceva ce doar utilizatorul cunoaște), posesie (ceva ce doar utilizatorul posedă) sau inerență (ceva ce caracterizează utilizatorul), factori care sunt independenți între ei, astfel încât compromiterea unuia dintre factori să nu afecteze fiabilitatea celorlalți, iar mecanismul de autentificare este conceput astfel încât să protejeze confidențialitatea datelor de autentificare;

3. *arhivare electronică* - serviciu care asigură primirea, stocarea, recuperarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe parcursul întregii perioade de păstrare;

4. *atestat electronic al atributelor* - atestat în format electronic care permite atributelor să fie autentificate;

5. *atestat electronic calificat al atributelor* - atestat electronic al atributelor care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 54;

6. *atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia* - atestat electronic al atributelor emis de un organism din sectorul public care este responsabil de o sursă autentică ori de un organism din sectorul public care este desemnat de Guvern să emită astfel de atestate ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice în conformitate cu art. 56;

7. *atribut* - o caracteristică, o calitate, un drept sau o permisiune a unei persoane fizice sau juridice sau a unui obiect;

8. *beneficiar* - persoană fizică sau juridică care utilizează un serviciu de încredere sau care se bazează pe date de identificare electronică ori pe atribute prezentate printr-un portofel pentru identitatea digitală sau prin alte mijloace de identificare electronică, în scopul furnizării unui serviciu ori al autorizării unei tranzacții;

9. *certificat pentru semnătura electronică* - 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;

10. *certificat calificat pentru semnătură electronică* - certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 30;

11. *certificat pentru sigiliul electronic* - atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective;

12. *certificat calificat pentru sigiliul electronic* - certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 40;

13. *certificat pentru autentificarea unui site internet* - atestat electronic 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;

14. *certificat calificat pentru autentificarea unui site internet* - certificat pentru autentificarea unui site internet care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 50;

15. *corelarea identității* - proces prin care datele de identificare personală sau mijloacele de identificare electronică sunt corelate sau asociate cu un cont existent care aparține aceleiași persoane;

16. *creatorul unui sigiliu* - persoană juridică care creează un sigiliu electronic;

17. *date cu caracter personal* - cu sensul definit în Legea nr. 195/2024 privind protecția datelor cu caracter personal;

18. *date de creare a semnăturilor electronice* - date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;

19. *date de creare a sigiliilor electronice* - date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;

20. *date de identificare personală* - set de date care permite în conformitate cu cadrul normativ aplicabil stabilirea identității unei persoane fizice sau juridice ori a unei persoane fizice care reprezintă o altă persoană fizică sau o persoană juridică;

21. *date de validare* - date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;

22. *dispozitiv de creare a semnăturilor electronice* - software sau hardware configurat, utilizat pentru a crea o semnătură electronică;

23. *dispozitiv de creare a semnăturilor electronice calificat* - dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute la art. 31;

24. *dispozitiv calificat de creare a semnăturii electronice la distanță* - dispozitiv calificat de creare a semnăturii electronice care este gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 32 în numele unui semnatar;

25. *dispozitiv de creare a sigiliului electronic* - software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;

26. *dispozitiv de creare a sigiliului electronic calificat* - dispozitiv de creare a sigiliului electronic care îndeplinește cerințele prevăzute la art. 42;

27. *dispozitiv calificat de creare a sigiliului electronic la distanță* - dispozitiv calificat de creare a sigiliului electronic care este gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 43 în numele unui creator de sigilii;

28. *document electronic* - orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;

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

30. *înregistrare de date* - date electronice înregistrate împreună cu metadatele aferente care susțin prelucrarea datelor;

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

32. *marcă temporală electronică calificată* - marcă temporală electronică care îndeplinește cerințele prevăzute la art. 47;

33. *mijloace de identificare electronică* - unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării pentru un serviciu online sau, după caz, pentru un serviciu offline;

34. *mod offline* - interacțiune între un utilizator și o terță parte într-un loc fizic care utilizează tehnologii de proximitate imediată, fără ca portofelul pentru identitatea digitală să fie necesar pentru accesarea unor sisteme la distanță prin intermediul rețelelor de comunicații electronice în scopul interacțiunii respective;

35. *organism de drept public* - organism care îndeplinește cumulativ următoarele condiții:

a) este constituită în scopul explicit de a răspunde nevoilor de interes general și nu are caracter industrial sau comercial;

b) are personalitate juridică; și

c) este finanțată în proporție majoritară de autorități publice centrale sau locale sau de alte organisme de drept public; ori gestionarea acestora este supravegheată de autoritățile sau organismele respective; ori au un consiliu administrativ, de conducere sau de supraveghere, în care jumătate dintre membrii săi sunt numiți de autorități ale administrației publice centrale sau locale ori de alte organisme de drept public;

36. *organism din sectorul public* - autoritate a administrației publice centrale sau locale, organism de drept public sau asociație formată din una sau mai multe astfel de autorități sau din unul sau mai multe astfel de organisme de drept public, ori 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;

37. *organism de evaluare a conformității* - persoană juridică independentă, acreditată în Republica Moldova sau într-un stat membru al Uniunii Europene, având competența de a efectua evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate pe care acesta le prestează ori ca fiind competent să efectueze certificarea portofelelor pentru identitatea digitală sau a mijloacelor de identificare electronică;

38. *portofel pentru identitatea digitală* - mijloc de identificare electronică care permite utilizatorului să stocheze, să gestioneze și să valideze în condiții de siguranță datele de identificare personală și atestatele electronice ale atributelor cu scopul de a le furniza beneficiarilor și altor utilizatori ai portofelelor pentru identitatea digitală, precum și să creeze și să aplice semnături electronice calificate sau sigilii electronice calificate;

39. *prestator de servicii de încredere* - persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;

40. *prestator de servicii de încredere calificat* - prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;

41. *produs* - hardware sau software ori componente relevante de hardware sau de software destinate să fie utilizate pentru prestarea de servicii de identificare electronică și de servicii de încredere;

42. *registru electronic* - secvență de înregistrări electronice de date, care asigură integritatea înregistrărilor respective și acuratețea ordinii cronologice a înregistrărilor respective;

43. *registru electronic calificat* - un registru electronic care este pus la dispoziție de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 62;

44. *semnatar* - persoană fizică care creează o semnătură electronică;

45. *semnătură electronică* - date în format electronic, atașate la, sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;

46. *semnătură electronică avansată* - semnătură electronică ce îndeplinește cerințele prevăzute la art. 27;

47. *semnătură electronică calificată* - 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;

48. *serviciu calificat de arhivare electronică* - serviciu de arhivare electronică care este prestat de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 60;

49. *serviciu de distribuție electronică înregistrată* - serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;

50. *serviciu de distribuție electronică înregistrată calificat* - serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 49;

51. *serviciu de încredere* - serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare din următoarele:

a) emiterea certificatelor pentru semnături electronice, a certificatelor pentru sigilii electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere;

b) validarea certificatelor pentru semnăturile electronice, a certificatelor pentru sigiliile electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere;

c) crearea semnăturilor electronice sau a sigiliilor electronice;

d) validarea semnăturilor electronice sau a sigiliilor electronice;

e) păstrarea semnăturilor electronice, a sigiliilor electronice, a certificatelor pentru semnăturile electronice sau a certificatelor pentru sigiliile electronice;

f) gestionarea dispozitivelor pentru crearea semnăturilor electronice la distanță sau a dispozitivelor pentru crearea sigiliilor electronice la distanță;

g) emiterea atestatelor electronice ale atributelor;

h) validarea atestatelor electronice a atributelor;

i) crearea mărcilor temporale electronice;

j) validarea mărcilor temporale electronice;

k) prestarea serviciilor de distribuție electronică înregistrate;

l) validarea datelor transmise prin intermediul serviciilor de distribuție electronică înregistrate și a probelor aferente;

m) arhivarea electronică a datelor electronice;

n) înregistrarea într-un registru electronic a datelor electronice și a documentelor în format electronic;

52. *serviciu de încredere calificat* - serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezenta lege;

53. *serviciu de platformă esențial* - oricare dintre următoarele:

a) serviciile de intermediere online;

b) motoarele de căutare online;

c) serviciile de rețele de socializare online;

d) serviciile de platformă de partajare a materialelor video;

e) serviciile de comunicații interpersonale care nu se bazează pe numere;

f) sistemele de operare;

g) browserele web;

h) asistenții virtuali;

i) serviciile de cloud computing;

j) serviciile de publicitate online, inclusiv orice rețea de publicitate, schimburile publicitare și orice alt serviciu de intermediere publicitară, prestat de o întreprindere care furnizează oricare dintre serviciile de platformă esențiale enumerate la literele (a)-(i);

54. *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;

55. *sigiliu electronic avansat* - sigiliu electronic care îndeplinește cerințele prevăzute la art. 38;

56. *sigiliu electronic calificat* - 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;

57. *sistem de identificare electronică* - sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice, ori pentru persoane fizice care reprezintă alte persoane fizice sau persoane juridice;

58. *sursă autentică* - registru sau un sistem, aflat în responsabilitatea unui organism din sectorul public sau a unei entități private, care conține și pune la dispoziție atribute referitoare la o persoană fizică sau juridică ori la un obiect și care este considerat a fi o sursă primară a informațiilor respective sau care este recunoscut ca fiind autentic în conformitate cu cadrul normativ aplicabil;

59. *utilizator* - persoană fizică sau juridică ori o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică, care utilizează servicii de încredere sau mijloace de identificare electronică, puse la dispoziție în conformitate cu prezenta lege;

60. *utilizator comercial* - persoană fizică sau juridică ce acționează cu titlu comercial sau profesional care utilizează servicii de platformă esențiale în scopul sau în cursul furnizării de bunuri sau servicii către utilizatorii finali;

61. *validare* - procesul prin care se verifică și se confirmă validitatea datelor în format electronic în conformitate cu prezenta lege.

Articolul 4. Pseudonime în tranzacțiile electronice

(1) Utilizarea pseudonimelor alese de utilizatori în cadrul tranzacțiilor electronice este permisă.

(2) Prevederile alin. (1) nu aduc atingere obligațiilor legale privind identificarea utilizatorilor, acolo unde aceasta este prevăzută de cadrul normativ aplicabil, și nici efectelor juridice recunoscute pseudonimelor.

Capitolul II

IDENTIFICARE ELECTRONICĂ

Secțiunea 1
Portofelul pentru identitatea digitală

Articolul 5. Portofelele pentru identitatea digitală

(1) În scopul asigurării accesului securizat, fiabil și neîntrerupt al persoanelor fizice și juridice din Republica Moldova la servicii publice și private, cu menținerea controlului deplin asupra datelor proprii, Instituția Publică Agenția de Guvernare Electronică asigură disponibilitatea unui portofel pentru identitatea digitală.

(2) Portofelele pentru identitatea digitală pot fi puse la dispoziția utilizatorilor și de către furnizori de drept privat, în condițiile prezentei legi.

(3) Codul sursă al componentelor de software ale aplicației portofelelor pentru identitatea digitală face obiectul unei licențe cu sursă deschisă.

(4) În cazuri justificate în mod corespunzător, organismul de supraveghere poate decide nepublicarea codului sursă al anumitor componente ale sistemului, altele decât cele instalate pe dispozitivele utilizatorilor, în măsura în care divulgarea acestuia ar putea afecta securitatea, integritatea sau funcționarea sistemului.

(5) Portofelele pentru identitatea digitală permit utilizatorului, într-un mod transparent și ușor de utilizat și de urmărit de către acesta:

1) să solicite, să obțină, să selecteze, să combine, să stocheze, să șteargă, să partajeze și să prezinte în condiții de siguranță, exclusiv sub controlul utilizatorului, datele de identificare personală și, după caz, în combinație cu atestate electronice ale atributelor, să se autentifice beneficiarilor online și, după caz, în mod offline, pentru a accesa servicii publice și private, asigurând, în același timp, că este posibilă divulgarea selectivă a datelor;

2) să genereze pseudonime și să le stocheze local și în formă criptată în portofelul pentru identitatea digitală;

3) să autentifice în condiții de siguranță portofelul pentru identitatea digitală al unei alte persoane și să primească și partajeze date de identificare personală și atestate electronice ale atributelor într-un mod securizat între cele două portofele pentru identitatea digitală;

4) să acceseze o evidență a tuturor tranzacțiilor efectuate cu ajutorul portofelului pentru identitatea digitală prin intermediul unui tablou de bord comun care să permită utilizatorului:

a) să vizualizeze o listă actualizată a beneficiarilor cu care utilizatorul a stabilit o conexiune și, după caz, a tuturor datelor partajate;

b) să solicite cu ușurință unui beneficiar să șteargă datele cu caracter personal în temeiul art. 17 al Legii nr. 195/2024 privind protecția datelor cu caracter personal;

c) să semnaleze cu ușurință un beneficiar autorității naționale pentru protecția datelor cu caracter personal, atunci când se primește o cerere de date presupus ilegală sau suspectă;

5) să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate;

6) să descarce, în măsura în care acest lucru este fezabil din punct de vedere tehnic, datele, atestatul electronic al atributelor și configurațiile utilizatorului;

7) să exercite dreptul utilizatorului la portabilitatea datelor.

(6) În special, portofelele pentru identitatea digitală:

1) permit utilizarea unor protocoale și interfețe comune:

a) pentru emiterea datelor de identificare personală, a atestatelor electronice calificate și necalificate ale atributelor sau a certificatelor calificate și necalificate către portofelul pentru identitatea digitală;

b) pentru ca beneficiarii să solicite și să valideze date de identificare personală și atestate electronice ale atributelor;

c) pentru partajarea și prezentarea către beneficiari a datelor de identificare personală, a atestatului electronic al atributelor sau a datelor conexe divulgate selectiv online și, după caz, în mod offline;

d) pentru a realiza integrarea în condiții de siguranță a utilizatorului prin utilizarea unui mijloc de identificare electronică în modul stabilit de Guvern

e) pentru interacțiunea între portofelele pentru identitatea digitală a două persoane în scopul de a primi, a valida și a partaja date de identificare personală și atestate electronice ale atributelor într-un mod securizat;

f) pentru autentificarea și identificarea beneficiarilor prin punerea în aplicare a mecanismelor de autentificare în conformitate cu art. 6;

g) pentru ca beneficiarii să verifice autenticitatea și valabilitatea portofelelor pentru identitatea digitală;

h) pentru a solicita unui beneficiar să șteargă datele cu caracter personal în temeiul art. 17 al Legii nr. 195/2024 privind protecția datelor cu caracter personal;

i) pentru a semnala un beneficiar autorității naționale pentru protecția datelor cu caracter personal în cazul în care se primește o cerere de date presupus ilegală sau suspectă;

j) pentru crearea de semnături sau sigilii electronice calificate prin intermediul dispozitivelor de creare a semnăturilor electronice sau a sigiliilor electronice calificate;

2) nu oferă prestatorilor de servicii de încredere care furnizează atestate electronice ale atributelor nicio informație cu privire la utilizarea respectivelor atestate electronice;

3) asigură faptul că beneficiarii pot fi autentificați și identificați prin punerea în aplicare a unor mecanisme de autentificare în conformitate cu art. 6;

4) îndeplinesc cerințele prevăzute la art. 12 în ceea ce privește nivelul de asigurare ridicat, în special în ceea ce privește cerințele privind dovedirea și verificarea identității, precum și gestionarea și autentificarea mijloacelor de identificare electronică;

5) în cazul atestatelor electronice ale atributelor cu politici de divulgare încorporate, pune în aplicare mecanismul adecvat pentru a informa utilizatorul că beneficiarul sau utilizatorul portofelului pentru identitatea digitală care solicită atestatul electronic al atributelor în cauză are permisiunea de a accesa astfel de atestate;

6) asigură faptul că datele de identificare personală, care sunt disponibile din sistemul de identificare electronică în cadrul căruia este furnizat portofelul pentru identitatea digitală, reprezintă în mod unic persoana fizică, persoana juridică sau persoana fizică ce reprezintă persoana fizică sau juridică și sunt asociate cu respectivul portofel pentru identitatea digitală;

7) oferă tuturor persoanelor fizice posibilitatea de a semna prin intermediul semnăturilor electronice calificate în mod implicit și gratuit.

(7) Furnizorii de portofele pentru identitatea digitală informează utilizatorii, fără întârziere, despre orice încălcare a securității care le-ar fi putut compromite total sau parțial portofelul pentru identitatea digitală sau conținutul lui, în special dacă portofelul pentru identitatea digitală al utilizatorilor a fost suspendat sau revocat în conformitate cu art. 9.

(8) Fără a aduce atingere art. 10, Guvernul poate să prevadă, funcționalități suplimentare ale portofelelor pentru identitatea digitală, inclusiv interoperabilitatea cu mijloacele naționale de identificare electronică existente. Aceste funcționalități suplimentare trebuie să fie conforme cu prezentul articol.

(9) Furnizorii de portofele pentru identitatea digitală pun la dispoziție cu titlu gratuit mecanisme de validare pentru:

a) a asigura faptul că autenticitatea și valabilitatea portofelelor pentru identitatea digitală pot fi verificate;

b) a permite utilizatorilor să verifice autenticitatea și valabilitatea identității beneficiarilor înregistrați în conformitate cu art. 6.

(10) Furnizorii de portofele pentru identitatea digitală se asigură că valabilitatea portofelului pentru identitatea digitală poate fi revocată în următoarele circumstanțe:

a) la cererea explicită a utilizatorului;

b) în cazul în care a fost compromisă securitatea portofelului pentru identitatea digitală;

c) în caz de deces al utilizatorului sau de încetare a activității persoanei juridice.

(11) Furnizorii de portofele pentru identitatea digitală se asigură că utilizatorii pot solicita cu ușurință asistență tehnică și pot raporta problemele tehnice sau orice alte incidente care au impact negativ asupra utilizării portofelului pentru identitatea digitală.

(12) Portofelele pentru identitatea digitală sunt furnizate în cadrul unui sistem de identificare electronică având nivelul de asigurare ridicat.

(13) Portofelele pentru identitatea digitală sunt proiectate și dezvoltate în conformitate cu principiul securității încă din stadiul conceperii, prin integrarea unor

măsuri tehnice și organizatorice adecvate care să asigure confidențialitatea, integritatea, disponibilitatea și autenticitatea datelor și serviciilor asociate, pe întregul ciclu de viață al portofelului.

(14) Portofelele pentru identitatea digitală se emit, se utilizează și sunt revocate în mod gratuit pentru toate persoanele fizice.

(15) Utilizatorii au controlul deplin asupra utilizării portofelului lor pentru identitatea digitală și asupra datelor din acesta. Furnizorul portofelului pentru identitatea digitală nu colectează informații cu privire la utilizarea portofelului pentru identitatea digitală care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul pentru identitatea digitală și nici nu combină date de identificare personală sau orice alte date cu caracter personal stocate sau legate de utilizarea portofelului pentru identitatea digitală cu date cu caracter personal provenind de la orice alte servicii oferite de respectivul furnizor sau de la servicii furnizate de terți care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul pentru identitatea digitală, cu excepția cazului în care utilizatorul a solicitat în mod expres contrariul. Datele cu caracter personal legate de punerea la dispoziție de portofele pentru identitatea digitală sunt păstrate separate logic de orice alte date deținute de furnizorul de portofele pentru identitatea digitală.

(16) Utilizarea portofelelor pentru identitatea digitală este voluntară. Accesul la serviciile publice și private, accesul la piața muncii și libertatea de a desfășura o activitate comercială nu sunt în niciun fel restricționate sau permise în condiții mai dezavantajoase pentru persoanele fizice sau juridice care nu utilizează portofelele pentru identitatea digitală. Accesul la serviciile publice și private rămâne posibil prin alte mijloace de identificare și autentificare existente.

(17) Cadrul tehnic al portofelului pentru identitatea digitală:

a) nu permite furnizorilor de atestate electronice ale atributelor sau oricărei alte părți, după emiterea atestatelor atributelor, să obțină date care permit urmărirea, conectarea sau corelarea tranzacțiilor sau a comportamentul utilizatorului sau obținerea în alt mod de cunoștințe privind tranzacțiile sau comportamentul utilizatorului, cu excepția cazului în care utilizatorul autorizează în mod explicit acest lucru;

b) permite aplicarea unor tehnici de protecție a vieții private care asigură imposibilitatea stabilirii unei legături, în cazul în care atestarea atributelor nu necesită identificarea utilizatorului.

(18) Orice prelucrare a datelor cu caracter personal efectuată furnizorii de portofele pentru identitatea digitală se efectuează în conformitate cu prevederile Legii nr. 195/2024 privind protecția datelor cu caracter personal, aplicând măsuri adecvate și eficace de protecție a datelor.

(19) Organismul de supraveghere publică, printr-un canal securizat și într-un format care permite prelucrarea automată, semnat electronic sau sigilat electronic, fără întârzieri nejustificate, informațiile privind:

a) mecanismul de întocmire și menținere a listei beneficiarilor înregistrați care recurg la portofelele pentru identitatea digitală în conformitate cu art. 6 și localizarea acestei liste;

b) lista furnizorilor portofelelor pentru identitatea digitală;

c) organismele din sectorul public responsabile de asigurarea faptului că datele de identificare personală sunt asociate cu portofelul pentru identitatea digitală în conformitate cu alin. (6) pct. 6);

d) mecanismul care permite validarea datelor de identificare personală menționate la alin. (6) pct. 6) și a identității beneficiarilor;

e) mecanismul de validare a autenticității și valabilității portofelelor pentru identitatea digitală.

(20) Dispozițiile art. 24 alin. (4) pct. 2) și pct. 4)-10) sunt aplicabile și furnizorilor de portofele pentru identitatea digitală.

(21) Se asigură accesibilitatea portofelelor pentru identitatea digitală pentru ca persoanele cu dizabilități să le poată utiliza în aceleași condiții ca și ceilalți utilizatori.

(22) Atunci când furnizorii de portofele pentru identitatea digitală și emitenții de mijloace de identificare electronică acționează cu titlu comercial sau profesional și utilizează servicii de platformă esențiale în scopul sau în cursul furnizării de servicii specifice portofelelor pentru identitatea digitală și de mijloace de identificare electronică utilizatorilor finali, sunt utilizatori comerciali, controlorii de acces le permit, în special, să beneficieze în mod efectiv de interoperabilitatea cu aceleași componente ale sistemului de operare, ale hardware-ului sau ale software-ului, precum și să aibă acces la respectivele componente în vederea asigurării interoperabilității. Interoperabilitatea efectivă și accesul menționate anterior sunt permise cu titlu gratuit și indiferent dacă componentele de hardware sau de software fac parte din sistemul de operare, în aceleași condiții în care respectivele componente îi sunt disponibile respectivului controlor de acces sau sunt folosite de acesta atunci când furnizează astfel de servicii.

(23) În scopul furnizării portofelelor pentru identitatea digitală, portofelelor pentru identitatea digitală și sistemelor de identificare electronică în cadrul cărora sunt furnizate nu li se aplică cerințele prevăzute la art. 16.

Articolul 6. Beneficiarii portofelului pentru identitatea digitală

(1) În cazul în care un beneficiar intenționează să recurgă la portofele pentru identitatea digitală pentru furnizarea de servicii publice sau private prin intermediul interacțiunii digitale, beneficiarul se înregistrează în lista beneficiarilor din Republica Moldova gestionată de organismul de supraveghere.

(2) Procesul de înregistrare se desfășoară prin intermediul Portalului guvernamental integrat EVO și este eficient din punctul de vedere al costurilor și proporțional cu riscurile, iar beneficiarul furnizează cel puțin:

a) informațiile necesare pentru autentificarea în portofelele pentru identitatea digitală, informații care includ cel puțin numele beneficiarului și numărul său de înregistrare de stat;

b) datele de contact ale beneficiarului;

c) utilizarea preconizată a portofelelor pentru identitatea digitală, inclusiv menționarea datelor pe care beneficiarul urmează să le solicite utilizatorilor.

(3) Beneficiarii nu solicită utilizatorilor să furnizeze alte date decât cele menționate în temeiul alin. (2) lit. (c).

(4) Prevederile alin. (1) și (2) nu aduc atingere cadrului normativ aplicabil prestării serviciilor specifice.

(5) Organismul de supraveghere pune la dispoziția publicului online informațiile menționate la alin. (2), într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.

(6) Beneficiarii înregistrați în conformitate cu prezentul articol informează fără întârziere organismul de supraveghere cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alin. (2).

(7) Atunci când intenționează să recurgă la portofele pentru identitatea digitală, beneficiarii se identifică față de utilizator.

(8) Beneficiarii sunt responsabili de îndeplinirea procedurii de autentificare și validare a datelor de identificare personală și de atestare electronică a atributelor solicitate în cadrul portofelelor pentru identitatea digitală. Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care cadrul normativ aplicabil nu impune identificarea utilizatorului.

(9) Intermediarii care acționează în numele beneficiarilor sunt considerați beneficiari și nu stochează date cu privire la conținutul tranzacției.

Articolul 7. Certificarea portofelelor pentru identitatea digitală

(1) Conformitatea portofelelor pentru identitatea digitală, precum și a sistemului de identificare electronică în cadrul căruia acestea sunt furnizate, cu cerințele prevăzute la art. 5, precum și cu standardele și specificațiile tehnice stabilite de Guvern, se certifică de către organisme de evaluare a conformității acreditate.

(2) Certificarea realizată în temeiul la alin. (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția efectuării unei evaluări a vulnerabilității la fiecare doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în timp util, certificarea este anulată.

(3) Respectarea cerințelor stabilite la art. 5 referitoare la operațiunile de prelucrare a datelor cu caracter personal poate să fie certificată în temeiul art. 42 din Legea nr. 195/2024 privind protecția datelor cu caracter personal.

Articolul 8. Publicarea unei liste a portofelelor pentru identitatea digitală certificate

(1) Organismul de supraveghere asigură menținerea și publicarea listei portofelelor pentru identitatea digitală furnizate și certificate în conformitate cu prezenta lege.

(2) Lista portofelelor pentru identitatea digitală se menține într-o formă care poate fi citită automat și include cel puțin:

a) certificatul și raportul de evaluare a certificării portofelului pentru identitatea digitală certificat;

b) o descriere a sistemului de identificare electronică în cadrul căruia este furnizat portofelul pentru identitatea digitală;

c) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la partea care furnizează portofelul pentru identitatea digitală;

d) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică;

e) dispozițiile pentru suspendarea sau revocarea sistemului de identificare electronică, a autentificării sau a părților compromise în cauză.

(3) Orice parte interesată poate transmite organismului o cerere de eliminare de pe lista menționată la alin. (1) a unui portofel pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia este furnizat acesta.

(4) În cazul în care informațiile înregistrare în lista menționată la alin. (1) se modifică, furnizorii portofelelor pentru identitatea digitală furnizează organismului de supraveghere informațiile actualizate.

(5) Organismul de supraveghere asigură actualizarea listei portofelelor pentru identitatea digitală certificate în termen de o lună de la primirea unei cereri în temeiul alin. (3) sau a informațiilor actualizate în temeiul alin. (4).

Articolul 9. Încălcarea securității portofelelor pentru identitatea digitală

(1) În cazul în care portofelele pentru identitatea digitală furnizate în temeiul art. 5, mecanismele de validare menționate la art. 5 alin. (8) sau sistemul de identificare electronică în cadrul căruia sunt furnizate portofelele pentru identitatea digitală fac obiectul unei încălcări a securității sau sunt compromise parțial într-un mod care afectează fiabilitatea lor sau a altor portofele pentru identitatea digitală, furnizorii portofelelor pentru identitatea digitală suspendă fără întârziere nejustificată furnizarea și utilizarea portofelelor pentru identitatea digitală. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați, precum și organismul de supraveghere.

(2) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) nu este remediată în termen de trei luni de la suspendare, furnizorii portofelelor pentru identitatea digitală retrag portofelele pentru identitatea digitală și le revocă valabilitatea. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați, precum și organismul de supraveghere cu privire la retragere.

(3) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) este remediată, furnizorii portofelelor pentru identitatea digitală reiau furnizarea și utilizarea portofelelor pentru identitatea digitală și informează fără întârzieri nejustificate utilizatorii și beneficiarii afectați, precum și organismul de supraveghere.

(4) Organismul de supraveghere, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la art. 8.

Articolul 10. Utilizarea transfrontalieră a portofelelor pentru identitatea digitală

(1) În cazul în care autoritățile sau instituțiile publice solicită identificarea sau autentificarea electronică pentru accesul la servicii publice online, acestea acceptă și utilizarea portofelelor pentru identitatea digitală furnizate în statele membre ale Uniunea Europeană, în măsura în care acestea sunt emise în conformitate cu cerințele stabilite prin legislația Uniunii Europene și pot fi verificate prin mecanisme tehnice interoperabile.

(2) Furnizorii de servicii din sectorul privat care, în temeiul cadrului normativ sau al obligațiilor contractuale, solicită identificarea sau autentificarea electronică a utilizatorilor acceptă utilizarea portofelelor pentru identitatea digitală, inclusiv a celor furnizate în statele membre ale Uniunea Europeană, la solicitarea utilizatorului și în limitele datelor necesare pentru prestarea serviciului.

(3) Portofelele pentru identitatea digitală furnizate în Republica Moldova pot fi utilizate pentru identificare și autentificare electronică în alte state, în baza acordurilor internaționale încheiate între Republica Moldova și statele respective ori cu organizațiile internaționale relevante.

(4) Organismul de supraveghere efectuează, la fiecare 24 de luni de la implementarea portofelelor pentru identitatea digitală, o evaluare a cererii, disponibilității și posibilității de utilizare a acestora, ținând seama de criterii precum gradul de adoptare de către utilizatori, disponibilitatea serviciilor, evoluțiile tehnologice, evoluția modelelor de utilizare și cererea utilizatorilor, iar rezultatele evaluării sunt publicate de către organismul de supraveghere pe pagina sa oficială.

Secțiunea a 2-a
Sisteme de identificare electronică

Articolul 11. Recunoașterea reciprocă

(1) Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică și o autentificare conform cadrului normativ al Republicii Moldova pentru a accesa un serviciu prestat online de un organism din sectorul public, mijloacele de identificare electronică emise într-un stat membru al Uniunii Europene sunt recunoscute în Republica Moldova 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 de sisteme de identificare electronică publicată de Comisia Europeană;

(b) nivelul de asigurare al respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare substanțial sau ridicat, conform clasificării prevăzute de lege;

(c) organismele din sectorul public care furnizează serviciul online să fie capabile să verifice validitatea și integritatea mijloacelor de identificare electronică emise într-un stat membru al Uniunii Europene.

(2) Organismul de supraveghere este responsabil pentru publicarea ghidurilor și procedurilor privind recunoașterea mijloacelor de identificare electronică transfrontaliere și pentru actualizarea acestora ori de câte ori apar modificări în lista sistemelor recunoscute sau în cerințele de securitate.

(3) Orice serviciu public online care acceptă autentificarea transfrontalieră trebuie să asigure transparența criteriilor și să informeze utilizatorii despre condițiile de recunoaștere și nivelul de asigurare necesar al mijloacelor de identificare electronice.

Articolul 12. Niveluri de asigurare ale mijloacelor de identificare electronică

(1) Un sistem de identificare electronică poate prevedea nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv.

(2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv:

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;

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;

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 frauduloasă a identității.

(3) Specificațiile tehnice, standardele și procedurile minime, în raport cu care sunt determinate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică se stabilesc de către Guvern. Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente:

a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică;

b) procedura pentru emiterea mijloacelor de identificare electronică solicitate;

c) mecanismul de autentificare, prin care persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar;

d) entitatea care emite mijloacele de identificare electronică;

e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și

f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise.

Articolul 13. Lista sistemelor naționale de identificare electronică

(1) Deținătorul unui sistem de identificare electronică este obligat să transmită organismului de supraveghere o notificare care să includă, fără întârzieri nejustificate, următoarele informații, precum și orice modificări ulterioare ale acestora:

1) o descriere a sistemului de identificare electronică notificat, incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului;

2) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la următoarele aspecte:

a) partea care emite mijloacele de identificare electronică; și

b) partea care desfășoară procedura de autentificare;

3) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică;

4) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală;

5) o descriere a modului în care sunt îndeplinite criteriile prevăzute la alin. (2) și specificațiile tehnice, standardele și procedurile pentru nivelurile de asigurare stabilite de Guvern;

6) o descriere a autentificării online;

7) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză.

(2) Organismul de supraveghere publică pe pagina sa oficială o listă a sistemelor de identificare electronică ce au fost notificate în temeiul alin. (1), împreună cu informațiile de bază cu privire la aceste sisteme.

(3) Deținătorul unui sistem de identificare electronică poate solicita organismului de supraveghere eliminarea sistemului său din lista prevăzută la alin. (2).

Articolul 14. Corelarea transfrontalieră a identităților

(1) Atunci când organismele din sectorul public din Republica Moldova acționează în calitate de beneficiari ai unor servicii transfrontaliere, organismul de supraveghere se asigură că se realizează corelarea fără echivoc a identităților pentru persoanele fizice care utilizează mijloace de identificare electronică sau portofele pentru identitatea digitală.

(2) Guvernul stabilește măsuri tehnice și organizatorice pentru a asigura un nivel ridicat de protecție a datelor cu caracter personal utilizate pentru corelarea identităților și pentru a preveni crearea de profiluri ale utilizatorilor.

Articolul 15. Interoperabilitate

(1) Sistemele naționale de identificare electronică publicate în temeiul art. 13 sunt interoperabile.

(2) Guvernul va stabili cadrul de interoperabilitate care trebuie să îndeplinească următoarele criterii:

a) urmărește să fie neutru din punctul de vedere al tehnologiei și nu acordă prioritate niciuneia dintre soluțiile tehnice specifice pentru identificarea electronică;

b) respectă standardele europene și internaționale, atunci când este posibil;

c) facilitează protecția, începând cu momentul conceperii, a vieții private și a securității;

(3) Cadru de interoperabilitate este alcătuit din următoarele elemente:

a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la art. 12;

b) o trimitere la cerințele tehnice minime referitoare la interoperabilitate;

c) o trimitere la un set minim de date de identificare personală necesare pentru a reprezenta în mod unic o persoană fizică sau juridică sau o persoană fizică ce reprezintă o altă persoană fizică sau o persoană juridică, care sunt disponibile din sistemele de identificare electronică;

d) regulamentul de procedură;

e) dispoziții referitoare la soluționarea litigiilor; și

f) standarde de securitate operaționale comune.

Articolul 16. Certificarea sistemelor de identificare electronică

(1) Conformitatea sistemelor de identificare electronică cu cerințele privind securitatea cibernetică prevăzute în prezenta lege, inclusiv conformitatea cu cerințele relevante în materie de securitate cibernetică prevăzute la art. 12 alin. (2) în ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică, este certificată de organismele de evaluare a conformității.

(2) Certificarea efectuată în temeiul alin. (1) este valabilă pentru o perioadă de cinci ani, cu condiția să se efectueze o evaluare a vulnerabilității o dată la doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în termen de trei luni de la identificarea sa, certificarea este anulată.

Capitolul III
SERVICII DE ÎNCREDERE
SECȚIUNEA 1
Dispoziții generale

Articolul 17. Răspunderea și sarcina probei

(1) 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 prezenta lege. Orice persoană fizică sau juridică ce a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezenta lege de către un prestator de servicii de încredere are dreptul de a solicita despăgubiri în conformitate cu cadrul normativ aplicabil.

(2) 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 alin. (1).

(3) Intenția sau neglijența din partea unui prestator de servicii de încredere calificat este prezumată, cu excepția cazului în care respectivul prestator de servicii de încredere calificat dovedește că prejudiciul menționat la alin. (1) nu a intervenit din intenția sau din neglijența sa.

(4) 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.

Articolul 18. Aspecte internaționale

(1) Serviciile de încredere prestate de prestatori de servicii de încredere cu sediul în orice stat membru al Uniunii Europene sau orice altă țară cu care Republica Moldova a încheiat un acord de recunoaștere reciprocă sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați cu sediul în Republica Moldova.

(2) Acordurile menționate la alin. (1) garantează că cerințele aplicabile prestatorilor de servicii de încredere calificați cu sediul în Republica Moldova și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de servicii de încredere din țara terță în cauză și de serviciile de încredere pe care le prestează.

(3) Acordurile menționate la alin. (1) garantează că serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați cu sediul în Republica Moldova sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță cu care a fost încheiat acordul.

Articolul 19. Accesibilitatea pentru persoanele cu dizabilități și cu nevoi speciale

Mijloacele de identificare electronică, prestarea serviciilor de încredere și furnizarea produselor destinate utilizatorului final care sunt utilizate pentru prestarea serviciilor respective sunt furnizate într-un limbaj clar și inteligibil și în conformitate cu Convenția Națiunilor Unite privind drepturile persoanelor cu handicap, fiind astfel accesibile și persoanelor care se confruntă cu limitări funcționale, cum ar fi persoanele în vârstă, și persoanelor cu acces limitat la tehnologiile digitale.

Secțiunea a 2-a
Servicii de încredere necalificate

Articolul 20. Cerințe pentru prestatorii de servicii de încredere necalificați

Un prestator de servicii de încredere necalificat care prestează servicii de încredere necalificate:

1) dispune de politici adecvate și ia măsurile corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere necalificat, care, includ cel puțin măsuri referitoare la:

a) procedurile de înregistrare și de integrare legate de un serviciu de încredere;

b) controalele procedurale sau administrative necesare pentru prestarea de servicii de încredere;

c) gestionarea și implementarea serviciilor de încredere;

2) notificarea organismului de supraveghere, persoanelor afectate care pot fi identificate, publicului – dacă chestiunea este de interes public –, și, după caz, altor autorități competente relevante, cu privire la orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la alin. 1) care are impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore din momentul în care a luat cunoștință de orice încălcare a securității sau perturbare.

Secțiunea a 3-a

Servicii de încredere calificate

Articolul 21. Supravegherea prestatorilor de servicii de încredere calificați

(1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin la fiecare 24 de luni, de către un organism de evaluare a conformității. Auditul confirmă că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezenta lege și la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică. 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) Prestatorii de servicii de încredere calificați informează organismul de supraveghere cu cel puțin o lună înainte de un audit planificat și, la cerere, îi permit organismului de supraveghere să participe în calitate de observator.

(3) Fără a aduce atingere alin. (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 calificate pe care le prestează îndeplinesc cerințele prevăzute în prezenta lege. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează, fără întârzieri nejustificate, autoritatea națională pentru protecția datelor cu caracter personal.

(4) În cazul în care prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în prezenta lege, organismul de supraveghere îi solicită să remedieze situația într-un termen stabilit, dacă este cazul.

(5) În cazul în care prestatorul respectiv nu remediază situația, dacă este cazul în termenul stabilit de organismul de supraveghere, acesta din urmă, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.

(6) În cazul în care autoritatea competentă la nivel național în domeniul securității cibernetice informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.

(7) În cazul în care autoritatea națională pentru protecția datelor cu caracter personal informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în Legea nr. 195/2024 privind protecția datelor cu caracter personal, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele

respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.

(8) Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la retragerea statutului de calificat, al său sau al serviciului în cauză.

Articolul 22. Inițierea unui serviciu de încredere calificat

(1) În cazul în care prestatorii de servicii de încredere intenționează să înceapă prestarea unui serviciu de încredere calificat, aceștia informează organismul de supraveghere cu privire la intenția lor, însoțită de un raport de evaluare a conformității emis de un organism de evaluare a conformității, care confirmă îndeplinirea cerințelor prevăzute în prezenta lege și la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică.

(2) Organismul de supraveghere verifică dacă prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezenta lege și, în special, cerințele pentru prestatorii de servicii de încredere calificați și pentru serviciile de încredere calificate prestate de aceștia.

(3) În cazul în care organismul de supraveghere constată că prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezenta lege, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta și publică informațiile referitoare la prestatorul respectiv în lista sigură.

(4) 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 urmează să se încheie verificarea.

(5) Prestatorii de servicii de încredere calificați pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în lista sigură.

(6) Prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene obțin statutul de prestator de servicii de încredere calificat în Republica Moldova în baza notificării privind intenția de a presta servicii de încredere calificate pe teritoriul Republicii Moldova, expediată organismul de supraveghere, fără necesitatea de a fi supuși verificărilor prevăzute pentru prestatorii naționali.

(7) Organismul de supraveghere, în termen de 10 zile lucrătoare de la data recepționării notificării, verifică statutul prestatorului de servicii de încredere în lista sigură a statului membru al Uniunii Europene și, în cazul confirmării statutului, asigură includerea prestatorului în lista respectivă.

(8) În cazul retragerii statutului de prestator de servicii de încredere calificat într-un stat membru al Uniunii Europene, organismul de supraveghere radiază

înregistrarea acestuia din Registrul de evidență a prestatorilor de servicii de încredere calificați.

Articolul 23. Lista sigură

(1) Organismul de supraveghere instituie, menține și publică o listă sigură care include informații referitoare la prestatorii de servicii de încredere calificați și la serviciile de încredere calificate prestate de aceștia.

(2) Lista sigură este instituită, menținută și publicată într-un mod securizat, fiind semnată sau sigilată electronic și pusă la dispoziție publicului într-un format adecvat prelucrării automate a datelor.

Articolul 24. Cerințe pentru prestatorii de servicii de încredere calificați

(1) Atunci când emite un certificat calificat sau un atestat electronic calificat al atributelor, un prestator de servicii de încredere calificat verifică identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia urmează să i se emită certificatul calificat sau atestatul electronic calificat al atributelor.

(2) Verificarea identității menționată la alin. (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora atunci când este necesar, în conformitate cu actele de punere în aplicare aprobate de Guvern:

a) prin intermediul portofelului pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la art. 12 în ceea ce privește nivelul de asigurare ridicat;

b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu lit. (a), (c) sau (d);

c) prin utilizarea altor metode de identificare care asigură identificarea persoanei cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității;

d) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu cadrul normativ aplicabil.

(3) Verificarea atributelor menționată la alin. (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, atunci când este necesar, în conformitate cu actele de punere în aplicare stabilite de Guvern:

a) prin intermediul portofelului pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la art. 12 în ceea ce privește nivelul de asigurare ridicat;

b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu alin. (3) lit. (a), (c) sau (d);

c) prin intermediul unui atestat electronic calificat al atributelor;

d) prin utilizarea altor metode, care asigură verificarea atributelor cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității;

e) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cadrul normativ aplicabil.

(4) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate:

1) informează organismul de supraveghere cu cel puțin o lună înainte de punerea în aplicare a oricărei modificări în prestarea serviciilor sale de încredere calificate sau cu cel puțin trei luni înainte în cazul în care intenționează să înceteze activitățile respective;

2) 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;

3) în ceea ce privește riscul de răspundere pentru daune în conformitate cu art. 17, menține suficiente resurse financiare și/sau obține o asigurare de răspundere adecvată, în conformitate cu dreptul intern;

4) înainte de stabilirea unei relații contractuale, informează, în mod clar, cuprinzător și ușor accesibil, într-un spațiu accesibil publicului și în mod individual, orice persoană care dorește să utilizeze un serviciu de încredere calificat în ceea ce privește clauzele și condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia;

5) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea, inclusiv prin folosirea unor tehnici criptografice adecvate;

6) utilizează sisteme demne de încredere pentru a stoca datele care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât:

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

b) numai persoanele autorizate să poată introduce și modifica datele stocate;

c) autenticitatea datelor să poată fi controlată;

7) dispune de politici adecvate și ia măsuri corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere calificat, inclusiv cel puțin măsuri referitoare la următoarele aspecte:

a) procedurile de înregistrare și de integrare legate de un serviciu;

b) controalele procedurale sau administrative;

c) gestionarea și implementarea serviciilor;

8) notifică organismului de supraveghere, persoanelor afectate care pot fi identificate, altor organisme competente relevante, după caz, și, la cererea organismului de supraveghere, publicului, dacă chestiunea este de interes public, orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la pct. 7 care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la producerea incidentului;

9) ia măsuri adecvate împotriva falsificării, furtului sau însușirii ilegale de date ori împotriva ștergerii sau modificării neautorizate a datelor sau a acțiunii neautorizate de a le face inaccesibile;

10) înregistrează și menține accesibile atât timp cât este necesar, după încetarea activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către acesta, în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic;

11) are un plan actualizat pentru a asigura, în cazul încetării serviciului, continuitatea serviciului conform dispozițiilor verificate de organismul de supraveghere în conformitate cu art. 64 alin. (3) pct. 2) lit. f);

12) în cazul prestatorilor de servicii de încredere calificați care eliberează certificate calificate, instituie și actualizează permanent o bază de date a certificatelor.

(5) Organismul de supraveghere poate solicita informații în plus față de informațiile notificate în temeiul alin. (4) sau rezultatul unei evaluări a conformității și poate stabili anumite condiții pentru acordarea permisiunii de a pune în aplicare modificările preconizate ale serviciilor de încredere calificate. 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 urmează să se încheie verificarea.

(6) 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.

(7) Prestatorii de servicii de încredere calificați care emit certificate calificate 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.

(8) Alin. (6) și (7) se aplică în mod corespunzător revocării atestatelor electronice calificate ale atributelor.

Articolul 25. Recunoașterea serviciilor de încredere calificate furnizate de prestatori de servicii calificate din statele membre ale Uniunii Europene

(1) Semnăturile electronice calificate bazate pe un certificat calificat emis într-un stat membru al Uniunii Europene și sigiliile electronice calificate bazate pe un certificat calificat emis într-un stat membru al Uniunii Europene sunt recunoscute drept semnături electronice calificate și, respectiv, drept sigilii electronice calificate în Republica Moldova.

(2) Dispozitivele de creare a semnăturilor electronice calificate și dispozitivele de creare a sigiliilor electronice calificate certificate într-un stat membru al Uniunii Europene sunt recunoscute drept dispozitive de creare a semnăturilor electronice calificate și, respectiv, drept dispozitive de creare a sigiliilor electronic calificate în Republica Moldova.

(3) Un certificat calificat pentru semnăturile electronice, un certificat calificat pentru sigilii electronice, un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță furnizat într-un stat membru al Uniunii Europene este recunoscut drept certificat calificat pentru semnăturile electronice, drept certificat calificat pentru sigilii electronice, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și, respectiv, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță în Republica Moldova.

(4) Un serviciu de validare calificat pentru semnături electronice calificate și un serviciu de validare calificat pentru sigilii electronice calificate furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu de validare calificat pentru semnături electronice calificate și, respectiv, drept serviciu de validare calificat pentru sigilii electronice calificate în Republica Moldova.

(5) Un serviciu calificat de păstrare a semnăturilor electronice calificate și un serviciu calificat de păstrare a sigiliilor electronice calificate furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu calificat de păstrare a semnăturilor electronice calificate și, respectiv, drept serviciu calificat de păstrare a sigiliilor electronice calificate în Republica Moldova.

(6) O marcă temporală electronică calificată furnizată într-un stat membru al Uniunii Europene este recunoscută drept marcă temporală electronică calificată în Republica Moldova.

(7) Un certificat calificat pentru autentificarea unui site internet emis într-un stat membru al Uniunii Europene este recunoscut drept certificat calificat pentru autentificarea unui site internet în Republica Moldova.

(8) Un serviciu de distribuție electronică înregistrată calificat furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu de distribuție electronică înregistrată calificat în Republica Moldova.

(9) Un atestat electronic calificat al atributelor emis într-un stat membru al Uniunii Europene este recunoscut drept atestat electronic calificat al atributelor în Republica Moldova.

(10) Un serviciu calificat de arhivare electronică furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu calificat de arhivare electronică în Republica Moldova.

(11) Un registru electronic calificat furnizat într-un stat membru al Uniunii Europene este recunoscut drept registru electronic calificat în Republica Moldova.

Secțiunea a 4-a
Semnătura electronică

Articolul 26. 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.

Articolul 27. Cerințe pentru semnături electronice avansate

(1) 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 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.

(2) În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele referitoare la semnăturile electronice avansate prevăzute la alin. (1).

Articolul 28. Semnăturile electronice în cadrul serviciilor publice

(1) În cadrul prestării serviciilor publice electronice de către organismele din sectorul public sau în numele acestora, atunci când cadrul normativ aplicabil solicită aplicarea unei semnături electronice, aceasta se realizează prin utilizarea semnăturii electronice calificate.

(2) Semnătura electronică calificată utilizată în cadrul serviciilor publice produce efecte juridice echivalente semnăturii olografe și este recunoscută de către toate autoritățile și instituțiile publice.

(3) Organismele din sectorul public nu pot solicita, pentru utilizarea serviciilor publice electronice, un nivel de securitate al semnăturii electronice mai ridicat decât cel al semnăturii electronice calificate.

Articolul 29. Certificate calificate pentru semnăturile electronice

(1) Certificatele calificate pentru semnăturile electronice îndeplinesc cerințele prevăzute la art. 30.

(2) Certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la art. 30.

(3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate.

(4) Prestatorul de servicii de încredere suspendă valabilitatea certificatelor calificate pentru semnăturile electronice la cererea titularilor acestora.

(5) În cazul în care un certificat calificat pentru semnătura electronică a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare, iar 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) 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.

(7) În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la art. 30.

Articolul 30. Cerințe pentru certificatele calificate pentru semnături electronice

Certificatele calificate pentru semnături electronice conțin:

1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice;

2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin:

a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat;

b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat;

3) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

4) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice;

5) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului;

6) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de încredere calificat;

7) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent;

8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 7);

9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii;

10) 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.

Articolul 31. Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate

(1) Dispozitivele de creare a semnăturilor electronice calificate îndeplinesc cerințele prevăzute la alin. (2) și (3).

(2) Dispozitivele de creare a semnăturilor electronice calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că:

a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil;

b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată;

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;

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.

(3) 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.

(4) Generarea sau gestionarea datelor de creare a semnăturii electronice sau duplicarea unor astfel de date de creare a semnăturii în scopul creării unei copii de rezervă se realizează numai în numele semnatarului și la cererea acestuia și de către un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a semnăturii electronice la distanță.

(5) În cazul în care un dispozitiv de creare a semnăturilor electronice calificat îndeplinește standardele stabilite de Guvern, se presupune că acesta respectă cerințele prevăzute la alin. (2) și (3).

Articolul 32. Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță

Gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță în calitate de serviciu calificat se efectuează numai de către un prestator de servicii de încredere calificat care:

1) generează sau gestionează datele de creare a semnăturilor electronice în numele semnatarului;

2) duplică datele de creare a semnăturilor electronice numai în scopul creării unei copii de rezervă, cu condiția să fie îndeplinite următoarele cerințe:

a) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale;

b) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului;

3) respectă toate cerințele identificate în raportul de certificare a dispozitivului calificat specific de creare a semnăturii electronice la distanță, emis în temeiul art. 33.

Articolul 33. Certificarea dispozitivelor de creare a semnăturilor electronice calificate

(1) Conformitatea dispozitivelor de creare a semnăturii electronice calificate cu cerințele prevăzute la art. 31 alin. (2) și (3) este certificată de organisme de evaluare a conformității.

(2) Certificarea menționată la alin. (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 stabilite de Guvern; sau

b) un alt proces decât procesul prevăzut la lit. a), cu condiția ca acest proces să utilizeze niveluri de securitate comparabile și ca organisme de evaluare a conformității să notifice organismului de supraveghere respectivul proces. Procesul respectiv poate fi utilizat numai în absența standardelor menționate la lit. a) sau dacă un proces de evaluare de securitate menționat la lit. a) este în curs de desfășurare.

(3) Perioada de valabilitate a certificării menționate la alin. (1) nu depășește cinci ani, cu condiția efectuării unei evaluări a vulnerabilităților la fiecare doi ani. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate, certificarea este anulată.

(4) Organismul de supraveghere publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate.

Articolul 34. Cerințe pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate calificate

(1) Procesul de validare a unei semnături electronice calificate sau a unei semnături electronice avansate bazate pe un certificat calificat confirmă validitatea unei semnături electronice cu următoarele condiții:

a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu art. 30;

b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;

c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar;

d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului;

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

f) integritatea datelor semnate nu a fost compromisă;

g) cerințele prevăzute la art. 27 au fost îndeplinite la momentul semnării.

(2) Suplimentar cerințelor prevăzute la alin. (1), procesul de validare a unei semnături electronice calificate include verificarea faptului că semnătura electronică a fost creată prin intermediul unui dispozitiv calificat de creare a semnăturilor electronice.

(3) Sistemul utilizat pentru validarea semnăturii electronice calificate sau a semnăturii electronice avansate bazate pe un certificat calificat furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.

(4) În cazul în care validarea semnăturilor electronice calificate sau a sau a semnăturilor electronice avansate bazate pe certificate calificate respectă standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1), inclusiv și a celei prevăzute la alin. (2) în cazul semnăturilor electronice calificate .

Articolul 35. Serviciul calificat de validare a semnăturilor electronice calificate

(1) Un serviciu calificat de validare a semnăturilor electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care:

a) realizează validarea în conformitate cu art. 34 alin. (1) și alin. (2); 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.

(2) În cazul în care serviciul calificat de validare pentru semnături electronice calificate îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele de la alin. (1).

Articolul 36. 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 semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.

(2) În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

Secțiunea a 5-a
Sigiliile electronice

Articolul 37. 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 38. Cerințele pentru sigiliile electronice avansate

(1) Un sigiliu electronic avansat îndeplinește următoarele cerințele:

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.

(2) În cazul în care un sigiliu electronic avansat îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

Articolul 39. Sigiliile electronice în cadrul serviciilor publice

(1) În cadrul prestării serviciilor publice electronice de către autoritățile publice și instituții publice sau în numele acestora, atunci când cadrul normativ aplicabil solicită aplicarea unui sigiliu electronic, aceasta se realizează prin utilizarea sigiliului electronic calificat.

(2) Organismele din sectorul public nu pot solicita, pentru utilizarea serviciilor publice electronice, un nivel de securitate al sigiliului electronic mai ridicat decât cel al sigiliului electronic calificat.

Articolul 40. Certificate calificate pentru sigiliul electronic

(1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute art. 41.

(2) Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la art. 41.

(3) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate.

(4) Prestatorul de servicii de încredere suspendă valabilitatea certificatelor calificate pentru sigiliile electronice la cererea titularilor acestora.

(5) În cazul în care un certificat calificat pentru sigiliu electronic a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare, iar 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) Certificatul calificat pentru sigiliu electronic care 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.

(7) În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la art. 41.

Articolul 41. Cerințe pentru certificatele calificate pentru sigiliile electronice

Certificatele calificate pentru sigiliile electronice conțin:

1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru sigilii electronice;

2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin:

a) în cazul unei persoane juridice: denumirea;

b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat;

3) cel puțin numele/prenumele creatorului sigiliului și numărul de identificare de stat;

4) datele de validare a sigiliilor electronice, care corespund datelor de creare a sigiliilor electronice;

5) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului;

6) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat;

7) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent;

8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 7);

9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii;

10) 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.

Articolul 42. Dispozitive de creare a sigiliilor electronice calificate

Dispozițiile art. 31 și 33 privind cerințele aplicabile dispozitivelor de creare a semnăturilor electronice calificate, certificarea acestora și publicarea listei dispozitivelor certificate și calificate se aplică, în mod corespunzător, și dispozitivelor de creare a sigiliilor electronice calificate.

Articolul 43. Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță

Dispozițiile art. 32 privind cerințele aplicabile serviciului calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță se aplică și serviciului calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță.

Articolul 44. Validarea și păstrarea sigiliilor electronice calificate

Dispozițiile art. 34, 35 și 36 privind validarea și păstrarea semnăturilor electronice calificate se aplică și validării și păstrării sigiliilor electronice calificate.

Articolul 45. Cerințe pentru validarea sigiliilor electronice avansate bazate pe certificate calificate

Dispozițiile art. 34 privind cerințele pentru validarea semnăturilor electronice avansate bazate pe certificate calificate se aplică și validării sigiliilor electronice avansate bazate pe certificate calificate.

Secțiunea a 6-a
Mărcile temporale electronice

Articolul 46. 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 47. 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.

(2) În cazul în care legătura dintre dată și oră și date și exactitatea sursei orei indicate îndeplinesc standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

Secțiunea a 7-a
Serviciul de distribuție electronică înregistrată

Articolul 48. 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.

Articolul 49. 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 datelor este indicată printr-o marcă temporală electronică calificată.

(2) În cazul datelor transferate între doi sau mai mulți prestatori de servicii de încredere, cerințele de la alin. (1) lit. (a)-(f) se aplică tuturor prestatorilor de servicii de încredere calificați.

(3) Prestatorii de servicii de distribuție electronică înregistrată calificate pot conveni asupra interoperabilității dintre serviciile de distribuție electronică înregistrată calificate pe care le prestează. Un astfel de cadru de interoperabilitate respectă cerințele prevăzute la alin. (1), iar respectarea acestor cerințe este confirmată de un organism de evaluare a conformității.

(4) În cazul în care procesul de trimitere și primire de date îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

Secțiunea a 8-a
Autentificarea unui site internet

Articolul 50. Cerințe pentru certificatele calificate pentru autentificarea unui site internet

(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute la alin. (2).

(2) Certificatele calificate pentru autentificarea unui site internet conțin:

1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unui site internet;

2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin:

a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat,

b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat;

3) în cazul persoanelor fizice: cel puțin numele/prenumele persoanei căreia i s-a emis certificatul sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

4) în cazul persoanelor juridice: un set unic de date care reprezintă fără echivoc persoana juridică căreia i se emite certificatul, incluzând cel puțin denumirea persoanei juridice căreia i se emite certificatul și, numărul de identificare de stat;

5) adresa persoanei fizice sau juridice căreia i s-a eliberat certificatul;

6) numele domeniului (domeniilor) gestionat(e) de persoana fizică sau juridică căreia i s-a emis certificatul;

7) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului;

8) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat;

9) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent;

10) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 9);

11) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.

(3) Certificatele calificate pentru autentificarea unui site internet emise în conformitate cu alin. (1) sunt recunoscute de furnizorii de browsere web. Furnizorii de browsere web asigură faptul că datele de identitate atestate în certificat și atributele suplimentare atestate sunt afișate într-un mod ușor de recunoscut de către utilizator. Furnizorii de browsere web asigură suport și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet menționate la alin. (1), cu excepția microîntreprinderilor sau a întreprinderilor mici, astfel cum sunt stabilite prin Legea nr. 179/2016 cu privire la întreprinderile mici şi mijlocii, în primii cinci ani de funcționare ca prestatori de servicii de navigare pe internet.

(4) Certificatele calificate pentru autentificarea unui site internet nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alin. (2).

(5) În cazul în care un certificat calificat pentru autentificarea unui site internet îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (2).

Articolul 51. Măsuri de precauție în materie de securitate cibernetică

(1) Furnizorii de browsere web nu iau nicio măsură contrară obligațiilor lor prevăzute la art. 50, în special cerințelor de recunoaștere a certificatelor calificate pentru autentificarea unui site internet și de afișare a datelor de identitate furnizate într-un mod ușor de recunoscut de către utilizator.

(2) Prin derogare de la alin. (1) și numai în cazul unor suspiciuni motivate legate de încălcări ale securității sau de pierderea integrității unui certificat identificat sau a unui set de certificate identificate, furnizorii de browsere web pot lua măsuri de precauție în legătură cu respectivul certificat sau set de certificate.

(3) În cazul în care un furnizor de browsere web ia măsuri de precauție conform alin. (2), furnizorul de browsere web își notifică suspiciunile în scris, fără întârzieri nejustificate, împreună cu o descriere a măsurilor luate pentru a remedia aceste suspiciuni, organismului de supraveghere, entității căreia i-a fost emis certificatul și prestatorului de servicii de încredere calificat care a emis certificatul sau setul de certificate. La primirea unei astfel de notificări, organismul de supraveghere emite furnizorului de browsere web în cauză o confirmare de primire.

(4) Organismul de supraveghere competent investighează, în conformitate cu art. 64 alin. (3) lit. h), aspectele prezentate în notificare. În cazul în care rezultatul investigației respective nu are ca rezultat retragerea statutului de calificat al certificatului, organismul de supraveghere informează furnizorul de browsere web

în consecință și îi solicită acestuia să pună capăt măsurilor de precauție menționate la alin. (2).

Secțiunea a 9-a
Atestatul electronic al atributelor

Articolul 52. Efectele juridice ale atestatului electronic al atributelor

(1) Unui atestat electronic al atributelor nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele privind atestatele electronice calificate ale atributelor.

(2) Un atestat electronic calificat al atributelor și atestatele atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism au același efect juridic ca atestatele emise în mod legal în format tipărit.

(3) Un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică într-un stat membru al Uniunii Europene sau în numele unui astfel de organism este recunoscut drept un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism în Republica Moldova.

Articolul 53. Atestatul electronic al atributelor în serviciile publice

Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este obligatorie în temeiul dreptului intern pentru a accesa un serviciu prestat online de un organism din sectorul public, datele de identificare personală din atestatul electronic al atributelor nu înlocuiesc identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării pentru identificarea electronică, cu excepția cazului în care acest lucru este permis în mod expres de statul membru. Într-un astfel de caz, se acceptă, de asemenea, atestatul electronic calificat al atributelor din alte state membre.

Articolul 54. Cerințe privind atestatul electronic calificat al atributelor

(1) Atestatul electronic calificat al atributelor îndeplinește cerințele prevăzute la alin. (2).

(2) Atestatul electronic calificat al atributelor conține:

1) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic calificat al atributelor;

2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite atestatul electronic calificat al atributelor, incluzând cel puțin:

a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat,

b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat;

3) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

4) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a identifica domeniul de aplicare al atributelor respective;

5) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului;

6) codul de identificare al atestatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat și, în cazurile aplicabile, indicarea sistemului de atestare din care face parte atestatul atributelor;

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

8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la pct. 7);

9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.

(3) Atestatele electronice calificate ale atributelor nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alin. (2).

(4) În cazul în care un atestat electronic calificat al atributelor este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se poate reveni în niciun caz la statutul său anterior.

(5) În cazul în care un atestat electronic calificat al atributelor îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (2).

Articolul 55. Verificarea atributelor în raport cu surse autentice

(1) Organismele din sectorul public care gestionează registre de stat sau alte sisteme informaționale ce constituie surse autentice de date asigură, în limitele competențelor și în conformitate cu cadrul normativ aplicabil, disponibilitatea mecanismelor electronice care permit verificarea atributelor persoanelor fizice și juridice de către prestatorii de servicii de încredere calificați ce emit atestate electronice ale atributelor, la cererea expresă a utilizatorului.

(2) Măsurile prevăzute la alin. (1) se aplică, cel puțin, pentru următoarele categorii de atribute, în măsura în care acestea se bazează pe surse autentice din sectorul public:

a) adresa;

b) vârsta;

c) genul;

d) starea civilă;

e) componența familiei;

f) naționalitatea sau cetățenia;

g) nivelul de studii, titluri și diplome;

h) calificări profesionale, titluri și licențe;

i) împuterniciri și mandate de reprezentare a persoanelor fizice sau juridice;

j) acte permisive;

k) pentru persoanele juridice, datele financiare și datele privind societățile.

Articolul 56. Cerințe privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism

(1) Un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește următoarele cerințe:

1) cerințele prevăzute la alin. (2);

2) cerința ca certificatul calificat care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat al organismului din sectorul public să conțină un set specific de atribute certificate într-o formă adecvată pentru prelucrarea automată, care:

a) indică faptul că organismul emitent este înființat în conformitate cu cadrul normativ aplicabil ca fiind responsabil de sursa autentică pe baza căreia este emis atestatul electronic al atributelor sau ca organism desemnat să acționeze în numele acestuia;

b) furnizează un set de date care reprezintă fără ambiguitate sursa autentică menționată la lit. a); și

c) identifică cadrul normativ menționat la lit. a).

(2) Un atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism conține:

a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism;

b) un set de date care reprezintă fără echivoc organismul public care emite atestatul electronic al atributelor, incluzând cel puțin statul membru în care este stabilit organismul public respectiv și denumirea sa și, după caz, numărul său de înregistrare, astfel cum figurează în registrele oficiale;

c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a identifica domeniul de aplicare al atributelor respective;

e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului;

f) codul de identificare al atestatului, care trebuie să fie unic pentru organismul public emitent și, în cazurile aplicabile, o indicare a sistemului de atestare din care face parte atestatul atributelor;

g) semnătura electronică calificată sau sigiliul electronic calificat al organismului emitent;

h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la lit. g);

i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.

(3) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se mai poate reveni la statutul anterior revocării.

(4) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

(5) Organismele din sectorul public care emit atestate electronice ale atributelor pun la dispoziție o interfață cu portofelele pentru identitatea digitală care sunt furnizate în conformitate cu art. 5.

Articolul 57. Emiterea atestatului electronic al atributelor pentru portofelele pentru identitatea digitală

(1) Furnizorii de atestate electronice ale atributelor oferă utilizatorilor portofelului pentru identitatea digitală posibilitatea de a solicita, de a obține, de a stoca și de a gestiona atestatul electronic al atributelor prin intermediul oricărui portofel pentru identitatea digitală furnizat în conformitate cu art. 5, fără restricții nejustificate legate de furnizorul portofelului, cu respectarea cerințelor de interoperabilitate, securitate și protecție a datelor stabilite de cadrul normativ aplicabil.

(2) Furnizorii de atestate electronice calificate ale atributelor pun la dispoziție o interfață cu portofelele pentru identitatea digitală care sunt furnizate în conformitate cu art. 5.

Articolul 58. Norme suplimentare privind prestarea serviciilor de atestare electronică a atributelor

(1) Prestatorii serviciilor de atestare electronică calificată și necalificată a atributelor nu combină datele cu caracter personal referitoare la prestarea serviciilor respective cu datele cu caracter personal care provin din orice alte servicii oferite de ei sau de partenerii lor comerciali.

(2) Datele cu caracter personal referitoare la prestarea serviciilor de atestare electronică a atributelor sunt păstrate separate logic de alte date deținute de furnizorul atestatului electronic al atributelor.

(3) Prestatorii de servicii de atestare electronică calificată a atributelor pun în aplicare prestarea unor astfel de servicii de încredere calificate într-un mod care este separat din punct de vedere funcțional de alte servicii pe care le prestează.

Secțiunea a 10-a
Servicii de arhivare electronică

Articolul 59. Efectul juridic al serviciilor de arhivare electronică

(1) Datelor electronice și documentelor electronice păstrate prin utilizarea unui serviciu de arhivare electronică nu li se refuză efectul juridic sau posibilitatea de a fi acceptate ca probă în procedurile judiciare doar pentru motivul că acestea sunt în format electronic sau că nu sunt păstrate prin utilizarea unui serviciu calificat de arhivare electronică.

(2) Datele electronice și documentele electronice păstrate prin utilizarea unui serviciu calificat de arhivare electronică beneficiază de prezumția de integritate și de acuratețe a originii pe toată durata perioadei de păstrare de către prestatorul de servicii de încredere calificat.

Articolul 60. Cerințe privind serviciile calificate de arhivare electronică

(1) Serviciile calificate de arhivare electronică îndeplinesc următoarele cerințe:

a) sunt prestate de prestatori de servicii de încredere calificați;

b) utilizează proceduri și tehnologii capabile să asigure durabilitatea și lizibilitatea datelor electronice și a documentelor electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținându-le totodată integritatea și acuratețea originii;

c) garantează că respectivele date electronice și documente electronice sunt păstrate astfel încât să fie protejate împotriva pierderii și modificării, cu excepția modificărilor privind suportul lor sau formatul lor electronic;

d) permit beneficiarilor autorizați să primească în mod automat un raport care confirmă faptul că datele electronice și documentele electronice extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate a datelor de la începutul perioadei de păstrare până în momentul extragerii.

(2) Raportul menționat la alin. (1) lit. d) este furnizat într-un mod fiabil și eficient și poartă semnătura electronică calificată sau sigiliul electronic calificat al prestatorului serviciului calificat de arhivare electronică.

(3) În cazul în care un serviciu calificat de arhivare electronică îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele privind serviciile calificate de arhivare electronică.

Secțiunea a 11-a
Registre electronice

Articolul 61. Efectele juridice ale registrelor electronice

(1) Unui registru electronic nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele pentru registrele electronice calificate.

(2) Înregistrările de date cuprinse într-un registru electronic calificat beneficiază de prezumția ordonării lor cronologice secvențiale unice și exacte și de prezumția de integritate.

Articolul 62. Cerințe privind registrele electronice calificate

(1) Registrele electronice calificate îndeplinesc următoarele cerințe:

a) sunt create și gestionate de unul sau mai mulți prestatori de servicii de încredere calificați;

b) stabilesc originea înregistrărilor de date din registru;

c) asigură ordonarea cronologică secvențială unică a înregistrărilor de date din registru;

d) înregistrează datele astfel încât orice modificare a lor ulterioară să poată fi detectată imediat, asigurând integritatea datelor în timp.

(2) În cazul în care registrul electronic îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

Capitolul IV
DOCUMENTE ELECTRONICE

Articolul 63. Efectele juridice ale documentelor electronice

(1) Documentul electronic semnat cu semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat este asimilat, după efectele acestuia, cu documentul similar pe suport de hârtie, semnat cu semnătură olografă.

(2) Documentul electronic emis de către o autoritate sau o instituţie publică sau de către o persoană în exercitarea şi în limitele atribuţiilor sale de putere publică, semnat cu o semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat este asimilat unui înscris autentic.

(3) Documentul electronic semnat cu un tip de semnătură electronică diferit de semnătura electronică calificată produce efecte juridice echivalente cu cele ale documentului similar pe suport de hârtie semnat olograf doar în cazurile prevăzute expres de actele normative sau atunci când părțile au convenit în mod explicit utilizarea semnăturilor electronice, printr-un înscris distinct semnat olograf sau cu semnătură electronică calificată.

(4) Actele normative sau acordul părților privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaștere a documentelor electronice, semnate cu alt tip de semnătură electronică decât cea calificată, asimilate, după efectele lor, cu documente similare pe suport de hârtie, semnate cu semnătură

olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum și obligațiile părților privind confidențialitatea și răspunderea materială.

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

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

(7) 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.

Capitolul V
CADRUL DE GUVERNANȚĂ

Articolul 64. Supravegherea cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere

(1) Organismul de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere este Serviciul de Informații și Securitate al Republicii Moldova.

(2) Rolul organismului de supraveghere desemnate în temeiul alin. (1) constă în:

a) supravegherea furnizorilor de portofele pentru identitatea digitală cu sediul în Republica Moldova, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii furnizori și de către portofelele pentru identitatea digitală furnizate de aceștia a cerințelor stabilite de prezenta lege;

b) supravegherea prestatorilor de servicii de încredere calificați cu sediul în Republicii Moldova, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii prestatori de servicii de încredere calificați și de către serviciile de încredere calificate prestate de aceștia a cerințelor stabilite în prezenta lege;

c) a lua măsuri, dacă este necesar, în ceea ce îi privește pe furnizorii de portofele pentru identitatea digitală cu sediul în Republica Moldova, prin intermediul unor activități de supraveghere ex post, atunci când sunt informate că furnizorii sau portofelele pentru identitatea digitală furnizate de aceștia încalcă prezenta lege;

d) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați cu sediul în Republica Moldova, prin intermediul activităților de supraveghere ex post, atunci când sunt informate că respectivii prestatori de servicii de încredere necalificați sau serviciile de încredere prestate de aceștia nu ar îndeplini cerințele stabilite de prezenta lege.

(3) În îndeplinirea rolului prevăzut la alin. (2), organismul de supraveghere:

1) în domeniul cadrului pentru portofelul pentru identitatea digitală:

a) solicită furnizorilor de portofele pentru identitatea digitală să remedieze orice încălcare a cerințelor prevăzute de prezenta lege;

b) suspendă sau anulează înregistrarea și includerea beneficiarilor în mecanismul menționat la art. 6 în cazul utilizării ilegale sau frauduloase a portofelului pentru identitatea digitală;

c) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal;

d) realizează activități de verificare a furnizorilor de portofele pentru identitatea digitală;

e) solicită informațiile necesare pentru monitorizarea conformității cu prezenta lege

2) în domeniul serviciilor de încredere:

a) analizează rapoartele de evaluare a conformității menționate la art. 21 alin. (1) și la art. 22 alin. (1);

b) realizează audituri sau solicită unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați, în conformitate cu art. 21 alin. (3);

c) acordă sau retrage statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează;

d) asigură că prestatorii de servicii de încredere calificate cu sediul în Republica Moldova şi serviciile de încredere calificate pe care aceştia le prestează îndeplinesc cerinţele stabilite de prezenta lege;

e) solicită prestatorilor de servicii de încredere să remedieze încălcările cerințelor prevăzute de prezenta lege;

f) verifică existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului atunci când prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate cu art. 24 alin. (4) pct. 10);

g) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal;

h) investighează cererile formulate de furnizorii de browsere web în temeiul art. 51 și să ia măsuri, dacă este necesar.

(4) În cazul în care organismul de supraveghere, în temeiul alin. (4) pct. 1) lit. a), solicită furnizorului unui portofel pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute de lege, iar furnizorul nu ia măsurile corespunzătoare, organismul de supraveghere poate dispune, ținând seama, în

special, de amploarea, durata și consecințele respectivei neîndepliniri, suspendarea sau încetarea furnizării portofelului pentru identitatea digitală.

(5) Organismul de supraveghere informează fără întârzieri nejustificate beneficiarii și utilizatorii portofelului pentru identitatea digitală cu privire la decizia de suspendare sau încetare a furnizării acestuia.

(6) Organismul de supraveghere transmite Parlamentului Republicii Moldova, până la 31 martie a fiecărui an, un raport cu privire la principalele activități desfășurate în anul calendaristic anterior în domeniul portofelului pentru identitatea digitală și al serviciilor de încredere.

Articolul 65. Punct unic de contact

Organismul de supraveghere acționează ca punct unic de contact pentru serviciile de încredere, portofelele pentru identitatea digitală și sistemele de identificare electronică, în relațiile cu autoritățile competente din alte state și cu organizațiile internaționale relevante.

Articolul 66. Cerințe de raportare

(1) Organismul de supraveghere asigură colectarea de date statistice în legătură cu funcționarea portofelelor pentru identitatea digitală și a serviciilor de încredere calificate furnizate pe teritoriul Republicii Moldova.

(2) Datele statistice colectate în conformitate cu alin. (1) includ următoarele:

a) numărul persoanelor fizice și juridice care dețin un portofel pentru identitatea digitală valabil;

b) tipul și numărul serviciilor care acceptă utilizarea portofelului pentru identitatea digitală;

c) numărul reclamațiilor din partea utilizatorilor și al incidentelor privind protecția consumatorilor sau protecția datelor în legătură cu beneficiarii și serviciile de încredere calificate;

d) un raport de sinteză care include date privind incidentele care împiedică utilizarea portofelului pentru identitatea digitală;

e) un rezumat al incidentelor semnificative de securitate, al încălcărilor securității datelor și al utilizatorilor afectați ai portofelelor pentru identitatea digitală sau ai serviciilor de încredere calificate.

(3) Datele statistice menționate la alin. (2) sunt puse la dispoziția publicului într-un format deschis, utilizat în mod obișnuit și prelucrabil automat.

Capitolul VI
RĂSPUNDEREA JURIDICĂ

Articolul 67. Răspunderea juridică în cadrul tranzacțiilor transfrontaliere

(1) Organismul de supraveghere este răspunzător pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere, ca urmare a nerespectării obligațiilor care îi revin potrivit

prezentei legi referitoare la asigurarea interoperabilității și securității sistemelor de identificare electronică notificate Comisiei Europene.

(2) Emitentul mijloacelor de identificare electronică este răspunzător pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere, ca urmare a nerespectării obligației de a asigura că mijloacele de identificare electronică emise corespund, la momentul emiterii și ulterior, datelor de identificare electronică ale persoanei căreia i-au fost atribuite.

(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere, pentru neasigurarea executării corecte a autentificării.

Articolul 68. Sancțiuni

(1) Încălcarea prevederilor prezentei legi de către prestatorii de servicii de încredere, calificați sau necalificați, atrage răspunderea acestora și aplicarea amenzilor, de către organismul de supraveghere competent.

(2) Încălcările prevederilor prezentei legi de către prestatorii de servicii de încredere calificați și necalificați fac obiectul aplicării unor amenzi în următoarele limite:

a) echivalentul în lei al sumei de 5 000 000 EUR, în cazul în care prestatorul de servicii de încredere este o persoană fizică; sau

b) în cazul persoanelor juridice, echivalentul în lei al sumei de 5 000 000 EUR sau până la 1% din cifra de afaceri anuală totală la nivel mondial a întreprinderii din care face parte prestatorul de servicii de încredere, realizată în exercițiul financiar anterior anului în care a fost constatată încălcarea, luându-se în considerare valoarea cea mai mare.

(3) Constatarea încălcărilor și aplicarea sancțiunilor se realizează de către organismul de supraveghere, în conformitate cu prezenta lege.

(4) Deciziile organismului de supraveghere pot fi contestate în instanța de judecată competentă, în condițiile legii.

Capitolul VII
DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 69. Dispoziții finale

(1) Prezenta lege intră în vigoare la expirarea a 18 de luni de la data publicării în Monitorul Oficial al Republicii Moldova, cu excepția prevederilor art. 67 și 68 care se pun în aplicare din momentul aderării Republicii Moldova la Uniunea Europeană.

(2) Guvernul, până la intrarea în vigoare a prezentei legi:

a) în termen de 3 luni de la data publicării prezentei legi, va întreprinde măsurile necesare pentru stabilirea autorității administrației publice centrale de specialitate

responsabile de realizarea politicii de stat în domeniul identificării electronice și serviciilor de încredere;

b) în termen de 6 luni de la data publicării prezentei legi, va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege;

c) în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.

(3) La data intrării în vigoare a prezentei legi se abrogă Legea nr 124/2022 privind identificarea electronică și serviciile de încredere.

(4) Instituția Publică Agenția de Guvernare Electronică va asigura disponibilitatea unui portofel pentru identitatea digitală certificat corespunzător în termen de 24 de luni de la data intrării în vigoare a legii.

Articolul 70. Dispoziții tranzitorii

(1) Prestatorii de servicii de încredere care au obținut statutul de prestator de servicii de încredere calificat, în urma finalizării procedurii de acreditare, conform Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere, își păstrează în continuare statutul, având obligația să prezinte rapoarte de audit al conformității prestării serviciilor de încredere calificate, efectuate de către organisme de evaluare a conformității conform prevederilor legii.

(2) Certificatele calificate emise persoanelor fizice în temeiul Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere sunt considerate în continuare certificate calificate pentru semnături electronice în temeiul prezentei legi până la expirarea acestora.

Președintele Parlamentului

NOTA DE FUNDAMENTARE

la proiectul de lege privind identificarea electronică și serviciile de încredere

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul de lege privind identificarea electronică și serviciile de încredere a fost elaborat de către Ministerul Dezvoltării Economice și Digitalizării.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Elaborarea proiectului de lege privind identificarea electronică și serviciile de încredere este determinată de necesitatea modernizării și consolidării cadrului normativ național în domeniul identității digitale și al serviciilor de încredere electronice, în scopul alinierii depline a acestuia la evoluțiile accelerate ale cadrului legislativ al Uniunii Europene și la standardele tehnice internaționale aplicabile în domeniu. Necesitatea intervenției legislative derivă atât din angajamentele asumate de Republica Moldova în procesul de integrare europeană, cât și din insuficiențele structurale ale reglementării actuale, care nu mai corespunde cerințelor tehnice și juridice impuse de ecosistemul digital european actual.

Temeiul juridic al elaborării proiectului de lege îl constituie, în principal, obligația de transpunere a 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 (eIDAS), astfel cum a fost modificat și completat prin Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală (eIDAS 2.0). Aceste instrumente juridice ale Uniunii Europene stabilesc un cadru uniform și obligatoriu pentru statele membre privind recunoașterea reciprocă a mijloacelor de identificare electronică, condițiile de funcționare a prestatorilor de servicii de încredere, cerințele aplicabile semnăturilor electronice, sigiliilor electronice, mărcilor temporale electronice, serviciilor de livrare electronică recomandată, certificatelor de autentificare a site-urilor web, arhivării electronice și atestărilor electronice ale atributelor, precum și cadrul tehnic și juridic pentru portofelele europene pentru identitatea digitală (European Digital Identity Wallet — EUDI Wallet). Transpunerea acestor acte în legislația națională derivă din angajamentele asumate de Republica Moldova în cadrul procesului de integrare europeană, al Acordului de Asociere cu Uniunea Europeană și al angajamentelor specifice asumate în procesul de aderare.

Transpunerea prevederilor eIDAS și eIDAS 2.0 este prevăzută în Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, în cadrul Clusterului 3 „Competitivitate și Creștere Incluzivă”, capitolul 10 „Societate informațională”, acțiunea 11, care stabilește măsurile necesare pentru alinierea cadrului normativ național la legislația Uniunii Europene în domeniul identificării electronice și al serviciilor de încredere.

Totodată, proiectul de lege contribuie la realizarea măsurii 2-3-10-MDED, cu termen de implementare - decembrie 2026, prevăzută în Agenda de Reforme aferentă Planului de creștere al Republicii Moldova pentru anii 2025–2027.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

În Republica Moldova, cadrul normativ în domeniul identificării electronice și al serviciilor de încredere este reglementat prin Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, prin care au fost transpuse parțial prevederile Regulamentului (UE) nr. 910/2014 (eIDAS). Adoptarea Legii nr. 124/2022 a constituit un pas important în consolidarea cadrului juridic național pentru utilizarea mecanismelor de identificare electronică și a serviciilor de încredere, contribuind la crearea bazei juridice pentru semnătura electronică calificată, sigiliul electronic calificat, marca temporală electronică calificată și serviciile de livrare electronică recomandată calificată. Implementarea legii a facilitat integrarea serviciilor publice electronice cu mecanisme de autentificare sigure și a contribuit la creșterea gradului de utilizare a instrumentelor digitale în relațiile administrative.

Totuși, ulterior adoptării Legii nr. 124/2022, cadrul normativ european în domeniul identității digitale și al serviciilor de încredere a fost semnificativ revizuit și extins prin aprobarea Regulamentului (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014, prin care a fost instituit cadrul european pentru identitatea digitală. Modificările respective au introdus un set amplu de noi mecanisme juridice și tehnice menite să consolideze ecosistemul european de identitate digitală, inclusiv prin instituirea portofelului european pentru identitatea digitală (European Digital Identity Wallet – EUDI Wallet). Acesta va permite persoanelor fizice și juridice să se identifice electronic și să partajeze, în mod securizat, date și atribute verificate ale identității lor în relațiile cu autoritățile publice și furnizorii de servicii private, atât la nivel național, cât și transfrontalier.

Portofelul european pentru identitatea digitală va constitui un instrument digital sigur, ușor de utilizat și controlat de utilizator, care va permite autentificarea electronică, accesarea serviciilor publice și private online și offline, precum și utilizarea unor atestări electronice ale atributelor, cum ar fi calificările academice, diplomele universitare sau alte dovezi ale identității și statutului unei persoane. De asemenea, cadrul european pentru identitatea digitală stabilește condițiile pentru integrarea utilizatorilor în ecosistemul portofelelor digitale prin utilizarea mijloacelor de identificare electronică cu niveluri de asigurare ridicat sau substanțial, precum și cerințe armonizate privind securitatea, interoperabilitatea și certificarea soluțiilor de identitate digitală. În același timp, portofelele europene pentru identitatea digitală vor permite utilizatorilor să creeze și să utilizeze semnături electronice calificate și sigilii electronice calificate, care vor fi recunoscute în întreaga Uniune Europeană. Utilizarea semnăturii electronice calificate în scopuri neprofesionale urmează să fie gratuită pentru persoanele fizice, în vederea facilitării accesului larg al cetățenilor la servicii digitale sigure.

Aceste evoluții se înscriu în obiectivele stabilite prin Programul de politică pentru 2030 privind Deceniul digital, instituit prin Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului, care prevede implementarea pe scară largă a unei identități digitale sigure, voluntare și controlate de utilizator, recunoscută în întreaga Uniune

Europeană și destinată facilitării accesului la servicii digitale și participării la economia digitală.

În acest context, Guvernul Republicii Moldova, prin intermediul Agenției de Guvernare Electronică, își propune dezvoltarea și lansarea unui portofel pentru identitatea digitală, aliniat la standardele europene privind identitatea digitală. Inițiativa are drept scop oferirea cetățenilor și mediului de afaceri a unui instrument digital modern care să permită identificarea electronică, autentificarea și utilizarea serviciilor de încredere într-un mod simplu, sigur și interoperabil. Portofelul național pentru identitatea digitală va constitui o componentă de bază a ecosistemului național de servicii digitale și va permite, în perspectivă, interoperabilitatea cu portofelele europene pentru identitatea digitală, facilitând accesul cetățenilor Republicii Moldova la servicii digitale în spațiul european.

În acest context, transpunerea cadrului juridic al Uniunii Europene în domeniul identificării electronice și al serviciilor de încredere reprezintă o precondiție esențială pentru dezvoltarea și lansarea portofelelor pentru identitatea digitală la nivel național, precum și pentru asigurarea interoperabilității acestora cu ecosistemele digitale europene.

Totodată, cadrul normativ național instituit prin Legea nr. 124/2022 nu mai reflectă în mod adecvat evoluțiile recente ale acquis-ului Uniunii Europene și nu permite transpunerea integrală a noilor prevederi europene privind identitatea digitală.

Prin urmare, se impune modernizarea și consolidarea cadrului normativ național, inclusiv prin substituirea Legii nr. 124/2022 cu o nouă lege, care să asigure transpunerea integrală a legislației Uniunii Europene în domeniul identificării electronice și al serviciilor de încredere și să creeze premisele necesare pentru implementarea portofelelor pentru identitatea digitală la nivel național, în conformitate cu standardele europene. Adoptarea cadrului legislativ propus va contribui la dezvoltarea unui ecosistem național modern de identitate digitală, la creșterea nivelului de încredere în serviciile digitale și la facilitarea accesului cetățenilor și al mediului de afaceri la servicii publice și private în format electronic, în conformitate cu obiectivele de transformare digitală și cu parcursul de integrare europeană al Republicii Moldova.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de lege are drept obiectiv general modernizarea și armonizarea deplină a cadrului normativ național în domeniul identificării electronice și al serviciilor de încredere, în vederea alinierii acestuia la acquis-ul Uniunii Europene, în special la prevederile Regulamentului (UE) nr. 910/2014 (eIDAS), astfel cum a fost modificat și completat prin Regulamentul (UE) 2024/1183 (eIDAS 2.0). Proiectul urmărește, în egală măsură, crearea cadrului juridic intern necesar pentru implementarea portofelelor pentru identitatea digitală la nivel național, compatibile cu portofelele europene pentru identitatea digitală (EUDI Wallet), și pentru asigurarea interoperabilității depline a ecosistemului digital național cu ecosistemele digitale ale statelor membre ale Uniunii Europene. Proiectul instituie totodată un cadru de supraveghere și responsabilitate clar, cu atribuții pentru Serviciul de Informații și Securitate, în calitate de organism de supraveghere, și stabilește un regim sancționator proporțional și eficace pentru neconformitățile prestatorilor de servicii de încredere.

În acest sens, proiectul de lege urmărește:

- transpunerea integrală a cadrului juridic european în domeniul identificării electronice și al serviciilor de încredere;

- instituirea cadrului juridic pentru portofelul european pentru identitatea digitală (European Digital Identity Wallet) și pentru portofelele digitale naționale interoperabile cu ecosistemul european;
- asigurarea interoperabilității sistemelor de identificare electronică ale Republicii Moldova cu cele ale statelor membre ale Uniunii Europene;
- consolidarea cadrului de reglementare și supraveghere a serviciilor de încredere, inclusiv a prestatorilor calificați de servicii de încredere;
- crearea premiselor pentru dezvoltarea serviciilor digitale sigure și accesibile pentru cetățeni, mediul de afaceri și autoritățile publice.

Printre elementele noi introduse prin proiectul de lege se regăsesc, în special:
- reglementarea portofelului digital pentru identitate și stabilirea cadrului juridic pentru emiterea, utilizarea și recunoașterea acestuia;
- instituirea mecanismelor de recunoaștere și interoperabilitate a schemelor de identificare electronică în conformitate cu cerințele europene;
- actualizarea cadrului juridic aplicabil serviciilor de încredere, inclusiv semnăturilor electronice, sigiliilor electronice, mărcilor temporale electronice, serviciilor de livrare electronică recomandată și certificatelor pentru autentificarea site-urilor web;
- consolidarea mecanismelor de supraveghere și control asupra furnizorilor de servicii de încredere;
- stabilirea cadrului juridic pentru acceptarea și utilizarea identităților digitale și a portofelelor digitale în furnizarea serviciilor publice și private;
- reglementarea registrelor electronice și a registrelor electronice calificate ca noi categorii de servicii de încredere;
- instituirea serviciului de arhivare electronică și a serviciului calificat de arhivare ca servicii de încredere reglementate;
- reglementarea atestărilor electronice ale atributelor (EAA), inclusiv a celor emise de organismele din sectorul public bazate pe surse autentice;
- instituirea serviciilor de gestionare a dispozitivelor de creare a semnăturilor/sigiliilor la distanță ca servicii de încredere calificate.

Adoptarea proiectului de lege va crea premisele necesare pentru dezvoltarea ecosistemului național de identitate digitală, compatibil cu cadrul european, și va contribui la accelerarea proceselor de digitalizare a serviciilor publice și private.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În procesul de elaborare a proiectului de lege au fost analizate mai multe opțiuni de reglementare.

Opțiunea 1 – Menținerea cadrului normativ existent

Această opțiune presupunea păstrarea cadrului normativ actual, reglementat prin Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere.

Această opțiune nu a fost considerată viabilă din multiple considerente tehnice și juridice. În primul rând, cadrul normativ existent reflectă doar parțial și incomplet prevederile Regulamentului (UE) nr. 910/2014 și nu acoperă în niciun mod modificările substanțiale introduse prin Regulamentul (UE) 2024/1183, în special cele referitoare la: (i) portofelul european pentru identitatea digitală (EUDI Wallet) și cadrul tehnic pentru emiterea, utilizarea și recunoașterea acestuia; (ii) noul regim al atestărilor electronice ale atributelor (EAA) și al atestărilor electronice calificate ale atributelor (QEAA); (iii) cerințele extinse de interoperabilitate și recunoaștere reciprocă a identităților digitale între

statele membre și statele asociate; (iv) noile obligații ale furnizorilor de servicii care acceptă mijloace de identificare electronică; și (v) cadrul armonizat privind arhivarea electronică calificată, serviciul calificat de gestionare a dispozitivelor de creare a semnăturilor la distanță și serviciul calificat de validare a semnăturilor electronice calificate.

Menținerea cadrului normativ actual ar limita capacitatea Republicii Moldova de a se alinia la standardele europene și de a dezvolta soluții digitale interoperabile la nivel european.

Opțiunea 2 – Modificarea și completarea Legii nr. 124/2022

O altă opțiune analizată a constat în modificarea și completarea Legii nr. 124/2022, prin introducerea noilor prevederi necesare pentru transpunerea integrală a modificărilor operate prin Regulamentul (UE) 2024/1183 (eIDAS 2.0), menținând totodată structura generală și arhitectura juridică a legii existente.

Totuși, această opțiune nu a fost considerată oportună din perspectivă juridică și tehnico-legislativă, deoarece modificările necesare sunt de o amploare, profunzime și complexitate care depășesc cu mult cadrul unei intervenții legislative ordinare de modificare și completare. Noile prevederi vizează nu doar completarea sau ajustarea unor dispoziții existente, ci instituirea unui set integral de concepte, mecanisme, proceduri și instituții juridice noi, complet absente din actuala reglementare, printre care: cadrul juridic complet pentru portofelul digital pentru identitate (emitere, utilizare, revocare, interoperabilitate transfrontalieră); regimul juridic al atestărilor electronice ale atributelor și al emitenților acestora; mecanismele de interoperabilitate europeană pentru schemele de identificare electronică notificate; noul cadru de obligații pentru furnizorii de servicii din sectorul public și privat care acceptă mijloace de identificare electronică; regimul extins al serviciilor calificate de încredere introduse prin eIDAS 2.0 (gestionare calificată a dispozitivelor de creare a semnăturilor la distanță, validare calificată etc.) și cadrul sancționator armonizat.

În conformitate cu articolul 63 alin. (1) din Legea nr. 100/2017 privind actele normative, modificarea unui act normativ este admisă doar în măsura în care nu afectează concepția generală sau caracterul unitar al acestuia. În caz contrar, actul normativ urmează a fi substituit printr-un nou act normativ, cu abrogarea integrală a celui existent.

Având în vedere amploarea modificărilor necesare pentru alinierea cadrului normativ național la acquis-ul Uniunii Europene, modificarea Legii nr. 124/2022 ar afecta în mod substanțial structura, concepția și arhitectura juridică a acesteia, ceea ce ar genera un act normativ fragmentat și dificil de aplicat.

Opțiunea selectată – Adoptarea unei noi legi

Prin urmare, s-a optat pentru elaborarea și adoptarea unei noi legi privind identificarea electronică și serviciile de încredere, care să abroge integral Legea nr. 124/2022 și să instituie un cadru normativ modern, coerent și pe deplin armonizat cu legislația Uniunii Europene.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Adoptarea proiectului de lege va avea un impact pozitiv asupra sectorului public, prin crearea unui cadru juridic modern și armonizat cu legislația Uniunii Europene privind identificarea electronică și serviciile de încredere. Impactul se va manifesta atât la nivelul autorităților centrale de specialitate, cât și la nivelul autorităților administrației publice

locale, al instituțiilor publice cu competențe în domeniul serviciilor electronice și al entităților responsabile de gestionarea infrastructurii digitale naționale.

Implementarea prevederilor proiectului va contribui la:

1) consolidarea infrastructurii naționale de identitate digitală și a serviciilor de încredere;

2) facilitarea interoperabilității dintre sistemele informaționale ale autorităților publice;

3) creșterea nivelului de securitate și încredere în utilizarea serviciilor publice electronice;

4) reducerea utilizării documentelor pe suport de hârtie și optimizarea proceselor administrative.

Autoritățile și instituțiile publice vor putea utiliza în mod uniform și interoperabil mecanisme de identificare electronică la niveluri de asigurare ridicat și substanțial, precum și servicii de încredere calificate, pentru furnizarea serviciilor publice electronice. Implementarea proiectului va facilita trecerea de la modelul actual de prestare a serviciilor publice, care implică frecvent prezența fizică a beneficiarilor și utilizarea documentelor pe suport de hârtie, la un model complet digitalizat, bazat pe autentificarea electronică sigură prin portofelul național pentru identitatea digitală. Această tranziție va contribui la creșterea eficienței administrative, la reducerea timpilor de așteptare și a costurilor administrative, și la simplificarea și fluidizarea interacțiunii autorităților publice cu cetățenii și mediul de afaceri.

În același timp, proiectul stabilește cadrul instituțional și atribuțiile autorităților competente pentru supravegherea și reglementarea prestatorilor de servicii de încredere, contribuind la consolidarea substanțială a capacității instituționale în acest domeniu. Sunt stabilite, în mod explicit: autoritatea responsabilă de gestionarea Listei de încredere naționale; autoritatea competentă pentru emiterea unui portofel pentru identitatea digitală furnizat de Guvern; procedurile de audit și certificare a prestatorilor calificați de servicii de încredere etc. În conformitate cu art. 64 din proiectul de lege, Serviciul de Informații și Securitate este desemnat în calitate de organism de supraveghere, exercitând competențe de monitorizare, control și asigurare a respectării cerințelor legale în domeniul serviciilor de încredere și al cadrului pentru portofelul de identitate digitală. Totodată, acesta îndeplinește rolul de punct unic de contact în relațiile cu autoritățile competente din alte state și cu organizațiile internaționale, facilitând cooperarea transfrontalieră și schimbul de informații relevante.

Agenția de Guvernare Electronică are un rol dublu în arhitectura sistemului, acționând atât în calitate de dezvoltator al portofelului național pentru identitatea digitală, cât și ca operator responsabil de asigurarea disponibilității, funcționării continue și îmbunătățirii acestuia. În această calitate, AGE asigură mentenanța tehnică, implementarea actualizărilor, respectarea cerințelor de securitate cibernetică și interoperabilitate, precum și integrarea portofelului cu alte servicii publice electronice, contribuind astfel la crearea unui ecosistem digital unitar și orientat către utilizator.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea proiectului de lege nu implică, în mod direct, cheltuieli suplimentare din bugetul de stat pentru adoptarea cadrului normativ.

Eventualele costuri vor fi asociate în principal cu:

1) dezvoltarea și modernizarea infrastructurii tehnice necesare pentru implementarea mecanismelor de identificare electronică, inclusiv implementarea unui portofel pentru identitatea digitală;

2) integrarea sistemelor informaționale ale autorităților publice cu infrastructura de identitate digitală;

3) adaptarea serviciilor publice electronice pentru utilizarea mijloacelor de identificare electronică și a serviciilor de încredere.

Aceste costuri urmează a fi acoperite din resursele planificate pentru digitalizarea sectorului public, inclusiv din proiecte finanțate din fonduri externe, programe de modernizare digitală sau alte mecanisme de finanțare destinate transformării digitale a administrației publice.

4.3 Impactul asupra sectorului privat

Proiectul de lege va genera un impact multidimensional asupra sectorului privat, prin instituirea unui cadru juridic modern, clar și previzibil pentru utilizarea identității digitale și a serviciilor de încredere în relațiile comerciale și juridice. Furnizorii de servicii digitale din sectorul privat care, conform noului cadru normativ, vor fi obligați să accepte portofelele digitale pentru identitate, inclusiv băncile, companiile de asigurări, furnizorii de utilități, platformele de comerț electronic și furnizorii de servicii medicale private, vor putea oferi servicii de onboarding complet digitalizate, securizate și conforme cu cerințele de protecție a datelor, contribuind la creșterea competitivității pe piața digitală. Sectorul bancar și financiar va beneficia de un cadru juridic stabil pentru utilizarea identităților digitale verificate în procesele de cunoaștere a clientelei și de onboarding digital, contribuind la reducerea costurilor de conformitate și la accelerarea digitalizării serviciilor financiare. Beneficiarii din sectorul privat care doresc să utilizeze portofelul pentru identitatea digitală se vor înregistra prin intermediul Portalului guvernamental integrat EVO. În procesul de utilizare a portofelului, aceștia au obligația de a solicita, accesa și prelucra exclusiv datele strict necesare pentru furnizarea serviciilor oferite, în limitele scopurilor determinate și comunicate inițial utilizatorilor. Este interzisă colectarea sau utilizarea ulterioară a unor date suplimentare fără un temei legal corespunzător sau fără informarea și, după caz, consimțământul explicit al utilizatorului. Totodată, beneficiarii sunt responsabili de implementarea unor măsuri tehnice și organizatorice adecvate pentru a garanta respectarea principiului minimizării datelor, precum și pentru a asigura securitatea, confidențialitatea și integritatea datelor cu caracter personal pe întreg ciclul de viață al acestora.

4.4. Impactul social

Proiectul de lege are un impact social pozitiv contribuind la extinderea și consolidarea incluziunii digitale și la facilitarea accesului cetățenilor la servicii publice și private în format electronic, fără condiționări legate de locul de reședință, mobilitate fizică sau disponibilitate de timp. Prin implementarea unui portofel pentru identitatea digitală și a mecanismelor armonizate de identificare electronică la niveluri de asigurare ridicat și substanțial, cetățenii vor beneficia de acces securizat și simplificat la un spectru larg de servicii digitale, de la servicii de e-guvernare (obținerea actelor de stare civilă, înregistrarea vehiculelor, plata impozitelor) la servicii private (deschiderea de conturi bancare, semnarea contractelor, accesarea serviciilor medicale la distanță). Proiectul contribuie, totodată, la reducerea inegalităților digitale, prin asigurarea accesibilității instrumentelor de identificare electronică pentru toate categoriile de populație, inclusiv persoanele în vârstă, persoanele cu dizabilități și cele din mediul rural. În perspectiva

aderării Republicii Moldova la Uniunea Europeană, portabilitatea identității digitale prin portofele compatibile cu standardele europene va permite cetățenilor Republicii Moldova să acceseze servicii digitale în spațiul european fără obstacole administrative, contribuind astfel la facilitarea liberei circulații și la integrarea socio-economică în Uniunea Europeană. În acest sens, proiectul instituie un set de garanții, menite să asigure accesul echitabil și nediscriminatoriu la serviciile digitale, precum și protecția drepturilor utilizatorilor:

Semnătura electronică calificată va fi oferită gratuit persoanelor fizice, prin intermediul portofelului pentru identitatea digitală, eliminând astfel barierele financiare care ar putea împiedica accesul la servicii electronice. Această măsură urmărește stimularea utilizării serviciilor digitale publice și private, contribuind la creșterea gradului de incluziune digitală și la reducerea dependenței de documentele pe suport de hârtie.

Utilizarea portofelului digital are caracter strict voluntar. Nicio persoană nu poate fi obligată, direct sau indirect, să utilizeze portofelul pentru identitatea digitală, iar refuzul de utilizare nu poate constitui temei pentru restrângerea sau condiționarea accesului la servicii publice sau private. Astfel, se asigură menținerea unor canale alternative de acces la servicii, inclusiv în format fizic sau prin alte mijloace de identificare și autentificare.

Totodată, *portofelul este conceput și dezvoltat în conformitate cu standardele de accesibilitate digitală aplicabile*, astfel încât să poată fi utilizat în mod eficient și autonom de către persoanele cu dizabilități și de către persoanele în vârstă. În acest sens, sunt avute în vedere cerințe privind interfețe intuitive, compatibilitatea cu tehnologii asistive, opțiuni de personalizare și suport adecvat pentru utilizatori, contribuind la prevenirea excluziunii digitale și la asigurarea egalității de șanse.

4.4.1. Impactul asupra datelor cu caracter personal

Proiectul de lege implică în mod intrinsec prelucrarea datelor cu caracter personal în contextul emiterii, utilizării și gestionării mijloacelor de identificare electronică, a portofelelor pentru identitatea digitală și a serviciilor de încredere. Cadrul juridic propus este elaborat cu respectarea principiilor și cerințelor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului (RGPD), astfel cum acestea au fost transpuse în legislația națională prin Legea nr. 195/2024 privind protecția datelor cu caracter personal. Proiectul înglobează principiul „privacy by design" (protecția datelor prin concepție) și principiul „privacy by default" (protecția datelor în mod implicit), asigurând că arhitectura tehnică a portofelului pentru identitatea digitală este proiectată astfel încât să minimizeze colectarea și prelucrarea datelor personale la strictul necesar. Utilizatorilor li se va garanta controlul deplin asupra atributelor de identitate partajate, partajarea realizându-se exclusiv pe baza consimțământului explicit, granular și revocabil al titularului. Proiectul prevede obligații specifice privind securitatea prelucrării datelor pentru prestatorii de servicii de încredere și pentru emitentul portofelului, inclusiv cerințe de pseudonimizare, criptare end-to-end și jurnal de audit. Centrul Național pentru Protecția Datelor cu Caracter Personal va fi consultat în cadrul elaborării actelor normative secundare și va exercita atribuțiile de supraveghere în materia protecției datelor cu caracter personal în legătură cu implementarea proiectului. Un element de bază pentru protecția vieții private îl constituie interdicția expresă impusă prestatorilor de servicii de atestare a atributelor de a combina datele provenite din serviciile de atestare cu date provenite din alte servicii pe care le oferă. Această separare logică și funcțională strictă asigură că datele de identitate ale utilizatorilor nu pot fi agregate sau corelate cu alte informații deținute de același prestator,

prevenind astfel crearea de profiluri de date extinse și protejând viața privată a utilizatorilor.

4.4.2 Impactul asupra echității și egalității de gen.

Proiectul de lege nu introduce prevederi care să genereze diferențe de tratament între persoane pe criterii de gen sau pe alte criterii de discriminare. Toate drepturile și obligațiile reglementate prin proiect se aplică în egală măsură persoanelor fizice, indiferent de sex, gen, vârstă, origine etnică, religie sau alte caracteristici personale.

Reglementarea identificării electronice și a serviciilor de încredere este neutră din perspectiva egalității de gen și se aplică în mod egal tuturor persoanelor fizice și juridice. Proiectul nu conține dispoziții directe sau indirecte care să restricționeze sau să condiționeze accesul la mijloace de identificare electronică sau la servicii de încredere pe criterii de gen.

Totodată, prin facilitarea accesului la servicii publice și private în format electronic, proiectul contribuie indirect la creșterea incluziunii sociale, la reducerea barierelor geografice și de mobilitate în accesarea serviciilor și la egalizarea oportunităților de participare la economia digitală pentru toate categoriile de populație, inclusiv cele din mediul rural sau cu acces limitat la servicii tradiționale.

4.5. Impactul asupra mediului

Proiectul de lege nu are un impact negativ direct asupra mediului înconjurător și nu implică activități cu potențial de poluare sau de afectare a echilibrului ecologic.

4.6. Alte impacturi și informații relevante

Din perspectiva securității cibernetice, proiectul de lege contribuie la consolidarea substanțială a rezilienței digitale naționale, prin stabilirea unor cerințe tehnice și operaționale riguroase pentru prestatorii de servicii de încredere, inclusiv obligații de certificare conform standardelor internaționale și cerințe de notificare promptă a incidentelor de securitate. Cadrul juridic propus este aliniat cerințelor Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2), contribuind la reducerea riscurilor cibernetice asociate identității digitale.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Proiectul de lege constituie principala măsură normativă de transpunere a Regulamentului (UE) nr. 910/2014 (eIDAS), astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (eIDAS 2.0). Proiectul transpune în legislația națională prevederile acestor acte ale Uniunii Europene, adaptate la specificul sistemului juridic al Republicii Moldova și la angajamentele asumate prin Acordul de Asociere cu Uniunea Europeană și prin Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029. Transpunerea are ca scop asigurarea compatibilității depline a cadrului normativ național cu acquis-ul Uniunii Europene în domeniu, facilitarea recunoașterii reciproce a mijloacelor de identificare electronică și a serviciilor de încredere între Republica Moldova și statele membre ale Uniunii Europene, precum și crearea premiselor pentru interoperabilitatea cu ecosistemele digitale europene.

Totodată, proiectul instituie un mecanism de recunoaștere unilaterală, cu caracter cuprinzător, a întregului portofoliu de servicii de încredere calificate reglementate la

nivelul Uniunii Europene. În acest sens, sunt recunoscute de drept, cu efecte juridice depline, serviciile de semnătură și sigilii electronice calificate, serviciile de gestionare a dispozitivelor calificate de creare a semnăturilor și sigiliilor la distanță, serviciile de validare și de păstrare a semnăturilor și sigiliilor electronice, mărcile temporale electronice calificate, certificatele pentru autentificarea site-urilor web, serviciile de distribuție electronică înregistrată calificată, atestatele electronice calificate ale atributelor, serviciile de arhivare electronică, precum și registrele electronice calificate.

În temeiul acestui principiu, serviciile de încredere întemeiate pe certificate calificate emise de prestatori calificați din Uniunea Europeană sunt recunoscute în Republica Moldova cu același statut juridic și produc aceleași efecte ca cele furnizate la nivel național, fără a fi necesară parcurgerea unor proceduri suplimentare de validare, autorizare sau echivalare. Această recunoaștere operează de drept, în mod direct și necondiționat, conferind securitate juridică și previzibilitate utilizatorilor și prestatorilor.

Aceeași logică se extinde asupra componentelor tehnice esențiale, respectiv dispozitivelor de creare a semnăturilor și sigiliilor electronice calificate certificate în Uniunea Europeană, care sunt acceptate automat ca fiind conforme cu cerințele aplicabile în Republica Moldova. Prin această abordare sunt eliminate barierele tehnice și juridice în utilizarea transfrontalieră a instrumentelor de semnare și autentificare electronică, fiind facilitată interoperabilitatea efectivă între sisteme și infrastructuri.

Prin instituirea acestui mecanism extins de recunoaștere automată, proiectul de lege asigură un nivel înalt de interoperabilitate juridică și tehnică cu ecosistemul european al serviciilor de încredere, în concordanță cu principiile și exigențele cadrului eIDAS.

În ansamblu, reglementarea propusă creează premisele integrării efective a Republicii Moldova în spațiul digital european, consolidând încrederea în tranzacțiile electronice, stimulând schimburile economice și susținând transformarea digitală a sectorului public și privat, în condițiile unui cadru juridic coerent, previzibil și aliniat la standardele Uniunii Europene.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Proiectul de lege privind identificarea electronică și serviciile de încredere transpunere a Regulamentului (UE) nr. 910/2014 (eIDAS), astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (eIDAS 2.0).

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu procedurile stabilite pentru transparența în procesul decizional şi în vederea elaborării actelor normative, Anunțul pentru inițierea elaborării proiectului de act normativ este plasat pe pagina web oficială a MDED (mded.gov.md), rubrica Transparența/Anunțuri privind consultările publice, precum şi pe platforma guvernamentală particip.gov.md: https://particip.gov.md/ro/document/stages/*/16240.

Totodată, proiectul urmează a fi supus avizării și consultării publice în conformitate cu art. 32 din Legea nr. 100/2017 cu privire la actele normative, prin expedierea acestuia tuturor părților interesate.

7. Concluziile expertizelor
Conform art. 36 din Legea 100/2017 cu privire la actele normative proiectul urmează a fi supus expertizei anticorupție, care va fi efectuată de către Centrul Național Anticorupție. Conform art. 37 din Legea nr.100/2017 cu privire la actele normative proiectul urmează a fi supus expertizei juridice de către Ministerul Justiției.
8. Modul de încorporare a actului în cadrul normativ existent
Proiectul de lege privind identificarea electronică și serviciile de încredere se integrează organic în cadrul normativ incident domeniului reglementat, constituind principalul instrument juridic de transpunere a acquis-ului Uniunii Europene în materia identității digitale și a serviciilor de încredere. Proiectul abrogă integral Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere și se corelează cu legislația existentă. Cadrul normativ secundar necesar implementării legii, inclusiv regulamentele privind funcționarea unui portofel pentru identitatea digitală, condițiile tehnice pentru prestatorii de servicii de încredere, procedurile de supraveghere etc. va fi elaborat de Ministerul Dezvoltării Economice și Digitalizării, și promovat pentru aprobarea de către Guvern, în termenele stabilite prin dispozițiile finale ale proiectului de lege.
9. Măsuri necesare pentru implementarea prevederilor proiectului actului normativ
Pentru implementarea eficientă a proiectului de lege, este necesară elaborarea și adoptarea unui set de acte normative secundare, inclusiv regulamente și instrucțiuni de aplicare, care să stabilească procedurile și standardele tehnice pentru furnizorii de servicii de încredere. Aceste reglementări vor defini cerințele de securitate, interoperabilitate și compatibilitate a infrastructurii de identificare electronică, asigurând funcționarea coerentă și sigură a sistemelor publice și private. De asemenea, cadrul normativ va clarifica procedurile de autorizare, control și supraveghere a furnizorilor de servicii de încredere, garantând protecția datelor cu caracter personal și integritatea operațiunilor electronice. În paralel, este necesară dezvoltarea unui portofel electronic pentru identitatea digitală, furnizat de către Guvern, care va permite cetățenilor și întreprinderilor să stocheze, să gestioneze și să utilizeze în siguranță acreditările digitale și semnăturile electronice. Portofelul va facilita autentificarea unitară în serviciile publice și private, va simplifica interacțiunile digitale și va contribui la creșterea securității și eficienței în relațiile electronice dintre utilizatori și autorități sau furnizori de servicii. Implementarea acestor măsuri va crea un cadru digital coerent, modern și interoperabil, aliniat la bunele practici internaționale și la standardele europene în domeniul identității digitale și al serviciilor de încredere.

Secretar de Stat **Michelle ILIEV**

TABEL DE CONCORDANȚĂ

1	**1. Titlul actului Uniunii Europene** **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**. CELEX: 02014R0910-20241018, *inclusiv modificările operate prin* ***Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală***					
2	**Titlul actului normativ național -** Proiectul Legii privind identificarea electronică și serviciile de încredere					
3	**Gradul general de compatibilitate -** Compatibil					
4	**Autoritatea/persoana responsabilă -** Ministerul Dezvoltării Economice și Digitalizării /					
5	**Data întocmirii 08.04.2026**					
6						
Actul UE în limba română **7**	**Actul UE în limba engleză** **8**	**Actul/actele normativ/e național/e în limba română** **9**	**Traducerea actului/actelor normativ/e în limba engleză** **10**	**Gradul de compatibilitate** **11**	**Observațiile Republicii Moldova** **12**	**Observațiile Comisiei Europene** **13**
CAPITOLUL I **DISPOZIȚII GENERALE**	**CHAPTER I** **GENERAL PROVISIONS**	**CAPITOLUL I** **DISPOZIȚII GENERALE**				
Articolul 1 **Obiect**	**Article 1** **Subject matter**	**Articolul 1.** **Obiect**				
Prezentul regulament urmărește să asigure buna funcționare a pieței interne și să asigure un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere utilizate în întreaga Uniune, pentru a permite și a facilita exercitarea de către persoanele fizice și juridice a dreptului de a participa la societatea digitală în condiții de siguranță și de a accesa servicii publice și private online în întreaga Uniune. În	This Regulation aims to ensure the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union, in order to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely and to access online public and private	Prezenta lege urmărește să asigure buna funcționare a pieței interne și să asigure un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere utilizate în Republica Moldova, pentru a permite și a facilita exercitarea de către persoanele fizice și juridice a dreptului de a participa la societatea digitală în condiții de siguranță și de a accesa servicii publice și private online. În acest scop, prezenta lege:		Compatibil	Republica Moldova nefiind stat membru al Uniunii Europene reglementează posibilitatea de recunoaștere unilaterală a prestatorilor de servicii de încredere calificați stabiliți în state membre ale Uniunii Europene, precum și serviciilor de încredere calificate furnizate de către aceștia.	

acest scop, 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 și furnizează și recunosc portofelele europene pentru identitatea digitală; (b) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice; (c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate, serviciile de certificare pentru autentificarea unui site internet, arhivarea electronică, atestarea electronică a atributelor, dispozitivele de creare a semnăturilor, dispozitivele de creare a sigiliilor electronice, precum și pentru registrele electronice.	services throughout the Union. For those purposes, this Regulation: (a) lays down the conditions under which Member States are to recognise natural and legal persons' electronic identification means falling under a notified electronic identification scheme of another Member State and provide and recognise European Digital Identity Wallets; (b) lays down rules for trust services, in particular for electronic transactions; (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature creation devices, electronic seal creation devices, and electronic ledgers.	a) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice; b) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate, serviciile de certificare pentru autentificarea unui site internet, arhivarea electronică, atestarea electronică a atributelor, dispozitivele de creare a semnăturilor, dispozitivele de creare a sigiliilor electronice, precum și pentru registrele electronice; c) stabilește modul în care Republica Moldova recunoaște prestatorii de servicii de încredere calificați stabiliți în state membre ale Uniunii Europene, precum și serviciile de încredere calificate furnizate de către aceștia.				
Articolul 2 **Domeniul de aplicare**	**Article 2** **Scope**	**Articolul 2** **Domeniul de aplicare**				
(1) Prezentul regulament se aplică sistemelor de identificare electronică care sunt notificate de către un	1. This Regulation applies to electronic identification schemes notified by a Member	(1) Prezenta lege se aplică sistemelor de identificare electronică, portofelelor pentru identitatea		Compatibil		

stat membru, portofelelor europene pentru identitatea digitală care sunt furnizate de un stat membru și prestatorilor de servicii de încredere cu sediul în Uniune.	State, to European Digital Identity Wallets provided by a Member State and to trust service providers established in the Union.	digitală și prestatorilor de servicii de încredere cu sediul în Republica Moldova.				
(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.	2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.	(2) Prezenta lege 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.		Compatibil		
(3) Prezentul regulament nu aduce atingere dreptului Uniunii sau dreptului intern privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma, ori cerințelor sectoriale privind forma.	3. This Regulation does not affect Union or national law related to the conclusion and validity of contracts, other legal or procedural obligations relating to form, or sector-specific requirements relating to form.	(3) Prezenta lege nu aduce atingere legislației privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma, ori cerințelor sectoriale privind forma.		Compatibil		
(4) Prezentul regulament nu aduce atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului.	4. This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council.	(4) Prezenta lege nu aduce atingere prevederilor Legii nr. 195/2024 privind protecția datelor cu caracter personal.		Compatibil		
Articolul 3 **Definiții**	**Article 3** **Definitions**	**Articolul 3.** **Definiții**				
În sensul prezentului regulament, se aplică următoarele definiții:	For the purposes of this Regulation, the following definitions apply:	În sensul prezentei legi, se aplică următoarele definiții:		Compatibil		
1. „identificare electronică” înseamnă procesul de utilizare a datelor de identificare personală în	(1) ‘electronic identification’ means the process of using person identification data in	29. identificare electronică - procesul de utilizare a datelor de identificare personală în		Compatibil		

format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică;	electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person;	format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică;				
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 pentru un serviciu online sau, după caz, pentru un serviciu offline;	(2) ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;	33. mijloace de identificare electronică - unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării pentru un serviciu online sau, după caz, pentru un serviciu offline;		Compatibil		
3. „date de identificare personală” înseamnă un set de date care este emis în conformitate cu dreptul Uniunii sau cu dreptul intern și care permite stabilirea identității unei persoane fizice sau juridice ori a unei persoane fizice care reprezintă o altă persoană fizică sau o persoană juridică;	(3) ‘person identification data’ means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.	20. date de identificare personală - set de date care permite în conformitate cu cadrul normativ aplicabil stabilirea identității unei persoane fizice sau juridice ori a unei persoane fizice care reprezintă o altă persoană fizică sau o persoană juridică;		Compatibil		
4. „sistem de identificare electronică” înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice ori pentru persoane fizice care reprezintă alte persoane fizice sau persoane juridice;	(4) ‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;	56. sistem de identificare electronică - sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice ori pentru persoane fizice care reprezintă alte persoane fizice sau persoane juridice;		Compatibil		
5. „autentificare” înseamnă un proces electronic care	(5) ‘authentication’ means an electronic	1. autentificare - proces electronic care permite		Compatibil		

permite confirmarea identificării electronice a unei persoane fizice sau juridice sau confirmarea originii și integrității unor date în format electronic;	process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;	confirmarea identificării electronice a unei persoane fizice sau juridice sau confirmarea originii și integrității unor date în format electronic;				
5a. „utilizator” înseamnă o persoană fizică sau juridică ori o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică, care utilizează servicii de încredere sau mijloace de identificare electronică, puse la dispoziție în conformitate cu prezentul regulament;	(5a) ‘user’ means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation;	58. utilizator - persoană fizică sau juridică ori o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică, care utilizează servicii de încredere sau mijloace de identificare electronică, puse la dispoziție în conformitate cu prezenta lege;		Compatibil		
6. „beneficiar” înseamnă o persoană fizică sau juridică care beneficiază de identificarea electronică, de portofelele europene pentru identitatea digitală sau de alte mijloace de identificare electronică sau de un serviciu de încredere;	(6) ‘relying party’ means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service;	8. beneficiar - persoană fizică sau juridică care utilizează un serviciu de încredere sau care se bazează pe date de identificare electronică ori pe atribute prezentate printr-un portofel pentru identitatea digitală sau prin alte mijloace de identificare electronică, în scopul furnizării unui serviciu ori al autorizării unei tranzacții;		Compatibil		
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,	(7) ‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities,	36. organism din sectorul public - autoritate a administrației publice centrale sau locale, organism de drept public sau asociație formată din una sau mai multe astfel de autorități sau din unul sau mai multe astfel de organisme de drept public, ori o entitate privată mandatată de cel puțin una dintre aceste autorități, organisme sau asociații să		Compatibil		

organisme sau asociații să presteze servicii publice atunci când acționează în temeiul unui astfel de mandat;	bodies or associations to provide public services, when acting under such a mandate;	presteze servicii publice atunci când acționează în temeiul unui astfel de mandat;				
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;	(8) ‘body governed by public law’ means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council;	35. organism de drept public - organism care îndeplinește cumulativ următoarele condiții: a) este constituită în scopul explicit de a răspunde nevoilor de interes general și nu are caracter industrial sau comercial; b) are personalitate juridică; și c) este finanțată în proporție majoritară de autorități publice centrale sau locale sau de alte organisme de drept public; ori gestionarea acestora este supravegheată de autoritățile sau organismele respective; ori au un consiliu administrativ, de conducere sau de supraveghere, în care jumătate dintre membrii săi sunt numiți de autorități ale administrației publice centrale sau locale ori de alte organisme de drept public;		Compatibil		
9. „semnatar” înseamnă o persoană fizică care creează o semnătură electronică;	(9) ‘signatory’ means a natural person who creates an electronic signature;	44. semnatar - persoană fizică care creează o semnătură electronică;		Compatibil		
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;	(10) ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;	45. semnătură electronică - date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;		Compatibil		

11. „semnătură electronică avansată” înseamnă o semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26;	(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;	46. semnătură electronică avansată - semnătură electronică ce îndeplinește cerințele prevăzute la art. 27;		Compatibil		
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;	(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;	47. semnătură electronică calificată - 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;		Compatibil		
13. „date de creare a semnăturilor electronice” înseamnă date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;	(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;	18. date de creare a semnăturilor electronice - date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;		Compatibil		
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;	(14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;	9. certificat pentru semnătura electronică - 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;		Compatibil		
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;	(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;	10. certificat calificat pentru semnătură electronică - certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 30;		Compatibil		
16. „serviciu de încredere” înseamnă un serviciu	(16) 'trust service' means an electronic service	51. serviciu de încredere - serviciu electronic		Compatibil		

electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare din următoarele: (a) emiterea certificatelor pentru semnături electronice, a certificatelor pentru sigilii electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere; (b) validarea certificatelor pentru semnăturile electronice, a certificatelor pentru sigiliile electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere; (c) crearea semnăturilor electronice sau a sigiliilor electronice; (d) validarea semnăturilor electronice sau a sigiliilor electronice; (e) păstrarea semnăturilor electronice, a sigiliilor electronice, a certificatelor pentru semnăturile electronice sau a certificatelor pentru sigiliile electronice; (f) gestionarea dispozitivelor pentru crearea semnăturilor electronice la distanță sau a dispozitivelor pentru crearea sigiliilor electronice la distanță; (g) emiterea atestatelor electronice ale atributelor; (h) validarea atestatelor electronice a atributelor;	normally provided for remuneration which consists of any of the following: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; (f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestation of attributes; (i) the creation of electronic	prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare din următoarele: a) emiterea certificatelor pentru semnături electronice, a certificatelor pentru sigilii electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere; b) validarea certificatelor pentru semnăturile electronice, a certificatelor pentru sigiliile electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere; c) crearea semnăturilor electronice sau a sigiliilor electronice; d) validarea semnăturilor electronice sau a sigiliilor electronice; e) păstrarea semnăturilor electronice, a sigiliilor electronice, a certificatelor pentru semnăturile electronice sau a certificatelor pentru sigiliile electronice; f) gestionarea dispozitivelor pentru crearea semnăturilor electronice la distanță sau a dispozitivelor pentru crearea sigiliilor electronice la distanță; g) emiterea atestatelor electronice ale atributelor; h) validarea atestatelor electronice a atributelor;				

(i) crearea mărcilor temporale electronice; (j) validarea mărcilor temporale electronice; (k) prestarea serviciilor de distribuție electronică înregistrate; (l) validarea datelor transmise prin intermediul serviciilor de distribuție electronică înregistrate și a probelor aferente; (m) arhivarea electronică a datelor electronice; (n) înregistrarea într-un registru electronic a datelor electronice și a documentelor în format electronic;	timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger;	i) crearea mărcilor temporale electronice; j) validarea mărcilor temporale electronice; k) prestarea serviciilor de distribuție electronică înregistrate; l) validarea datelor transmise prin intermediul serviciilor de distribuție electronică înregistrate și a probelor aferente; m) arhivarea electronică a datelor electronice; n) înregistrarea într-un registru electronic a datelor electronice și a documentelor în format electronic;				
17. „serviciu de încredere calificat” înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;	(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;	52. serviciu de încredere calificat - serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezenta lege;		Compatibil		
18. „organism de evaluare a conformității” înseamnă un organism de evaluare a conformității în sensul definiției de la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul respectiv 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 ori ca fiind competent să efectueze certificarea portofelelor europene pentru identitatea	(18) 'conformity assessment body' means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or	37. organism de evaluare a conformității - persoană juridică independentă, acreditată în Republica Moldova sau într-un stat membru al Uniunii Europene, având competența de a efectua evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate pe care acesta le prestează ori ca fiind competent să efectueze certificarea portofelelor pentru identitatea digitală sau a mijloacelor de identificare electronică;		Compatibil		

digitală sau a mijloacelor de identificare electronică;	electronic identification means;					
19. „prestator de servicii de încredere” înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;	(19) 'trust service provider' means a natural or legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;	39. prestator de servicii de încredere - persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;		Compatibil		
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;	(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;	40. prestator de servicii de încredere calificat - prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;		Compatibil		
21. „produs” înseamnă hardware sau software ori componente relevante de hardware sau de software destinate să fie utilizate pentru prestarea de servicii de identificare electronică și de servicii de încredere;	(21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services;	41. produs - hardware sau software ori componente relevante de hardware sau de software destinate să fie utilizate pentru prestarea de servicii de identificare electronică și de servicii de încredere;		Compatibil		
22. „dispozitiv de creare a semnăturilor electronice” înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;	(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;	22. dispozitiv de creare a semnăturilor electronice - software sau hardware configurat, utilizat pentru a crea o semnătură electronică;		Compatibil		
23. „dispozitiv de creare a semnăturilor electronice calificat” înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II;	(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;	23. dispozitiv de creare a semnăturilor electronice calificat - dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute la art. 31;		Compatibil		
23a. „dispozitiv calificat de creare a semnăturii electronice la distanță”	(23a) ‘remote qualified electronic signature creation device’ means a	24. dispozitiv calificat de creare a semnăturii electronice la distanță - dispozitiv calificat		Compatibil		

înseamnă un dispozitiv calificat de creare a semnăturii electronice care este gestionat de un prestator de servicii de încredere calificat în conformitate cu articolul 29a în numele unui semnatar;	qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;	de creare a semnăturii electronice care este gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 32 în numele unui semnatar;				
23b. „dispozitiv calificat de creare a sigiliului electronic la distanță” înseamnă un dispozitiv calificat de creare a sigiliului electronic care este gestionat de un prestator de servicii de încredere calificat în conformitate cu articolul 39a în numele unui creator de sigilii;	(23b) ‘remote qualified electronic seal creation device’ means a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;	25. dispozitiv calificat de creare a sigiliului electronic la distanță - dispozitiv calificat de creare a sigiliului electronic care este gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 43 în numele unui creator de sigilii;		Compatibil		
24. „creatorul unui sigiliu” înseamnă o persoană juridică care creează un sigiliu electronic;	(24) 'creator of a seal' means a legal person who creates an electronic seal;	16. creatorul unui sigiliu - persoană juridică care creează un sigiliu electronic;		Compatibil		
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;	(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;	54. 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;		Compatibil		
6. „sigiliu electronic avansat” înseamnă un sigiliu electronic care îndeplinește cerințele prevăzute la articolul 36;	(26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;	55. sigiliu electronic avansat - sigiliu electronic care îndeplinește cerințele prevăzute la art. 38;		Compatibil		
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;	(27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;	56. sigiliu electronic calificat - 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;		Compatibil		

28. „date de creare a sigiliilor electronice” înseamnă date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;	(28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;	19. date de creare a sigiliilor electronice - date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;		Compatibil		
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;	(29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;	11. certificat pentru sigiliul electronic - atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective;		Compatibil		
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;	(30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;	12. certificat calificat pentru sigiliul electronic - certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 40;		Compatibil		
31. „dispozitiv de creare a sigiliului electronic” înseamnă software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;	(31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;	25. dispozitiv de creare a sigiliului electronic - software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;		Compatibil		
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;	(32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;	27. dispozitiv calificat de creare a sigiliului electronic la distanță - dispozitiv calificat de creare a sigiliului electronic care este gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 43 în numele unui creator de sigilii;		Compatibil		
33. „marcă temporală electronică” înseamnă date în format electronic care leagă alte date în format electronic de un anumit	(33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a	31. marcă temporală electronică - date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind		Compatibil		

moment, stabilind dovezi că acestea din urmă au existat la acel moment;	particular time establishing evidence that the latter data existed at that time;	dovezi că acestea din urmă au existat la acel moment;				
34. „marcă temporală electronică calificată” înseamnă o marcă temporală electronică care îndeplinește cerințele prevăzute la articolul 42;	(34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;	32. marcă temporală electronică calificată - marcă temporală electronică care îndeplinește cerințele prevăzute la art. 47;		Compatibil		
35. „document electronic” înseamnă orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;	(35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;	28. document electronic - orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;		Compatibil		
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;	(36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;	49. serviciu de distribuție electronică înregistrată - serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;		Compatibil		
37. „serviciu de distribuție electronică înregistrată calificat” înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la articolul 44;	(37) 'qualified electronic registered delivery service' means an electronic registered delivery service that meets the requirements laid down in Article 44;	50. serviciu de distribuție electronică înregistrată calificat - serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 60;		Compatibil		
38. „certificat pentru autentificarea unui site internet” înseamnă un atestat	(38) 'certificate for website authentication' means an electronic	13. certificat pentru autentificarea unui site internet - atestat electronic		Compatibil		

electronic 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;	attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;	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;				
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;	(39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;	14. certificat calificat pentru autentificarea unui site internet - certificat pentru autentificarea unui site internet care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 50;		Compatibil		
40. „date de validare” înseamnă date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;	(40) 'validation data' means data that is used to validate an electronic signature or electronic seal;	21. date de validare - date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;		Compatibil		
41. „validare” înseamnă procesul prin care se verifică și se confirmă validitatea datelor în format electronic în conformitate cu prezentul regulament;	(41) 'validation' means the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation;	61. validare - procesul prin care se verifică și se confirmă validitatea datelor în format electronic în conformitate cu prezenta lege.		Compatibil		
42. „portofel european pentru identitatea digitală” înseamnă un mijloc de identificare electronică care permite utilizatorului să stocheze, să gestioneze și să valideze în condiții de siguranță datele de identificare personală și atestatele electronice ale atributelor cu scopul de a le furniza beneficiarilor și altor utilizatori ai portofelelor europene pentru identitatea digitală și să semneze prin intermediul semnăturilor electronice calificate sau să	(42) 'European Digital Identity Wallet' means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic	38. portofel pentru identitatea digitală - mijloc de identificare electronică care permite utilizatorului să stocheze, să gestioneze și să valideze în condiții de siguranță datele de identificare personală și atestatele electronice ale atributelor cu scopul de a le furniza beneficiarilor și altor utilizatori ai portofelelor pentru identitatea digitală, precum și să creeze și să aplice semnături electronice calificate sau sigilii electronice calificate;		Compatibil		

sigileze prin intermediul sigiliilor electronice calificate;	signatures or to seal by means of qualified electronic seals;					
43. „atribut” înseamnă o caracteristică, o calitate, un drept sau o permisiune a unei persoane fizice sau juridice sau a unui obiect;	(43) 'attribute' means a characteristic, quality, right or permission of a natural or legal person or of an object;	7. atribut - o caracteristică, o calitate, un drept sau o permisiune a unei persoane fizice sau juridice sau a unui obiect;		Compatibil		
44. „atestat electronic al atributelor” înseamnă un atestat în format electronic care permite atributelor să fie autentificate;	(44) 'electronic attestation of attributes' means an attestation in electronic form that allows the authentication of attributes;	4. atestat electronic al atributelor - atestat în format electronic care permite atributelor să fie autentificate;		Compatibil		
45. „atestat electronic calificat al atributelor” înseamnă un atestat electronic al atributelor care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa V;	(45) 'qualified electronic attestation of attributes' means an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;	5. atestat electronic calificat al atributelor - atestat electronic al atributelor care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 54;		Compatibil		
46. „atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia” înseamnă un atestat electronic al atributelor emis de un organism din sectorul public care este responsabil de o sursă autentică ori de un organism din sectorul public care este desemnat de statul membru să emită astfel de atestate ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice în conformitate cu articolul 45f și cu anexa VII;	(46) 'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' means an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance	6. atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia - atestat electronic al atributelor emis de un organism din sectorul public care este responsabil de o sursă autentică ori de un organism din sectorul public care este desemnat de Guvern să emită astfel de atestate ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice în conformitate cu art.56;		Compatibil		

	with Article 45f and with Annex VII;					
47. „sursă autentică” înseamnă un registru sau un sistem, aflat în responsabilitatea unui organism din sectorul public sau a unei entități private, care conține și pune la dispoziție atribute referitoare la o persoană fizică sau juridică ori la un obiect și care este considerat a fi o sursă primară a informațiilor respective sau care este recunoscut ca fiind autentic în conformitate cu dreptul Uniunii sau cu dreptul intern, inclusiv cu practica administrativă;	(47) 'authentic source' means a repository or system, held under the responsibility of a public sector body or private entity, which contains and provides attributes about a natural or legal person or object, and is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law;	58. sursă autentică - registru sau un sistem, aflat în responsabilitatea unui organism din sectorul public sau a unei entități private, care conține și pune la dispoziție atribute referitoare la o persoană fizică sau juridică ori la un obiect și care este considerat a fi o sursă primară a informațiilor respective sau care este recunoscut ca fiind autentic în conformitate cu cadrul normativ aplicabil;		Compatibil		
48. „arhivare electronică” înseamnă un serviciu care asigură primirea, stocarea, recuperarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe parcursul întregii perioade de păstrare;	(48) 'electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;	3. arhivare electronică - serviciu care asigură primirea, stocarea, recuperarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe parcursul întregii perioade de păstrare;		Compatibil		
49. „serviciu calificat de arhivare electronică” înseamnă un serviciu de arhivare electronică care este prestat de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la articolul 45j;	(49) 'qualified electronic archiving service' means an electronic archiving service provided by a qualified trust service provider and that meets the requirements laid down in Article 45j;	48. serviciu calificat de arhivare electronică - serviciu de arhivare electronică care este prestat de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 60;		Compatibil		

50. „marca de încredere a portofelului UE pentru identitatea digitală” înseamnă o indicație verificabilă, simplă și ușor de recunoscut, care se comunică în mod clar, a faptului că un portofel european pentru identitatea digitală a fost pus la dispoziție în conformitate cu prezentul regulament;	(50) ‘EU Digital Identity Wallet Trust Mark’ means a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;	-		Prevederi UE neaplicabile	Norma este aplicabilă în privința portofelelor UE pentru identitatea digitală furnizate de state membre.	
51. „autentificarea strictă a utilizatorilor” înseamnă o autentificare care se bazează pe utilizarea a cel puțin doi factori de autentificare din categoriile diferite ale cunoștințelor, ceva ce doar utilizatorul cunoaște, ale posesiei, ceva ce doar utilizatorul posedă sau ale inerenței, ceva ce reprezintă utilizatorul, care sunt independenți, în sensul că încălcarea securității unuia dintre factori nu compromite fiabilitatea celorlalți, și care este concepută în așa fel încât să protejeze confidențialitatea datelor de autentificare;	(51) 'strong user authentication' means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;	2. autentificarea strictă a utilizatorilor - procedură de autentificare bazată pe utilizarea a cel puțin doi factori de autentificare din categorii diferite, și anume: cunoștințe (ceva ce doar utilizatorul cunoaște), posesie (ceva ce doar utilizatorul posedă) sau inerență (ceva ce caracterizează utilizatorul), factori care sunt independenți între ei, astfel încât compromiterea unuia dintre factori să nu afecteze fiabilitatea celorlalți, iar mecanismul de autentificare este conceput astfel încât să protejeze confidențialitatea datelor de autentificare;		Compatibil		
52. „registru electronic” înseamnă o secvență de înregistrări electronice de date, care asigură integritatea înregistrărilor respective și acuratețea ordinii cronologice a înregistrărilor respective;	(52) 'electronic ledger' means a sequence of electronic data records, which ensures the integrity of those records and the accuracy of the chronological ordering of those records;	42. registru electronic - secvență de înregistrări electronice de date, care asigură integritatea înregistrărilor respective și acuratețea ordinii cronologice a înregistrărilor respective;		Compatibil		
53. „registru electronic calificat” înseamnă o un	(53) 'qualified electronic ledger' means an	43. registru electronic calificat - un registru		Compatibil		

registru electronic care este pus la dispoziție de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la articolul 45l;	electronic ledger which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45l;	electronic care este pus la dispoziție de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 62;				
54. „date cu caracter personal” înseamnă orice informație în sensul definiției de la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;	(54) 'personal data' means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679;	17. date cu caracter personal - cu sensul definit în Legea nr. 195/2024 privind protecția datelor cu caracter personal;		Compatibil		
55. „corelarea identității” înseamnă un proces prin care datele de identificare personală sau mijloacele de identificare electronică sunt corelate sau asociate cu un cont existent care aparține aceleiași persoane;	(55) 'identity matching' means a process by which person identification data or electronic identification means are matched or associated with an existing account belonging to the same person;	15. corelarea identității - proces prin care datele de identificare personală sau mijloacele de identificare electronică sunt corelate sau asociate cu un cont existent care aparține aceleiași persoane;		Compatibil		
56. „înregistrare de date” înseamnă date electronice înregistrate împreună cu metadatele aferente care susțin prelucrarea datelor;	(56) 'data record' means electronic data recorded together with metadata supporting the processing of data;	30. înregistrare de date - date electronice înregistrate împreună cu metadatele aferente care susțin prelucrarea datelor;		Compatibil		
57. „mod offline” înseamnă, în ceea ce privește utilizarea portofelelor europene pentru identitatea digitală, o interacțiune între un utilizator și o terță parte într-un loc fizic care utilizează tehnologii de proximitate imediată, fără ca portofelul european pentru identitatea digitală să fie necesar pentru accesarea unor sisteme la distanță prin intermediul rețelelor de comunicații electronice în scopul interacțiunii respective.	(57) 'offline mode' means, as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.	34. mod offline - interacțiune între un utilizator și o terță parte într-un loc fizic care utilizează tehnologii de proximitate imediată, fără ca portofelul pentru identitatea digitală să fie necesar pentru accesarea unor sisteme la distanță prin intermediul rețelelor de comunicații electronice în scopul interacțiunii respective;		Compatibil		

		53. serviciu de platformă esențial - oricare dintre următoarele: a) serviciile de intermediere online; b) motoarele de căutare online; c) serviciile de rețele de socializare online; d) serviciile de platformă de partajare a materialelor video; e) serviciile de comunicații interpersonale care nu se bazează pe numere; f) sistemele de operare; g) browserele web; h) asistenții virtuali; i) serviciile de cloud computing; j) serviciile de publicitate online, inclusiv orice rețea de publicitate, schimburile publicitare și orice alt serviciu de intermediere publicitară, prestat de o întreprindere care furnizează oricare dintre serviciile de platformă esențiale enumerate la literele (a)-(i);		Compatibil	Definiție preluată din Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului din 14 septembrie 2022 privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE) 2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale)	
		60. utilizator comercial - persoană fizică sau juridică ce acționează cu titlu comercial sau profesional care utilizează servicii de platformă esențiale în scopul sau în cursul furnizării de bunuri sau servicii către utilizatorii finali;		Compatibil	Definiție preluată din Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului din 14 septembrie 2022 privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE)	

					2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale)	
Articolul 4 **Principiul pieței interne**	**Article 4** **Internal market principle**					
(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.	1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.			Prevederi UE neaplicabile	Norma vizează circulația serviciilor de încredere între statele membre UE	
(2) Produsele și serviciile de încredere care sunt conforme cu prezentul regulament sunt autorizate pentru a circula liber pe piața internă.	2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.			Prevederi UE neaplicabile	Norma vizează circulația serviciilor de încredere între statele membre UE	
Articolul 5 **Pseudonime în tranzacțiile electronice**	**Article 5** **Pseudonyms in electronic transactions**	**Articolul 4.** **Pseudonime în tranzacțiile electronice**				
Fără a aduce atingere normelor specifice din dreptul Uniunii sau din dreptul intern care impun utilizatorilor să se identifice sau efectelor juridice conferite pseudonimelor în temeiul dreptului intern, utilizarea pseudonimelor alese de utilizator nu este interzisă.	Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited.	(1) Utilizarea pseudonimelor alese de utilizatori în cadrul tranzacțiilor electronice este permisă. (2) Prevederile alin. (1) nu aduc atingere obligațiilor legale privind identificarea utilizatorilor, acolo unde aceasta este prevăzută de cadrul normativ aplicabil, și nici efectelor juridice recunoscute pseudonimelor.		Compatibil		
CAPITOLUL II	**CHAPTER II**	**Capitolul II** **IDENTIFICARE ELECTRONICĂ**				

IDENTIFICARE ELECTRONICĂ	**ELECTRONIC IDENTIFICATION**					
SECȚIUNEA 1 **Portofelul european pentru identitatea digitală**	**SECTION 1** **European Digital Identity Wallet**	**Secțiunea 1** **Portofelul pentru identitatea digitală**				
Articolul 5a **Portofelele europene pentru identitatea digitală**	**Article 5a** **European Digital Identity Wallets**	**Articolul 5.** **Portofelele pentru identitatea digitală**				
(1) În scopul garantării faptului că toate persoanele fizice și juridice din Uniune au un acces transfrontalier securizat, fiabil și neîntrerupt la servicii publice și private, păstrând totodată controlul deplin asupra datelor lor, fiecare stat membru furnizează cel puțin un portofel european pentru identitatea digitală în termen de 24 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la alineatul (23) de la prezentul articol și la articolul 5c alineatul (6).	1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).	(1) În scopul asigurării accesului securizat, fiabil și neîntrerupt al persoanelor fizice și juridice din Republica Moldova la servicii publice și private, cu menținerea controlului deplin asupra datelor proprii, Instituția Publică Agenția de Guvernare Electronică asigură disponibilitatea unui portofel pentru identitatea digitală.		Compatibil		
(2) Portofelele europene pentru identitatea digitală sunt furnizate în unul sau mai multe dintre următoarele moduri: (a) direct de către un stat membru; (b) pe baza unui mandat din partea unui stat membru; (c) în mod independent de un stat membru, dar fiind recunoscute de respectivul stat membru.	2. European Digital Identity Wallets shall be provided in one or more of the following ways: (a) directly by a Member State; (b) under a mandate from a Member State; (c) independently from a Member State, but recognised by that Member State.	(2) Portofelele pentru identitatea digitală pot fi puse la dispoziția utilizatorilor și de către furnizori de drept privat, în condițiile prezentei legi.		Compatibil	Norma vizează modul în care statele membre UE pot furniza portofelele europene pentru identitatea digitală	
(3) Codul sursă al componentelor de software	3. The source code of the application software	(3) Codul sursă al componentelor de software ale		Compatibil		

ale aplicației portofelelor europene pentru identitatea digitală face obiectul unei licențe cu sursă deschisă. Statele membre pot prevedea ca, din motive justificate în mod corespunzător, codul sursă al anumitor componente, altele decât cele instalate pe dispozitivele utilizatorilor, să nu fie divulgat.	components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.	aplicației portofelelor pentru identitatea digitală face obiectul unei licențe cu sursă deschisă. (4) În cazuri justificate în mod corespunzător, organismul de supraveghere poate decide nepublicarea codului sursă al anumitor componente ale sistemului, altele decât cele instalate pe dispozitivele utilizatorilor, în măsura în care divulgarea acestuia ar putea afecta securitatea, integritatea sau funcționarea sistemului.				
(4) Portofelele europene pentru identitatea digitală permit utilizatorului, într-un mod transparent și ușor de utilizat și de urmărit de către acesta: (a) să solicite, să obțină, să selecteze, să combine, să stocheze, să șteargă, să partajeze și să prezinte în condiții de siguranță, exclusiv sub controlul utilizatorului, datele de identificare personală și, după caz, în combinație cu atestate electronice ale atributelor, să se autentifice beneficiarilor online și, după caz, în mod offline, pentru a accesa servicii publice și private, asigurând, în același timp, că este posibilă divulgarea selectivă a datelor; (b) să genereze pseudonime și să le stocheze local și în formă criptată în portofelul european pentru identitatea digitală;	4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible; (b) generate pseudonyms and store	(5) Portofelele pentru identitatea digitală permit utilizatorului, într-un mod transparent și ușor de utilizat și de urmărit de către acesta: 1) să solicite, să obțină, să selecteze, să combine, să stocheze, să șteargă, să partajeze și să prezinte în condiții de siguranță, exclusiv sub controlul utilizatorului, datele de identificare personală și, după caz, în combinație cu atestate electronice ale atributelor, să se autentifice beneficiarilor online și, după caz, în mod offline, pentru a accesa servicii publice și private, asigurând, în același timp, că este posibilă divulgarea selectivă a datelor; 2) să genereze pseudonime și să le stocheze local și în formă criptată în portofelul pentru identitatea digitală; 3) să autentifice în condiții de siguranță portofelul		Compatibil		

(c) să autentifice în condiții de siguranță portofelul european pentru identitatea digitală al unei alte persoane și să primească și partajeze date de identificare personală și atestate electronice ale atributelor într-un mod securizat între cele două portofele europene pentru identitatea digitală; (d) să acceseze o evidență a tuturor tranzacțiilor efectuate cu ajutorul portofelului european pentru identitatea digitală prin intermediul unui tablou de bord comun care să permită utilizatorului: (i) să vizualizeze o listă actualizată a beneficiarilor cu care utilizatorul a stabilit o conexiune și, după caz, a tuturor datelor partajate; (ii) să solicite cu ușurință unui beneficiar să șteargă datele cu caracter personal în temeiul articolului 17 din Regulamentul (UE) 2016/679; (iii) să semnaleze cu ușurință un beneficiar autorității naționale competente pentru protecția datelor, atunci când se primește o cerere de date presupus ilegală sau suspectă; (e) să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate;	them encrypted and locally within the European Digital Identity Wallet; (c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets; (d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to: (i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged; (ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679; (iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received; (e) sign by means of qualified electronic signatures or seal by	pentru identitatea digitală al unei alte persoane și să primească și partajeze date de identificare personală și atestate electronice ale atributelor într-un mod securizat între cele două portofele pentru identitatea digitală; 4) să acceseze o evidență a tuturor tranzacțiilor efectuate cu ajutorul portofelului pentru identitatea digitală prin intermediul unui tablou de bord comun care să permită utilizatorului: a) să vizualizeze o listă actualizată a beneficiarilor cu care utilizatorul a stabilit o conexiune și, după caz, a tuturor datelor partajate; b) să solicite cu ușurință unui beneficiar să șteargă datele cu caracter personal în temeiul art. 17 al Legii nr. 195/2024 privind protecția datelor cu caracter personal; c) să semnaleze cu ușurință un beneficiar autorității naționale pentru protecția datelor cu caracter personal, atunci când se primește o cerere de date presupus ilegală sau suspectă; 5) să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate; 6) să descarce, în măsura în care acest lucru este fezabil din punct de vedere tehnic, datele, atestatul				

(f) să descarce, în măsura în care acest lucru este fezabil din punct de vedere tehnic, datele, atestatul electronic al atributelor și configurațiile utilizatorului; (g) să exercite dreptul utilizatorului la portabilitatea datelor.	means of qualified electronic seals; (f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations; (g) exercise the user's rights to data portability.	electronic al atributelor și configurațiile utilizatorului; 7) să exercite dreptul utilizatorului la portabilitatea datelor.				
(5) În special, portofelele europene pentru identitatea digitală: (a) permit utilizarea unor protocoale și interfețe comune: (i) pentru emiterea datelor de identificare personală, a atestatelor electronice calificate și necalificate ale atributelor sau a certificatelor calificate și necalificate către portofelul european pentru identitatea digitală; (ii) pentru ca beneficiarii să solicite și să valideze date de identificare personală și atestate electronice ale atributelor; (iii) pentru partajarea și prezentarea către beneficiari a datelor de identificare personală, a atestatului electronic al atributelor sau a datelor conexe divulgate selectiv online și, după caz, în mod offline; (iv) pentru ca utilizatorul să permită interacțiunea cu portofelul european pentru identitatea digitală și să afișeze o marcă de încredere a portofelului UE pentru identitatea digitală;	5. European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: (i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet; (ii) for relying parties to request and validate person identification data and electronic attestations of attributes; (iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode; (iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital	5. În special, portofelele pentru identitatea digitală: 1) permit utilizarea unor protocoale și interfețe comune: a. pentru emiterea datelor de identificare personală, a atestatelor electronice calificate și necalificate ale atributelor sau a certificatelor calificate și necalificate către portofelul pentru identitatea digitală; b. pentru ca beneficiarii să solicite și să valideze date de identificare personală și atestate electronice ale atributelor; c. pentru partajarea și prezentarea către beneficiari a datelor de identificare personală, a atestatului electronic al atributelor sau a datelor conexe divulgate selectiv online și, după caz, în mod offline; d. pentru a realiza integrarea în condiții de siguranță a utilizatorului prin utilizarea unui mijloc de identificare electronică în modul stabilit de Guvern e. pentru interacțiunea între portofelele pentru identitatea digitală a două		Compatibil		

(v) pentru a realiza integrarea în condiții de siguranță a utilizatorului prin utilizarea unui mijloc de identificare electronică în conformitate cu articolul 5a alineatul (24); (vi) pentru interacțiunea între portofelele europene pentru identitatea digitală a două persoane în scopul de a primi, a valida și a partaja date de identificare personală și atestate electronice ale atributelor într-un mod securizat; (vii) pentru autentificarea și identificarea beneficiarilor prin punerea în aplicare a mecanismelor de autentificare în conformitate cu articolul 5b; (viii) pentru ca beneficiarii să verifice autenticitatea și valabilitatea portofelelor europene pentru identitatea digitală; (ix) pentru a solicita unui beneficiar să șteargă datele cu caracter personal în temeiul articolului 17 din Regulamentul (UE) 2016/679; (x) pentru a semnala un beneficiar autorității naționale pentru protecția datelor competente în cazul în care se primește o cerere de date presupus ilegală sau suspectă; (xi) pentru crearea de semnături sau sigilii electronice calificate prin intermediul dispozitivelor de creare a semnăturilor	Identity Wallet Trust Mark; (v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24); (vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner; (vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b; (viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets; (ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679; (x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received; (xi) for the creation of qualified electronic signatures or electronic	persoane în scopul de a primi, a valida și a partaja date de identificare personală și atestate electronice ale atributelor într-un mod securizat; f. pentru autentificarea și identificarea beneficiarilor prin punerea în aplicare a mecanismelor de autentificare în conformitate cu art. 6; g. pentru ca beneficiarii să verifice autenticitatea și valabilitatea portofelelor pentru identitatea digitală; h. pentru a solicita unui beneficiar să șteargă datele cu caracter personal în temeiul articolului 17 al Legii nr. 195/2024 privind protecția datelor cu caracter personal; i. pentru a semnala un beneficiar autorității naționale pentru protecția datelor cu caracter personal în cazul în care se primește o cerere de date presupus ilegală sau suspectă; j. pentru crearea de semnături sau sigilii electronice calificate prin intermediul dispozitivelor de creare a semnăturilor electronice sau a sigiliilor electronice calificate; 2) nu oferă prestatorilor de servicii de încredere care furnizează atestate electronice ale atributelor nicio informație cu privire la utilizarea respectivelor atestate electronice; 3) asigură faptul că beneficiarii pot fi autentificați și identificați prin			

electronice sau a sigiliilor electronice calificate; (b) nu oferă prestatorilor de servicii de încredere care furnizează atestate electronice ale atributelor nicio informație cu privire la utilizarea respectivelor atestate electronice; (c) asigură faptul că beneficiarii pot fi autentificați și identificați prin punerea în aplicare a unor mecanisme de autentificare în conformitate cu articolul 5b; (d) îndeplinesc cerințele prevăzute la articolul 8 în ceea ce privește nivelul de asigurare ridicat, în special în ceea ce privește cerințele privind dovedirea și verificarea identității, precum și gestionarea și autentificarea mijloacelor de identificare electronică; (e) în cazul atestatelor electronice ale atributelor cu politici de divulgare încorporate, pune în aplicare mecanismul adecvat pentru a informa utilizatorul că beneficiarul sau utilizatorul portofelului european pentru identitatea digitală care solicită atestatul electronic al atributelor în cauză are permisiunea de a accesa astfel de atestate; (f) asigură faptul că datele de identificare personală, care sunt disponibile din sistemul de identificare electronică în cadrul căruia este furnizat portofelul european pentru	seals by means of qualified electronic signature or electronic seal creation devices; (b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations; (c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b; (d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication; (e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the	punerea în aplicare a unor mecanisme de autentificare în conformitate cu art. 6; 4) îndeplinesc cerințele prevăzute la art. 12 în ceea ce privește nivelul de asigurare ridicat, în special în ceea ce privește cerințele privind dovedirea și verificarea identității, precum și gestionarea și autentificarea mijloacelor de identificare electronică; 5) în cazul atestatelor electronice ale atributelor cu politici de divulgare încorporate, pune în aplicare mecanismul adecvat pentru a informa utilizatorul că beneficiarul sau utilizatorul portofelului pentru identitatea digitală care solicită atestatul electronic al atributelor în cauză are permisiunea de a accesa astfel de atestate; 6) asigură faptul că datele de identificare personală, care sunt disponibile din sistemul de identificare electronică în cadrul căruia este furnizat portofelul pentru identitatea digitală, reprezintă în mod unic persoana fizică, persoana juridică sau persoana fizică ce reprezintă persoana fizică sau juridică și sunt asociate cu respectivul portofel pentru identitatea digitală; 7) oferă tuturor persoanelor fizice posibilitatea de a semna prin intermediul semnăturilor electronice calificate în mod implicit și gratuit.				

identitatea digitală, reprezintă în mod unic persoana fizică, persoana juridică sau persoana fizică ce reprezintă persoana fizică sau juridică și sunt asociate cu respectivul portofel european pentru identitatea digitală; (g) oferă tuturor persoanelor fizice posibilitatea de a semna prin intermediul semnăturilor electronice calificate în mod implicit și gratuit. Prin excepție de la dispozițiile de la primul paragraf litera (g), statele membre pot să prevadă măsuri proporționale pentru a asigura faptul că utilizarea gratuită a semnăturilor electronice calificate de către persoanele fizice este limitată la scopuri neprofesionale.	permission to access such attestation; (f) ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet; (g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge. Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.					
(6) Statele Membre informează utilizatorii, fără întârziere, despre orice încălcare a securității care le-ar fi putut compromite total sau parțial portofelul european pentru identitatea digitală sau conținutul lui, în	6. Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its	(7) Furnizorii de portofele pentru identitatea digitală informează utilizatorii, fără întârziere, despre orice încălcare a securității care le-ar fi putut compromite total sau parțial portofelul pentru identitatea		Compatibil		

special dacă portofelul european pentru identitatea digitală al utilizatorilor a fost suspendat sau revocat în conformitate cu articolul 5e.	contents, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.	digitală sau conținutul lui, în special dacă portofelul pentru identitatea digitală al utilizatorilor a fost suspendat sau revocat în conformitate cu art. 9.				
(7) Fără a aduce atingere articolul 5f, statele membre pot să prevadă, în conformitate cu dreptul intern, funcționalități suplimentare ale portofelelor europene pentru identitatea digitală, inclusiv interoperabilitatea cu mijloacele naționale de identificare electronică existente. Aceste funcționalități suplimentare trebuie să fie conforme cu prezentul articol.	7. Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply with this Article.	(8) Fără a aduce atingere art. 10, Guvernul poate să prevadă, funcționalități suplimentare ale portofelelor pentru identitatea digitală, inclusiv interoperabilitatea cu mijloacele naționale de identificare electronică existente. Aceste funcționalități suplimentare trebuie să fie conforme cu prezentul articol.		Compatibil		
(8) Statele membre pun la dispoziție cu titlu gratuit mecanisme de validare pentru: (a) a asigura faptul că autenticitatea și valabilitatea portofelelor europene pentru identitatea digitală pot fi verificate; (b) a permite utilizatorilor să verifice autenticitatea și valabilitatea identității beneficiarilor înregistrați în conformitate cu articolul 5b.	8. Member States shall provide validation mechanisms free-of-charge, in order to: (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified; (b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.	(9) Furnizorii de portofele pentru identitatea digitală pun la dispoziție cu titlu gratuit mecanisme de validare pentru: a) a asigura faptul că autenticitatea și valabilitatea portofelelor pentru identitatea digitală pot fi verificate; b) a permite utilizatorilor să verifice autenticitatea și valabilitatea identității beneficiarilor înregistrați în conformitate cu art. 6.		Compatibil		
(9) Statele membre se asigură că valabilitatea portofelului european pentru identitatea digitală poate fi revocată în următoarele circumstanțe:	9. Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances:	(10) Furnizorii de portofele pentru identitatea digitală se asigură că valabilitatea portofelului pentru identitatea digitală poate fi revocată în următoarele circumstanțe:		Compatibil		

(a) la cererea explicită a utilizatorului; (b) în cazul în care a fost compromisă securitatea portofelului european pentru identitatea digitală; (c) în caz de deces al utilizatorului sau de încetare a activității persoanei juridice.	(a) upon the explicit request of the user; (b) where the security of the European Digital Identity Wallet has been compromised; (c) upon the death of the user or cease of activity of the legal person.	a) la cererea explicită a utilizatorului; b) în cazul în care a fost compromisă securitatea portofelului pentru identitatea digitală; c) în caz de deces al utilizatorului sau de încetare a activității persoanei juridice.				
(10) Furnizorii de portofele europene pentru identitatea digitală se asigură că utilizatorii pot solicita cu ușurință asistență tehnică și pot raporta problemele tehnice sau orice alte incidente care au impact negativ asupra utilizării portofelului european pentru identitatea digitală.	10. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Digital Identity Wallets.	(11) Furnizorii de portofele pentru identitatea digitală se asigură că utilizatorii pot solicita cu ușurință asistență tehnică și pot raporta problemele tehnice sau orice alte incidente care au impact negativ asupra utilizării portofelului pentru identitatea digitală.		Compatibil		
(11) Portofelele europene pentru identitatea digitală sunt furnizate în cadrul unui sistem de identificare electronică având nivelul de asigurare ridicat.	11. European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.	(12) Portofelele pentru identitatea digitală sunt furnizate în cadrul unui sistem de identificare electronică având nivelul de asigurare ridicat.		Compatibil		
(12) Portofelele europene pentru identitatea digitală garantează securitatea de la stadiul conceperii.	12. European Digital Identity Wallets shall ensure security-by-design.	(13) Portofelele pentru identitatea digitală sunt proiectate și dezvoltate în conformitate cu principiul securității încă din stadiul conceperii, prin integrarea unor măsuri tehnice și organizatorice adecvate care să asigure confidențialitatea, integritatea, disponibilitatea și autenticitatea datelor și serviciilor asociate, pe întregul ciclu de viață al portofelului.		Compatibil		
(13) Portofelele europene pentru identitatea digitală se emit, se utilizează și sunt	13. The issuance, use and revocation of the European Digital	(14) Portofelele pentru identitatea digitală se emit, se utilizează și sunt revocate în		Compatibil		

revocate în mod gratuit pentru toate persoanele fizice.	Identity Wallets shall be free of charge to all natural persons.	mod gratuit pentru toate persoanele fizice.				
(14) Utilizatorii au controlul deplin asupra utilizării portofelului lor european pentru identitatea digitală și asupra datelor din acesta. Furnizorul portofelului european pentru identitatea digitală nu colectează informații cu privire la utilizarea portofelului european pentru identitatea digitală care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul european pentru identitatea digitală și nici nu combină date de identificare personală sau orice alte date cu caracter personal stocate sau legate de utilizarea portofelului european pentru identitatea digitală cu date cu caracter personal provenind de la orice alte servicii oferite de respectivul furnizor sau de la servicii furnizate de terți care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul european pentru identitatea digitală, cu excepția cazului în care utilizatorul a solicitat în mod expres contrariul. Datele cu caracter personal legate de punerea la dispoziție de portofele europene pentru identitatea digitală sunt păstrate separate logic de orice alte date deținute de furnizorul de portofele europene pentru identitatea	14. Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital	(15) Utilizatorii au controlul deplin asupra utilizării portofelului lor pentru identitatea digitală și asupra datelor din acesta. Furnizorul portofelului pentru identitatea digitală nu colectează informații cu privire la utilizarea portofelului pentru identitatea digitală care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul pentru identitatea digitală și nici nu combină date de identificare personală sau orice alte date cu caracter personal stocate sau legate de utilizarea portofelului pentru identitatea digitală cu date cu caracter personal provenind de la orice alte servicii oferite de respectivul furnizor sau de la servicii furnizate de terți care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul pentru identitatea digitală, cu excepția cazului în care utilizatorul a solicitat în mod expres contrariul. Datele cu caracter personal legate de punerea la dispoziție de portofele pentru identitatea digitală sunt păstrate separate logic de orice alte date deținute de furnizorul de portofele pentru identitatea digitală.		Compatibil		

digitală. În cazul în care portofelul european pentru identitatea digitală este furnizat de părți private în conformitate cu alineatul (2) literele (b) și (c) de la prezentul articol, dispozițiile articolului 45h alineatul (3) se aplică mutatis mutandis.	Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply mutatis mutandis.					
(15) Utilizarea portofelelor europene pentru identitatea digitală este voluntară. Accesul la serviciile publice și private rămâne posibil prin alte mijloace de identificare și autentificare existente.	15. The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.	(16) Utilizarea portofelelor pentru identitatea digitală este voluntară. Accesul la serviciile publice și private, accesul la piața muncii și libertatea de a desfășura o activitate comercială nu sunt în niciun fel restricționate sau permise în condiții mai dezavantajoase pentru persoanele fizice sau juridice care nu utilizează portofelele pentru identitatea digitală. Accesul la serviciile publice și private rămâne posibil prin alte mijloace de identificare și autentificare existente.		Compatibil		
(16) Cadrul tehnic al portofelului european pentru identitatea digitală: (a) nu permite furnizorilor de atestate electronice ale atributelor sau oricărei alte părți, după emiterea atestatelor atributelor, să obțină date care permit urmărirea, conectarea sau corelarea tranzacțiilor sau a comportamentul utilizatorului sau obținerea în alt mod de cunoștințe privind tranzacțiile sau	16. The technical framework of the European Digital Identity Wallet shall: (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of	(17) Cadrul tehnic al portofelului pentru identitatea digitală: a) nu permite furnizorilor de atestate electronice ale atributelor sau oricărei alte părți, după emiterea atestatelor atributelor, să obțină date care permit urmărirea, conectarea sau corelarea tranzacțiilor sau a comportamentul utilizatorului sau obținerea în alt mod de cunoștințe privind tranzacțiile sau		Compatibil		

comportamentul utilizatorului, cu excepția cazului în care utilizatorul autorizează în mod explicit acest lucru; (b) permite aplicarea unor tehnici de protecție a vieții private care asigură imposibilitatea stabilirii unei legături, în cazul în care atestarea atributelor nu necesită identificarea utilizatorului.	transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user; (b) enable privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user.	comportamentul utilizatorului, cu excepția cazului în care utilizatorul autorizează în mod explicit acest lucru; b) permite aplicarea unor tehnici de protecție a vieții private care asigură imposibilitatea stabilirii unei legături, în cazul în care atestarea atributelor nu necesită identificarea utilizatorului.				
(17) Orice prelucrare a datelor cu caracter personal efectuată de statele membre sau, în numele acestora, de organisme sau părți responsabile de furnizarea portofelelor europene pentru identitatea digitală drept mijloace de identificare electronică se efectuează în conformitate cu măsuri adecvate și eficace de protecție a datelor. Trebuie să se demonstreze conformitatea unei astfel de prelucrări cu Regulamentul (UE) 2016/679. Statele membre pot adopta dispoziții de drept intern pentru a preciza mai în detaliu aplicarea acestor măsuri.	17. Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated. Member States may introduce national provisions to further specify the application of such measures.	(18) Orice prelucrare a datelor cu caracter personal efectuată furnizorii de portofele pentru identitatea digitală se efectuează în conformitate cu prevederile Legii nr. 195/2024 privind protecția datelor cu caracter personal, aplicând măsuri adecvate și eficace de protecție a datelor.		Compatibil		
(18) Statele membre transmit Comisiei, fără întârzieri nejustificate, informații cu privire la: (a) organismul responsabil cu întocmirea și menținerea listei beneficiarilor înregistrați care recurg la portofelele europene pentru	18. Member States shall, without undue delay, notify the Commission of information about: (a) the body responsible for establishing and maintaining the list of registered relying parties	(19) Organismul de supraveghere publică, printr-un canal securizat și într-un format care permite prelucrarea automată, semnat electronic sau sigilat electronic, fără întârzieri nejustificate, informațiile privind:		Compatibil	Prevederea din Regulamentul UE este concepută pentru mecanismul instituțional specific Uniunii Europene, astfel, pentru Republica Moldova, aceste aspecte pot fi	

identitatea digitală în conformitate cu articolul 5b alineatul (5) și localizarea acestei liste; (b) organismele responsabile de furnizarea portofelelor europene pentru identitatea digitală în conformitate cu articolul 5a alineatul (1); (c) organismele responsabile de asigurarea faptului că datele de identificare personală sunt asociate cu portofelul european pentru identitatea digitală în conformitate cu articolul 5a alineatul (5) litera (f); (d) mecanismul care permite validarea datelor de identificare personală menționate la articolul 5a alineatul (5) litera (f) și a identității beneficiarilor; (e) mecanismul de validare a autenticității și valabilității portofelelor europene pentru identitatea digitală. Comisia pune informațiile transmise în temeiul primului paragraf la dispoziția publicului prin intermediul unui canal sigur, într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.	that rely on European Digital Identity Wallets in accordance with Article 5b(5) and the location of that list; (b) the bodies responsible for the provision of European Digital Identity Wallets in accordance with Article 5a(1); (c) the bodies responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f); (d) the mechanism allowing for the validation of the person identification data referred to in Article 5a(5), point (f), and of the identity of the relying parties; (e) the mechanism by which to validate the authenticity and validity of European Digital Identity Wallets. The Commission shall make available the information notified pursuant to the first subparagraph to the public through a secure channel, in electronically signed or sealed form suitable for automated processing.	a) mecanismul de întocmire și menținere a listei beneficiarilor înregistrați care recurg la portofelele pentru identitatea digitală în conformitate cu art. 6 și localizarea acestei liste; b) lista furnizorilor portofelelor pentru identitatea digitală; c) organismele din sectorul public responsabile de asigurarea faptului că datele de identificare personală sunt asociate cu portofelul pentru identitatea digitală în conformitate cu alin. (6) pct. 6); d) mecanismul care permite validarea datelor de identificare personală menționate la alin. (6) pct. 6) și a identității beneficiarilor; e) mecanismul de validare a autenticității și valabilității portofelelor pentru identitatea digitală.			reglementate la nivel național, fără mecanismul de notificare către Comisie.	
(19) Fără a aduce atingere alineatului (22) de la	19. Without prejudice to paragraph 22 of this					

prezentul articol, articolul 11 se aplică mutatis mutandis portofelului european pentru identitatea digitală.	Article, Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.					
(20) Articolul 24 alineatul (2) litera (b) și literele (d)-(h) se aplică mutatis mutandis furnizorilor de portofelele europene pentru identitatea digitală.	20. Article 24(2), points (b), and (d) to (h), shall apply mutatis mutandis to providers of European Digital Identity Wallets.	(20) Dispozițiile art. 24 alin. (4) pct. 2) și pct. 4)-10) sunt aplicabile și furnizorilor de portofele pentru identitatea digitală.		Compatibil		
(21) Se asigură accesibilitatea portofelelor europene pentru identitatea digitală pentru ca persoanele cu dizabilități să le poată utiliza în aceleași condiții ca și ceilalți utilizatori, în conformitate cu Directiva (UE) 2019/882 a Parlamentului European și a Consiliului.	21. European Digital Identity Wallets shall be made accessible for use, by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council.	(21) Se asigură accesibilitatea portofelelor pentru identitatea digitală pentru ca persoanele cu dizabilități să le poată utiliza în aceleași condiții ca și ceilalți utilizatori.		Compatibil		
(22) În scopul furnizării portofelelor europene pentru identitatea digitală, portofelelor europene pentru identitatea digitală și sistemelor de identificare electronică în cadrul cărora sunt furnizate nu li se aplică cerințele prevăzute la articolele 7, 9, 10, 12 și 12a.	22. For the purposes of the provision of European Digital Identity Wallets, European Digital Identity Wallets and the electronic identification schemes under which they are provided shall not be subject to the requirements laid down in Articles 7, 9, 10, 12 and 12a.	(22) În scopul furnizării portofelelor pentru identitatea digitală, portofelelor pentru identitatea digitală și sistemelor de identificare electronică în cadrul cărora sunt furnizate nu li se aplică cerințele prevăzute la art. 16.		Compatibil		
(23) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatele (4), (5), (8) și	23. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele		Compatibil		

(18) de la prezentul articol, privind implementarea portofelului european pentru identitatea digitală. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	normative necesare punerii în aplicare a prevederilor prezentei legi.				
(24) Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații tehnice și proceduri pentru a facilita integrarea utilizatorilor în sistemul reprezentat de portofelul european pentru identitatea digitală fie prin mijloace de identificare electronică conforme cu nivelul de asigurare ridicat, fie prin mijloace de identificare electronică conforme cu nivelul de asigurare substanțial combinate cu proceduri suplimentare de integrare la distanță care, împreună, îndeplinesc cerințele nivelului de asigurare ridicat. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	24. The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 5b	**Article 5b**	**Articolul 6**				

Beneficiarii portofelului european pentru identitatea digitală	**Relying parties of the European Digital Identity Wallet**	**Beneficiarii portofelului pentru identitatea digitală**				
(1) În cazul în care un beneficiar intenționează să recurgă la portofele europene pentru identitatea digitală pentru furnizarea de servicii publice sau private prin intermediul interacțiunii digitale, beneficiarul se înregistrează în statul membru în care este stabilit.	1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.	(1) În cazul în care un beneficiar intenționează să recurgă la portofele pentru identitatea digitală pentru furnizarea de servicii publice sau private prin intermediul interacțiunii digitale, beneficiarul se înregistrează în lista beneficiarilor din Republica Moldova gestionată de organismul de supraveghere.		Compatibil		
(2) Procesul de înregistrare este eficient din punctul de vedere al costurilor și proporțional cu riscurile. Beneficiarul furnizează cel puțin: (a) informațiile necesare pentru autentificarea în portofelele europene pentru identitatea digitală, informații care includ cel puțin: (i) statul membru în care este stabilit beneficiarul; și (ii) numele beneficiarului și, după caz, numărul său de înregistrare, astfel cum figurează într-un registru oficial, împreună cu datele de identificare ale respectivului registru oficial; (b) datele de contact ale beneficiarului; (c) utilizarea preconizată a portofelelor europene pentru identitatea digitală, inclusiv menționarea datelor pe care	2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least: (a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes: (i) the Member State in which the relying party is established; and (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record; (b) the contact details of the relying party; (c) the intended use of European Digital Identity Wallets, including an indication	(2) Procesul de înregistrare se desfășoară prin intermediul Portalului guvernamental integrat EVO și este eficient din punctul de vedere al costurilor și proporțional cu riscurile, iar beneficiarul furnizează cel puțin: a) informațiile necesare pentru autentificarea în portofelele pentru identitatea digitală, informații care includ cel puțin numele beneficiarului și numărul său de înregistrare de stat; b) datele de contact ale beneficiarului; c) utilizarea preconizată a portofelelor pentru identitatea digitală, inclusiv menționarea datelor pe care beneficiarul urmează să le solicite utilizatorilor.		Compatibil		

beneficiarul urmează să le solicite utilizatorilor.	of the data to be requested by the relying party from users.					
(3) Beneficiarii nu solicită utilizatorilor să furnizeze alte date decât cele menționate în temeiul alineatului (2) litera (c).	3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).	(3) Beneficiarii nu solicită utilizatorilor să furnizeze alte date decât cele menționate în temeiul alin. (2) lit. (c).		Compatibil		
(4) Alineatele (1) și (2) nu aduc atingere dreptului Uniunii sau dreptului intern care se aplică prestării de servicii specifice.	4. Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.	(4) Prevederile alin. (1) și (2) nu aduc atingere cadrului normativ aplicabil prestării serviciilor specifice.		Compatibil		
(5) Statele membre pun la dispoziția publicului online informațiile menționate la alineatul (2), într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.	5. Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.	(5) Organismul de supraveghere pune la dispoziția publicului online informațiile menționate la alineatul (2), într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.		Compatibil		
(6) Beneficiarii înregistrați în conformitate cu prezentul articol informează fără întârziere statele membre cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alineatului (2).	6. Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.	(6) Beneficiarii înregistrați în conformitate cu prezentul articol informează fără întârziere organismul de supraveghere cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alin. (2).		Compatibil		
(7) Statele membre stabilesc un mecanism comun care să permită identificarea și autentificarea beneficiarilor, astfel cum se menționează la articolul 5a alineatul (5) litera (c).	7. Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 5a(5), point (c).			Prevederi UE neaplicabile	Mecanismul comun pentru identificarea și autentificarea beneficiarilor urmează a fi stabilit de statele membre ale Uniunii Europene, iar Republica Moldova, nefiind stat membru, nu participă la	

					instituirea acestuia, urmând să se alinieze ulterior mecanismului deja stabilit la nivelul Uniunii Europene.	
(8) Atunci când intenționează să recurgă la portofele europene pentru identitatea digitală, beneficiarii se identifică față de utilizator.	8. Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user.	(7) Atunci când intenționează să recurgă la portofele pentru identitatea digitală, beneficiarii se identifică față de utilizator.		Compatibil		
(9) Beneficiarii sunt responsabili de îndeplinirea procedurii de autentificare și validare a datelor de identificare personală și de atestare electronică a atributelor solicitate în cadrul portofelelor europene pentru identitatea digitală. Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care dreptul Uniunii sau de dreptul intern nu impun identificarea utilizatorului.	9. Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.	(8) Beneficiarii sunt responsabili de îndeplinirea procedurii de autentificare și validare a datelor de identificare personală și de atestare electronică a atributelor solicitate în cadrul portofelelor europene pentru identitatea digitală. Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care cadrul normativ aplicabil nu impune identificarea utilizatorului.		Compatibil		
(10) Intermediarii care acționează în numele beneficiarilor sunt considerați beneficiari și nu stochează date cu privire la conținutul tranzacției.	10. Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.	(9) Intermediarii care acționează în numele beneficiarilor sunt considerați beneficiari și nu stochează date cu privire la conținutul tranzacției.		Compatibil		
(11) Până la 21 noiembrie 2024, Comisia stabilește specificațiile tehnice și procedurile privind cerințele prevăzute la alineatele (2), (5) și (6)-(9) de la prezentul articol prin intermediul unor acte de punere în aplicare	11. By 21 November 2024, the Commission shall establish technical specifications and procedures for the requirements referred to in paragraphs 2, 5 and 6 to 9 of this Article by	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura		Compatibil		

privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se menționează la articolul 5a alineatul (23). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
Articolul 5c **Certificarea portofelelor europene pentru identitatea digitală**	**Article 5c** **Certification of European Digital Identity Wallets**	**Articolul 7.** **Certificarea portofelelor pentru identitatea digitală**				
(1) Conformitatea portofelelor europene pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia sunt furnizate cu cerințele prevăzute la articolul 5a alineatele (4), (5) și (8), cu cerința privind separarea logică prevăzută la articolul 5a alineatul (14) și, după caz, cu standardele și specificațiile tehnice menționate la articolul 5a alineatul (24) este certificată de organisme de evaluare a conformității desemnate de statele membre.	1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.	(1) Conformitatea portofelelor pentru identitatea digitală, precum și a sistemului de identificare electronică în cadrul căruia acestea sunt furnizate, cu cerințele prevăzute la art. 5, precum și cu standardele și specificațiile tehnice stabilite de Guvern, se certifică de către organisme de evaluare a conformității acreditate.		Compatibil	La art. 7 alin. (1) se propune instituirea unei norme cu caracter general din care să rezulte că conformitatea portofelelor pentru identitatea digitală cu cerințele prevăzute la art. 5, inclusiv din perspectiva securității cibernetice, precum și cu standardele și specificațiile tehnice stabilite de Guvern, se certifică de către organisme de evaluare a conformității acreditate.	
(2) Certificarea conformității portofelelor europene pentru identitatea digitală cu cerințele menționate la alineatul (1) de la prezentul articol care sunt relevante în materie de	2. Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant					

securitate cibernetică sau cu părți ale acestora se efectuează în conformitate cu sistemele europene de certificare a securității cibernetice adoptate în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului (4) și indicate în actele de punere în aplicare menționate la alineatul (6) de la prezentul articol.	for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council (4) and referred to in the implementing acts referred to in paragraph 6 of this Article.					
(3) Pentru cerințele menționate la alineatul (1) de la prezentul articol care nu sunt relevante în materie de securitate cibernetică și pentru cerințele menționate la alineatul (1) de la prezentul articol care sunt relevante în materie de securitate cibernetică, în măsura în care sistemele de certificare a securității cibernetice menționate la alineatul (2) de la prezentul articol nu acoperă sau acoperă doar parțial cerințele de securitate cibernetică respective, statele membre instituie, și pentru respectivele cerințe, sisteme de certificare naționale în conformitate cu cerințele stabilite în actele de punere în aplicare menționate la alineatul (6) de la prezentul articol. Statele membre transmit proiectele lor de sisteme de certificare naționale Grupului european de cooperare privind identitatea	3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group					

digitală constituit în temeiul articolului 46e alineatul (1) (denumit în continuare „grupul de cooperare”) Grupul de cooperare poate emite avize și recomandări.	established pursuant to Article 46e(1) (the ‘Cooperation Group’). The Cooperation Group may issue opinions and recommendations.					
(4) Certificarea realizată în temeiul la alineatului (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția efectuării unei evaluări a vulnerabilității la fiecare doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în timp util, certificarea este anulată.	4. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled. 5. Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation(EU) 2016/679.	(2) Certificarea realizată în temeiul la alin. (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția efectuării unei evaluări a vulnerabilității la fiecare doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în timp util, certificarea este anulată.		Compatibil		
(5) Respectarea cerințelor stabilite la articolul 5a din prezentul regulament referitoare la operațiunile de prelucrare a datelor cu caracter personal poate să fie certificată în temeiul Regulamentului (UE) 2016/679.	5. Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation(EU) 2016/679.	(3) Respectarea cerințelor stabilite la art. 5 referitoare la operațiunile de prelucrare a datelor cu caracter personal poate să fie certificată în temeiul art. 42 din Legea nr. 195/2024 privind protecția datelor cu caracter personal.		Compatibil		
(6) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificarea	6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura		Compatibil		

portofelelor europene pentru identitatea digitală menționată la alineatele (1), (2) și (3) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
(7) Statele membre comunică Comisiei denumirile și adresele organismelor de evaluare a conformității menționate la alineatul (1). Comisia pune informațiile respective la dispoziția tuturor statelor membre.	7. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.			Prevederi UE neaplicabile	Prevederea nu necesită transpunere în legislația Republicii Moldova, deoarece instituie o obligație procedurală specifică statelor membre ale Uniunii Europene de a comunica informații Comisiei Europene, mecanism care funcționează exclusiv în cadrul instituțional al Uniunii Europene și nu este aplicabil statelor terțe.	
(8) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47 prin care se stabilesc criteriile specifice care urmează să fie îndeplinite de organismele de evaluare a conformității desemnate menționate la alineatul (1) de la prezentul articol.	8. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.			Prevederi UE neaplicabile	Prevederea nu necesită transpunere în legislația Republicii Moldova, deoarece stabilește o competență normativă a Comisia Europeană de a adopta acte delegate în cadrul dreptului Uniunii Europene	
Articolul 5d **Publicarea unei liste a portofelelor europene**	**Article 5d** **Publication of a list of certified European**	**Articolul 8.** **Publicarea unei liste a portofelelor pentru**				

pentru identitatea digitală certificate	Digital Identity Wallets	identitatea digitală certificate				
(1) Statele membre informează, fără întârzieri nejustificate, Comisia și grupul de cooperare constituit în temeiul articolului 46e alineatul (1) cu privire la portofelele europene pentru identitatea digitală care au fost furnizate în temeiul articolului 5a și au fost certificate de organismele de evaluare a conformității menționate la articolul 5c alineatul (1). Statele membre informează, fără întârzieri nejustificate, Comisia și grupul de cooperare constituit în temeiul articolului 46e alineatul (1) în cazul în care o certificare este anulată și indică motivele anulării.	1. Member States shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c(1). They shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1), without undue delay if a certification is cancelled and shall state the reasons for the cancellation.	(1) Organismul de supraveghere asigură menținerea și publicarea listei portofelelor pentru identitatea digitală furnizate și certificate în conformitate cu prezenta lege.		Compatibil		
(2) Fără a aduce atingere articolului 5a alineatul (18), informațiile menționate la alineatul (1) de la prezentul articol, furnizate de statele membre, includ cel puțin: (a) certificatul și raportul de evaluare a certificării portofelului european pentru identitatea digitală certificat; (b) o descriere a sistemului de identificare electronică în cadrul căruia este furnizat portofelul european pentru identitatea digitală; (c) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la partea care furnizează portofelul	2. Without prejudice to Article 5a(18), the information provided by Member States referred to in paragraph 1 of this Article shall include at least: (a) the certificate and certification assessment report of the certified European Digital Identity Wallet; (b) a description of the electronic identification scheme under which the European Digital Identity Wallet is provided; (c) the applicable supervisory regime and	(2) Lista portofelelor pentru identitatea digitală se menține într-o formă care poate fi citită automat și include cel puțin: a) certificatul și raportul de evaluare a certificării portofelului pentru identitatea digitală certificat; b) o descriere a sistemului de identificare electronică în cadrul căruia este furnizat portofelul pentru identitatea digitală; c) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la partea care furnizează portofelul pentru identitatea digitală;		Compatibil		

european pentru identitatea digitală; (d) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică; (e) dispozițiile pentru suspendarea sau revocarea sistemului de identificare electronică, a autentificării sau a părților compromise în cauză.	information on the liability regime with respect to the party providing the European Digital Identity Wallet; (d) the authority or authorities responsible for the electronic identification scheme; (e) arrangements for suspension or revocation of the electronic identification scheme or authentication or of the compromised parts concerned.	d) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică; e) dispozițiile pentru suspendarea sau revocarea sistemului de identificare electronică, a autentificării sau a părților compromise în cauză.				
(3) Pe baza informațiilor primite în temeiul alineatului (1), Comisia stabilește, publică în Jurnalul Oficial al Uniunii Europene și menține într-o formă care poate fi citită automat o listă a portofelelor europene pentru identitatea digitală certificate.	3. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the Official Journal of the European Union and maintain in a machine-readable form a list of certified European Digital Identity Wallets.	(1) Organismul de supraveghere asigură menținerea și publicarea listei portofelelor pentru identitatea digitală furnizate și certificate în conformitate cu prezenta lege.		Compatibil		
(4) Un stat membru poate transmite Comisiei o cerere de eliminare de pe lista menționată la alineatul (3) a unui portofel european pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia este furnizat acesta.	4. A Member State may submit a request to the Commission to remove a European Digital Identity Wallet and the electronic identification scheme under which it is provided from the list referred to in paragraph 3.	(3) Orice parte interesată poate transmite organismului o cerere de eliminare de pe lista menționată la alin. (1) a unui portofel pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia este furnizat acesta.		Compatibil		
(5) În cazul în care informațiile transmise în temeiul alineatului (1) se modifică, statul membru furnizează Comisiei informațiile actualizate.	5. Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission	(4) În cazul în care informațiile înregistrare în lista menționată la alin. (1) se modifică, furnizorii portofelelor pentru identitatea digitală furnizează		Compatibil		

	with updated information.	organismului de supraveghere informațiile actualizate.				
(6) Comisia actualizează lista menționată la alineatul (3) prin publicarea în Jurnalul Oficial al Uniunii Europene a modificărilor corespunzătoare aduse listei în termen de o lună de la primirea unei cereri în temeiul alineatului (4) sau a informațiilor actualizate în temeiul alineatului (5).	6. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the Official Journal of the European Union the corresponding amendments to the list within one month of receipt of a request pursuant to paragraph 4 or of updated information pursuant to paragraph 5.	(5) Organismul de supraveghere asigură actualizarea listei portofelelor pentru identitatea digitală certificate în termen de o lună de la primirea unei cereri în temeiul alin. (3) sau a informațiilor actualizate în temeiul alin. (4).		Compatibil		
(7) Până la 21 noiembrie 2024, Comisia stabilește formatele și procedurile aplicabile în vederea îndeplinirii cerințelor prevăzute la alineatele (1), (4) și (5) de la prezentul articol prin intermediul unor acte de punere în aplicare cu privire la implementarea portofelelor europene pentru identitatea digitală, astfel cum se menționează la articolul 5a alineatul (23). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	7. By 21 November 2024, the Commission shall establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 5e Încălcarea securității portofelelor europene pentru identitatea digitală	**Article 5e Security breach of European Digital Identity Wallets**	**Articolul 9. Încălcarea securității portofelelor pentru identitatea digitală**				
(1) În cazul în care portofelele europene pentru identitatea digitală furnizate în temeiul articolului 5a,	1. Where European Digital Identity Wallets provided pursuant to Article 5a, the validation	(1) În cazul în care portofelele pentru identitatea digitală furnizate în temeiul art. 5, mecanismele de validare		Compatibil		

mecanismele de validare menționate la articolul 5a alineatul (8) sau sistemul de identificare electronică în cadrul căruia sunt furnizate portofelele europene pentru identitatea digitală fac obiectul unei încălcări a securității sau sunt compromise parțial într-un mod care afectează fiabilitatea lor sau a altor portofele europene pentru identitatea digitală, statele membre care au furnizat portofelele europene pentru identitatea digitală suspendă fără întârziere nejustificată furnizarea și utilizarea portofelelor europene pentru identitatea digitală. În cazul în care acest lucru este justificat de gravitatea încălcării securității sau a compromiterii menționate la primul paragraf, statul membru retrage fără întârzieri nejustificate portofelele europene pentru identitatea digitală. Statul membru informează în mod corespunzător utilizatorii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1), beneficiarii și Comisia.	mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets. Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.	menționate la art. 5 alin. (8) sau sistemul de identificare electronică în cadrul căruia sunt furnizate portofelele pentru identitatea digitală fac obiectul unei încălcări a securității sau sunt compromise parțial într-un mod care afectează fiabilitatea lor sau a altor portofele pentru identitatea digitală, furnizorii portofelelor pentru identitatea digitală suspendă fără întârziere nejustificată furnizarea și utilizarea portofelelor pentru identitatea digitală. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați, precum și organismul de supraveghere.				
(2) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) primul paragraf de la prezentul articol nu este remediată în	2. If the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is not remedied within three months of	(2) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) nu este remediată în termen de trei luni de la suspendare, furnizorii		Compatibil		

termen de trei luni de la suspendare, statul membru care a furnizat portofelele europene pentru identitatea digitală retrage portofelele europene pentru identitatea digitală și le revocă valabilitatea. Statul membru informează în mod corespunzător utilizatorii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1), beneficiarii și Comisia cu privire la retragere.	the suspension, the Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission of the withdrawal accordingly.	portofelelor pentru identitatea digitală retrag portofelele pentru identitatea digitală și le revocă valabilitatea. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați, precum și organismul de supraveghere cu privire la retragere.				
(3) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) primul paragraf de la prezentul articol este remediată, statul membru furnizor reia furnizarea și utilizarea portofelelor europene pentru identitatea digitală și informează fără întârzieri nejustificate utilizatorii și beneficiarii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) și Comisia.	3. Where the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is remedied, the providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c(1) and the Commission without undue delay.	(3) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) este remediată, furnizorii portofelelor pentru identitatea digitală reiau furnizarea și utilizarea portofelelor pentru identitatea digitală și informează fără întârzieri nejustificate utilizatorii și beneficiarii afectați, precum și organismul de supraveghere.		Compatibil		
(4) Comisia publică în Jurnalul Oficial al Uniunii Europene, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 5d.	4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 5d without undue delay.	(4) Organismul de supraveghere, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la art. 8.				
(5) Până la 21 noiembrie 2024, Comisia stabilește,	5. By 21 November 2024, the Commission	Articolul 69. Dispoziții finale		Compatibil		

prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru măsurile menționate la alineatele (1), (2) și (3) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
Articolul 5f Utilizarea transfrontalieră a portofelelor europene pentru identitatea digitală	**Article 5f Cross-border reliance on European Digital Identity Wallets**	**Articolul 10. Utilizarea transfrontalieră a portofelelor pentru identitatea digitală**				
(1) În cazul în care statele membre solicită identificarea și autentificarea electronică pentru a accesa un serviciu online furnizat de un organism din sectorul public, acestea acceptă și portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament.	1. Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.	(1) În cazul în care autoritățile sau instituțiile publice solicită identificarea sau autentificarea electronică pentru accesul la servicii publice online, acestea acceptă și utilizarea portofelelor pentru identitatea digitală furnizate în statele membre ale Uniunea Europeană, în măsura în care acestea sunt emise în conformitate cu cerințele stabilite prin legislația Uniunii Europene și pot fi verificate prin mecanisme tehnice interoperabile.		Compatibil		
2) În cazul în care beneficiarii privați care furnizează servicii, cu excepția microîntreprinderilor și a întreprinderilor mici, astfel cum sunt definite la articolul 2 din anexa la	2. Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to	(2) Furnizorii de servicii din sectorul privat care, în temeiul legislației sau al obligațiilor contractuale, solicită identificarea sau autentificarea electronică a utilizatorilor pot accepta utilizarea portofelelor pentru		Compatibil		

Recomandarea 2003/361/CE a Comisiei (5), au obligația în temeiul dreptului Uniunii sau al dreptului intern să utilizeze autentificarea strictă a utilizatorului pentru identificarea online sau în cazul în care autentificarea strictă a utilizatorului pentru identificarea online este obligatorie în temeiul unei obligații contractuale, inclusiv în domeniile transporturilor, energiei, serviciilor bancare și financiare, securității sociale, sănătății, apei potabile, serviciilor poștale, infrastructurii digitale, educației sau telecomunicațiilor, respectivii beneficiari privați, în termen de 36 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la articolul 5a alineatul (23) și la articolul 5c alineatul (6) și, numai la cererea voluntară a utilizatorului, acceptă și utilizarea portofelelor europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament.	Commission Recommendation 2003/361/EC (5), are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.	identitatea digitală, inclusiv a celor furnizate în statele membre ale Uniunea Europeană, la solicitarea utilizatorului și în limitele datelor necesare pentru prestarea serviciului.				
(3) În cazul în care furnizorii de platforme online foarte mari menționate la articolul 33 din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului (6) impun autentificarea utilizatorului pentru accesul	3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council (6) require user	(2) Furnizorii de servicii din sectorul privat care, în temeiul legislației sau al obligațiilor contractuale, solicită identificarea sau autentificarea electronică a utilizatorilor acceptă utilizarea portofelelor pentru identitatea digitală, inclusiv a celor		Compatibil		

la servicii online, aceștia acceptă și facilitează și utilizarea portofelelor europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament pentru autentificarea utilizatorului, numai la cererea voluntară a acestuia și în ceea ce privește datele minime necesare pentru serviciul online specific pentru care se solicită autentificarea.	authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.	furnizate în statele membre ale Uniunea Europeană, la solicitarea utilizatorului și în limitele datelor necesare pentru prestarea serviciului.				
4) În cooperare cu statele membre, Comisia facilitează elaborarea unor coduri de conduită în strânsă colaborare cu toate părțile interesate relevante, inclusiv cu societatea civilă, pentru a contribui la disponibilitatea și utilizarea pe scară largă a portofelelor europene pentru identitatea digitală care se încadrează în domeniul de aplicare al prezentului regulament și pentru a încuraja prestatorii de servicii să finalizeze elaborarea codurilor de conduită.	4. In cooperation with Member States, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to the wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct.			Prevederi UE neaplicabile	Prevederea nu necesită transpunere în legislația Republicii Moldova, deoarece stabilește un mecanism de cooperare și facilitare coordonat de Comisia Europeană împreună cu statele membre ale Uniunii Europene, însă Republica Moldova ar putea participa la astfel de inițiative sau procese de elaborare a codurilor de conduită în cazul în care este invitată în cadrul cooperării cu Uniunea Europeană.	
(5) În termen de 24 de luni de la implementarea portofelelor europene pentru identitatea digitală, Comisia evaluează cererea, disponibilitatea și posibilitatea de utilizare a portofelelor europene pentru	5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall assess the demand for, and the availability and usability of, European Digital	(4) Organismul de supraveghere efectuează, la fiecare 24 de luni de la implementarea portofelelor pentru identitatea digitală, o evaluare a cererii, disponibilității și posibilității de utilizare a acestora, ținând		Compatibil		

identitatea digitală, ținând seama de criterii precum adoptarea de către utilizatori, prezența transfrontalieră a prestatorilor de servicii, evoluțiile tehnologice, evoluția modelelor de utilizare și cererea consumatorilor.	Identity Wallets, taking into account criteria such as user take-up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.	seama de criterii precum gradul de adoptare de către utilizatori, disponibilitatea serviciilor, evoluțiile tehnologice, evoluția modelelor de utilizare și cererea utilizatorilor, iar rezultatele evaluării sunt publicate de către organismul de supraveghere pe pagina sa oficială.				
SECȚIUNEA 2 **Sisteme de identificare electronică**	**SECTION 2** **Electronic identification schemes**	**Secțiunea a 2-a** **Sisteme de identificare electronică**				
Articolul 6 **Recunoașterea reciprocă**	**Article 6** **Mutual recognition**	**Articolul 11.** **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	1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met: (a) the electronic identification means is issued under an electronic identification	(1) Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică și o autentificare conform cadrului normativ al Republicii Moldova pentru a accesa un serviciu prestat online de un organism din sectorul public, mijloacele de identificare electronică emise într-un stat membru al Uniunii Europene sunt recunoscute în Republica Moldova 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 de sisteme de identificare electronică publicată de Comisia Europeană;		Compatibil		

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 identificare electronică respective să corespundă nivelului de asigurare substanțial sau ridicat; (c) organismul din sectorul public relevant utilizează nivelul de asigurare „substanțial” sau „ridicat” în legătură cu accesarea online a serviciului respectiv. 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).	scheme that is included in the list published by the Commission pursuant to Article 9; (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high; (c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online. Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.	(b) nivelul de asigurare al respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare substanțial sau ridicat, conform clasificării prevăzute de lege; (c) organismele din sectorul public care furnizează serviciul online să fie capabile să verifice validitatea și integritatea mijloacelor de identificare electronică emise într-un stat membru al Uniunii Europene.				
(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	2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public	(2) Organismul de supraveghere este responsabil pentru publicarea ghidurilor și procedurilor privind recunoașterea mijloacelor de identificare electronică transfrontaliere și pentru actualizarea acestora ori de câte ori apar modificări în lista sistemelor recunoscute sau în cerințele de securitate.		Compatibil		

public în scopul autentificării transfrontaliere pentru serviciul furnizat online de către organismele respective.	sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.	(3) Orice serviciu public online care acceptă autentificarea transfrontalieră trebuie să asigure transparența criteriilor și să informeze utilizatorii despre condițiile de recunoaștere și nivelul de asigurare necesar al mijloacelor de identificare electronice.				
Articolul 7 **Eligibilitatea pentru notificarea sistemelor de identificare electronică**	**Article 7** **Eligibility for notification of electronic identification schemes**					
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: (a) mijloacele de identificare electronică din cadrul sistemului sunt emise de statul membru care notifică, pe baza unui mandat din partea statului membru care notifică, sau independent de statul membru care notifică și sunt recunoscute de respectivul stat membru; (b) mijloacele de identificare electronică pot fi utilizate pentru a accesa cel puțin un serviciu prestat de un organism din sectorul public care necesită identificarea electronică în statul membru care notifică; (c) sistemul de identificare electronică și mijloacele emise în temeiul acestuia îndeplinesc cerințele aferente cel puțin unuia	An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) if the following conditions are met: (a) the electronic identification means under the scheme are issued by the notifying Member State, under a mandate from the notifying Member State, or independently of the notifying Member State and recognised by that Member State; (b) the electronic identification means under the scheme can be used to access at least one service provided by a public sector body which requires electronic identification in the notifying Member State;			Prevederi UE neaplicabile	Normele nu sunt aplicabile în context național, întrucât se referă la proceduri de notificare și recunoaștere a sistemelor de identificare electronică între state membre ale Uniunii Europene.	

dintre nivelurile de asigurare prevăzute în actul de punere în aplicare menționat la articolul 8 alineatul (3); (d) statul membru care notifică se asigură că datele de identificare personală, reprezentând în mod unic persoana în cauză, sunt atribuite persoanei fizice sau juridice în conformitate cu specificațiile tehnice aferente nivelului de asigurare relevant; (e) partea care emite mijloacele de identificare electronică se asigură că mijloacele de identificare electronică sunt atribuite persoanelor menționate la litera (d); (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. Autentificarea transfrontalieră este furnizată gratuit atunci când este efectuată în legătură cu un serviciu online prestat de un organism din sectorul public. (g) cu cel puțin șase luni înaintea notificării efectuate în temeiul articolului 9 alineatul (1), statul membru care notifică furnizează celorlalte state membre o descriere a sistemului respectiv;	(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the levels of assurance set out in the implementing act referred to in Article 8(3); (d) the notifying Member State ensures that the person identification data, uniquely representing the person in question, are attributed to the natural or legal person in conformity with the technical specifications applicable to the relevant assurance level; (e) the party issuing the electronic identification means under the scheme ensures that the electronic identification means are attributed to the persons referred to in point (d) of this Article; (f) the notifying Member State ensures the availability of authentication online, so that any relying party established in another Member State can confirm the person identification data received in electronic form. Cross-border authentication shall be provided free of charge when carried out in					

(h) sistemul de identificare electronică îndeplinește cerințele prevăzute în actul de punere în aplicare menționat la articolul 12 alineatul (8).	relation to a service provided online by a public sector body. (g) at least six months before notification pursuant to Article 9(1), the notifying Member State shall provide the other Member States with a description of that scheme; (h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).					
Articolul 8 **Niveluri de asigurare ale mijloacelor de identificare electronică**	**Article 8** **Assurance levels of electronic identification means**	**Articolul 12.** **Niveluri de asigurare ale mijloacelor de identificare electronică**				
(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.	1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.	(1) Un sistem de identificare electronică poate prevedea nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv.		Compatibil		
(2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv: (a) nivelul de asigurare scăzut se referă la un mijloc de identificare electronică care asigură un grad limitat de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane, al cărui scop este	2. The assurance levels low, substantial and high shall meet respectively the following criteria: (a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited	(2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv: 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		Compatibil		

de a reduce riscul unei utilizări frauduloase sau al modificării frauduloase a identității; (b) nivelul de asigurare substanțial se referă la un mijloc de identificare electronică care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane, al cărui scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității; (c) nivelul de asigurare ridicat se referă la un mijloc de identificare electronică care asigură un grad mai ridicat de încredere decât mijloacele cu nivel de asigurare substanțial, al cărui scop este de a împiedica utilizarea frauduloasă sau modificarea frauduloasă a identității.	degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity; (b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity; (c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification	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; 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; 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				

	means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.	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 frauduloasă a identității.				
(3) Până la 18 septembrie 2015, ținând cont de standardele internaționale relevante și sub rezerva alineatului (2), Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice, standardele și procedurile minime, în raport cu care sunt determinate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică. Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente: (a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică; (b) procedura pentru emiterea mijloacelor de identificare electronică solicitate; (c) mecanismul de autentificare, prin care	3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means. Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements: (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means; (b) the procedure for the issuance of the	(3) Specificațiile tehnice, standardele și procedurile minime, în raport cu care sunt determinate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică se stabilesc de către Guvern. Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente: a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică; b) procedura pentru emiterea mijloacelor de identificare electronică solicitate; c) mecanismul de autentificare, prin care persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar;		Compatibil		

persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar; (d) entitatea care emite mijloacele de identificare electronică; (e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și (f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	requested electronic identification means; (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party; (d) the entity issuing the electronic identification means; (e) any other body involved in the application for the issuance of the electronic identification means; and (f) the technical and security specifications of the issued electronic identification means. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	d) entitatea care emite mijloacele de identificare electronică; e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise.				
Articolul 9 **Notificarea**	**Article 9** **Notification**	**Articolul 13.** **Lista sistemelor naționale de identificare electronică**				
(1) Statul membru care notifică înaintează Comisiei următoarele informații și, fără întârzieri nejustificate, orice modificări ulterioare ale acestora: (a) o descriere a sistemului de identificare electronică notificat, incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare	1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto: (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of	(1) Deținătorul unui sistem de identificare electronică este obligat să transmită organismului de supraveghere o notificare care să includă, fără întârzieri nejustificate, următoarele informații, precum și orice modificări ulterioare ale acestora: 1) o descriere a sistemului de identificare electronică notificat,		Compatibil		

electronică din cadrul sistemului; (b) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la: (i) partea care emite mijloacele de identificare electronică; și (ii) partea care desfășoară procedura de autentificare; (c) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică; (d) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală; (e) o descriere a modului în care sunt îndeplinite cerințele prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul (8); (f) o descriere a autentificării menționate la articolul 7 litera (f); (g) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză.	electronic identification means under the scheme; (b) the applicable supervisory regime and information on the liability regime with respect to the following: (i) the party issuing the electronic identification means; and (ii) the party operating the authentication procedure; (c) the authority or authorities responsible for the electronic identification scheme; (d) information on the entity or entities which manage the registration of the unique person identification data; (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met; (f) a description of the authentication referred to in point (f) of Article 7; (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.	incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului; 2) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la următoarele aspecte: a) partea care emite mijloacele de identificare electronică; și b) partea care desfășoară procedura de autentificare; 3) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică; 4) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală; 5) o descriere a modului în care sunt îndeplinite criteriile prevăzute la alin. (2) și specificațiile tehnice, standardele și procedurile pentru nivelurile de asigurare stabilite de Guvern; 6) o descriere a autentificării online; 7) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză.				
(2) Comisia publică în Jurnalul Oficial al Uniunii Europene, fără întârzieri nejustificate, lista sistemelor	2. The Commission shall, without undue delay, publish in the Official Journal of the	(2) Organismul de supraveghere publică pe pagina sa oficială o listă a sistemelor de identificare		Compatibil		

de identificare electronică ce au fost notificate în temeiul alineatului (1), împreună cu informațiile de bază cu privire la aceste sisteme.	European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 together with basic information about those schemes.	electronică ce au fost notificate în temeiul alin. (1), împreună cu informațiile de bază cu privire la aceste sisteme.				
(3) Comisia publică în Jurnalul Oficial al Uniunii Europene modificările la lista menționată la alineatul (2) în termen de o lună de la data primirii respectivei notificări.	3. The Commission shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within one month of the date of receipt of that notification.					
(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.	4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request.	(3) Deținătorul unui sistem de identificare electronică poate solicita organismului de supraveghere eliminarea sistemului său din lista prevăzută la alin. (2).		Compatibil		
(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	5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

menționată la articolul 48 alineatul (2).	examination procedure referred to in Article 48(2).					
Articolul 10 **Încălcarea securității sistemelor de identificare electronică**	**Article 10** **Security breach of electronic identification schemes**					
(1) În cazul în care fie sistemul de identificare electronică notificat, fie autentificarea 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.	1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.			Prevederi UE neaplicabile		
(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.	2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.			Prevederi UE neaplicabile		
(3) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) nu este	3. If the breach or compromise referred to in paragraph 1 is not remedied within three			Prevederi UE neaplicabile		

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).	months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.					
Articolul 11 **Răspunderea**	**Article 11** **Liability**	**Articolul 67.** **Răspunderea juridică în cadrul tranzacțiilor transfrontaliere**				
(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 literele (d) și (f).	1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.	(1) Organismul de supraveghere este răspunzător pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere, ca urmare a nerespectării obligațiilor care îi revin potrivit prezentei legi referitoare la asigurarea interoperabilității și securității sistemelor de identificare electronică notificate Comisiei Europene.		Compatibil		
(2) Partea care emite mijloacele de identificare electronică este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau	2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person	(2) Emitentul mijloacelor de identificare electronică este răspunzător pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei		Compatibil		

juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligației menționate la articolul 7 litera (e).	due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.	tranzacții transfrontaliere, ca urmare a nerespectării obligației de a asigura că mijloacele de identificare electronică emise corespund, la momentul emiterii și ulterior, datelor de identificare electronică ale persoanei căreia i-au fost atribuite.				
(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenșional 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).	3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.	(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din culpă oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere, pentru neasigurarea executării corecte a autentificării.		Compatibil		
(4) Alineatele (1), (2) și (3) se aplică în conformitate cu normele de drept intern privind răspunderea.	4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.			Prevederi UE neaplicabile		
(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).	5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.			Prevederi UE neaplicabile		
Articolul 11a Corelarea transfrontalieră a identităților	**Article 11a Cross-border identity matching**	**Articolul 14. Corelarea transfrontalieră a identităților**				
(1) Atunci când acționează în calitate de beneficiari ai	1. When acting as relying parties for cross-	(1) Atunci când organismele din sectorul public din		Compatibil		

unor servicii transfrontaliere, statele membre asigură corelarea fără echivoc a identităților pentru persoanele fizice care utilizează mijloace de identificare electronică notificate sau portofele europene pentru identitatea digitală.	border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.	Republica Moldova acționează în calitate de beneficiari ai unor servicii transfrontaliere, organismul de supraveghere se asigură că se realizează corelarea fără echivoc a identităților pentru persoanele fizice care utilizează mijloace de identificare electronică sau portofele pentru identitatea digitală.				
(2) Statele membre prevăd măsuri tehnice și organizatorice pentru a asigura un nivel ridicat de protecție a datelor cu caracter personal utilizate pentru corelarea identităților și pentru a preveni crearea de profiluri ale utilizatorilor.	2. Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users.	Guvernul stabilește măsuri tehnice și organizatorice pentru a asigura un nivel ridicat de protecție a datelor cu caracter personal utilizate pentru corelarea identităților și pentru a preveni crearea de profiluri ale utilizatorilor.		Compatibil		
(3) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	3. By 21 November 2024, the Commission shall establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 1 of this Article by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 12 **Interoperabilitate**	**Article 12** **Interoperability**	**Articolul 15.** **Interoperabilitate**				
(1) Sistemele naționale de identificare electronică notificate în temeiul	1. The national electronic identification schemes notified	(1) Sistemele naționale de identificare electronică publicate în temeiul art. 13 sunt interoperabile.		Compatibil		

articolului 9 alineatul (1) sunt interoperabile.	pursuant to Article 9(1) shall be interoperable.					
(2) În sensul alineatului (1), se stabilește un cadru de interoperabilitate.	2. For the purposes of paragraph 1, an interoperability framework shall be established.	(2) Guvernul va stabili cadrul de interoperabilitate care trebuie să îndeplinească următoarele criterii: a) urmărește să fie neutru din punctul de vedere al tehnologiei și nu acordă prioritate niciuneia dintre soluțiile tehnice specifice pentru identificarea electronică; b) respectă standardele europene și internaționale, atunci când este posibil; c) facilitează protecția, începând cu momentul conceperii, a vieții private și a securității;		Compatibil		
(3) Cadrul 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; (b) respectă standardele europene și internaționale, atunci când este posibil; (c) facilitează protecția, începând cu momentul conceperii, a vieții private și a securității („privacy and security by design”);	3. The interoperability framework shall meet the following criteria: (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State; (b) it follows European and international standards, where possible; (c) it facilitates the implementation of privacy and security by design.			Compatibil		
(4) Cadrul de interoperabilitate este alcătuit din: (a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la articolul 8; (b) o clasificare a nivelurilor naționale de asigurare; (c) o trimitere la cerințele tehnice minime referitoare la interoperabilitate; (d) un set minim de date de identificare personală; (e) regulamentul de procedură; (f) dispoziții referitoare la soluționarea litigiilor; (g)	4. The interoperability framework shall consist of: (a) a reference to minimum technical requirements related to the levels of assurance referred to in Article 8; (b) a mapping of national levels of assurance; (c) a reference to minimum technical requirements related to interoperability; (d) a minimum set of person identification data; (e) a procedure rulebook; (f)	(3) Cadru de interoperabilitate este alcătuit din următoarele elemente: a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la art. 12; b) o trimitere la cerințele tehnice minime referitoare la interoperabilitate; c) o trimitere la un set minim de date de identificare personală necesare pentru a reprezenta în mod unic o persoană fizică sau juridică sau o persoană fizică ce		Compatibil		

standarde de securitate operaționale comune.	arrangements for dispute resolution; (g) common operational security standards.	reprezintă o altă persoană fizică sau o persoană juridică, care sunt disponibile din sistemele de identificare electronică; d) regulamentul de procedură; e) dispoziții referitoare la soluționarea litigiilor; și f) standarde de securitate operaționale comune.				
(5) Statele membre efectuează evaluări inter pares ale sistemelor de identificare electronică care intră în domeniul de aplicare al prezentului regulament și care trebuie să fie notificate în conformitate cu articolul 9 alineatul (1) litera (a).	5. Member States shall carry out peer reviews of the electronic identification schemes that fall within the scope of this Regulation and that are to be notified pursuant to Article 9(1), point (a).			Prevederi UE neaplicabile		
(6) Până la 18 martie 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, modalitățile procedurale necesare pentru efectuarea evaluărilor inter pares menționate la alineatul (5) de la prezentul articol, în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	6. By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 of this Article with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
(8) Până la 18 septembrie 2025, în vederea stabilirii unor condiții uniforme	8. By 18 September 2025, for the purpose of setting uniform	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi:				

pentru punerea în aplicare a cerinței menționate la alineatul (1) de la prezentul articol, sub rezerva criteriilor stabilite la alineatul (3) de la prezentul articol 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) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	conditions for the implementation of the requirement under paragraph 1 of this Article, the Commission shall, subject to the criteria set out in paragraph 3 of this Article and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
(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).	9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).			Prevederi UE neaplicabile		
Articolul 12a Certificarea sistemelor de identificare electronică	**Article 12a Certification of electronic identification schemes**	**Articolul 16. Certificarea sistemelor de identificare electronică**				
(1) Conformitatea sistemelor de identificare electronică ce trebuie notificate cu cerințele privind securitatea cibernetică prevăzute în prezentul regulament, inclusiv conformitatea cu cerințele relevante în	1. The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements	(1) Conformitatea sistemelor de identificare electronică cu cerințele privind securitatea cibernetică prevăzute în prezenta lege, inclusiv conformitatea cu cerințele relevante în materie de securitate cibernetică prevăzute la art. 12 alin. (2) în		Compatibil		

materie de securitate cibernetică prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică, este certificată de organismele de evaluare a conformității desemnate de statele membre.	set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.	ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică, este certificată de organismele de evaluare a conformității desemnate de statele membre.				
(2) Certificarea efectuată în temeiul alineatului (1) de la prezentul articol se efectuează în cadrul unui sistem de certificare a securității cibernetice relevant în conformitate cu Regulamentul (UE) 2019/881 sau al unor părți ale acestuia, în măsura în care certificatul de securitate cibernetică sau unele părți ale acestuia acoperă respectivele cerințe privind securitatea cibernetică.	2. Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.			Compatibil		
(3) Certificarea efectuată în temeiul alineatului (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția să se efectueze o evaluare a vulnerabilității o dată la doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în termen de trei luni de la identificarea sa, certificarea este anulată.	3. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied within three months of such identification, certification shall be cancelled.	(2) Certificarea efectuată în temeiul alin. (1) este valabilă pentru o perioadă de cinci ani, cu condiția să se efectueze o evaluare a vulnerabilității o dată la doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în termen de trei luni de la identificarea sa, certificarea este anulată.		Compatibil		
(4) În pofida alineatului (2), statele membre pot, în conformitate cu alineatul respectiv, să solicite de la un stat membru care notifică	4. Notwithstanding paragraph 2, Member States may request, in accordance with that paragraph, additional			Prevederi UE neaplicabile		

informații suplimentare cu privire la sistemele de identificare electronică sau la părți certificate ale acestora.	information from a notifying Member State about electronic identification schemes or part thereof certified.					
(5) Evaluarea inter pares privind sistemele de identificare electronică menționată la articolul 12 alineatul (5) nu se aplică sistemelor de identificare electronică sau unor părți ale acestor sisteme certificate în conformitate cu alineatul (1) de la prezentul articol. Statele membre pot utiliza un certificat sau o declarație de conformitate, emis(ă) în conformitate cu un sistem de certificare relevant sau cu părți ale unor astfel de sisteme, cu cerințele care nu țin de securitatea cibernetică prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelul de asigurare ale sistemelor de identificare electronică.	5. The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.			Prevederi UE neaplicabile		
(6) Statele membre transmit Comisiei denumirile și adresele organismelor de evaluare a conformității menționate la alineatul (1). Comisia pune informațiile respective la dispoziția tuturor statelor membre.	6. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.			Prevederi UE neaplicabile		
Articolul 12b **Accesul la componentele de hardware și de software**	**Article 12b** **Access to hardware and software features**	**Articolul 5. Portofelele pentru identitatea digitală**				

Atunci când furnizorii de portofele europene pentru identitatea digitală și emitenții de mijloace de identificare electronică notificate, care acționează cu titlu comercial sau profesional și utilizează servicii de platformă esențiale în sensul definiției de la articolul 2 punctul 2 din Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului (7) în scopul sau în cursul furnizării de servicii specifice portofelelor europene pentru identitatea digitală și de mijloace de identificare electronică utilizatorilor finali, sunt utilizatori comerciali în sensul definiției de la articolul 2 punctul 21 din regulamentul menționat, controlorii de acces le permit, în special, să beneficieze în mod efectiv de interoperabilitatea cu aceleași componente ale sistemului de operare, ale hardware-ului sau ale software-ului, precum și să aibă acces la respectivele componente în vederea asigurării interoperabilității. Interoperabilitatea efectivă și accesul menționate anterior sunt permise cu titlu gratuit și indiferent dacă componentele de hardware sau de software fac parte din sistemul de operare, în aceleași condiții în care respectivele componente îi	Where providers of European Digital Identity Wallets and issuers of notified electronic identification means that act in a commercial or professional capacity and use core platform services as defined in Article 2, point (2), of Regulation (EU) 2022/1925 of the European Parliament and of the Council (7) for the purpose or in the course of providing European Digital Identity Wallet services and electronic identification means to end-users are business users as defined in Article 2, point (21), of that Regulation, gatekeepers shall in particular allow them effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access shall be allowed free of charge and regardless of whether the hardware or software features are part of the operating system, are available to, or are used by, that gatekeeper when providing such services,	(22) Atunci când furnizorii de portofele pentru identitatea digitală și emitenții de mijloace de identificare electronică acționează cu titlu comercial sau profesional și utilizează servicii de platformă esențiale în scopul sau în cursul furnizării de servicii specifice portofelelor pentru identitatea digitală și de mijloace de identificare electronică utilizatorilor finali, sunt utilizatori comerciali, controlorii de acces le permit, în special, să beneficieze în mod efectiv de interoperabilitatea cu aceleași componente ale sistemului de operare, ale hardware-ului sau ale software-ului, precum și să aibă acces la respectivele componente în vederea asigurării interoperabilității. Interoperabilitatea efectivă și accesul menționate anterior sunt permise cu titlu gratuit și indiferent dacă componentele de hardware sau de software fac parte din sistemul de operare, în aceleași condiții în care respectivele componente îi sunt disponibile respectivului controlor de acces sau sunt folosite de acesta atunci când furnizează astfel de servicii.		Compatibil		

sunt disponibile respectivului controlor de acces sau sunt folosite de acesta atunci când furnizează astfel de servicii, în sensul articolului 6 alineatul (7) din Regulamentul (UE) 2022/1925. Prezentul articol nu aduce atingere articolului 5a alineatul (14) din prezentul regulament.	within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This Article is without prejudice to Article 5a(14) of this Regulation.					
CAPITOLUL III **SERVICII DE ÎNCREDERE**	**CHAPTER III** **TRUST SERVICES**	**Capitolul III** **SERVICII DE ÎNCREDERE**				
SECȚIUNEA 1 **Dispoziții generale**	**SECTION 1** **General provisions**	**SECȚIUNEA 1** **Dispoziții generale**				
Articolul 13 **Răspunderea și sarcina probei**	**Article 13** **Liability and burden of proof**	**Articolul 17.** **Răspunderea și sarcina probei**				
(1) Prestatorii de servicii de încredere sunt răspunzători pentru prejudiciile cauzate în mod intenșional 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. Intenția sau neglijența din partea unui prestator de servicii de încredere calificat este prezumată, cu excepția cazului în care respectivul	1. Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Regulation by a trust service provider shall have the right to seek compensation in	(1) 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 prezenta lege. Orice persoană fizică sau juridică ce a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezenta lege de către un prestator de servicii de încredere are dreptul de a solicita despăgubiri în conformitate cu cadrul normativ aplicabil. (2) Sarcina de a proba intenția sau neglijența unui prestator de servicii de		Compatibil		

prestator de servicii de încredere calificat dovedește că prejudiciul nu a intervenit din intenția sau din neglijența sa.	accordance with Union and national law. The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph. The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.	încredere necalificat revine persoanei fizice sau juridice care introduce o acțiune în despăgubiri pentru prejudiciul menționat la alin. (1).				
(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.	2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable by third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.	(4) 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.		Compatibil		
(3) Alineatele (1) și (2) se aplică în conformitate cu normele de drept intern privind răspunderea.	3. Paragraphs 1 and 2 shall apply in accordance with national rules on liability.			Compatibil		

Articolul 14 **Aspecte internaționale**	**Article 14** **International aspects**	**Articolul 18.** **Aspecte internaționale**				
(1) Serviciile de încredere prestate de prestatori de servicii de încredere stabiliți într-o țară terță sau de o organizație internațională sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune dacă serviciile de încredere care provin din țara terță sau de la organizația internațională sunt recunoscute prin intermediul unor acte de punere în aplicare sau al unui acord încheiat între Uniune și țara terță sau organizația internațională în cauză în conformitate cu articolul 218 din TFUE. Actele de punere în aplicare menționate la primul paragraf se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country or international organisation are recognised under an implementing act or an agreement concluded between the Union and the third country or international organisation concerned in accordance with Article 218 TFEU. The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(1) Serviciile de încredere prestate de prestatori de servicii de încredere cu sediul în orice stat membru al Uniunii Europene sau orice altă țară cu care Republica Moldova a încheiat un acord de recunoaștere reciprocă sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile electronice de încredere calificate prestate de prestatori de servicii de încredere calificați cu sediul în Republica Moldova.		Compatibil		
(2) Actele de punere în aplicare și acordul menționate la alineatul (1) garantează că cerințele aplicabile prestatorilor de servicii de încredere calificați stabiliți în Uniune și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de	2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by	(2) Acordurile menționate la alin. (1) garantează că cerințele aplicabile prestatorilor de servicii de încredere calificați cu sediul în Republica Moldova și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de		Compatibil		

prestatorii de servicii de încredere din țara terță în cauză sau de organizațiile internaționale, precum și de serviciile de încredere pe care aceștia le prestează. În special, țările terțe și organizațiile internaționale elaborează, mențin și publică o listă sigură a prestatorilor de servicii de încredere recunoscuți.	the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.	servicii de încredere din țara terță în cauză și de serviciile de încredere pe care le prestează.				
(3) Acordurile menționate la alineatul (1) garantează că 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.	3. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.	(3) Acordurile menționate la alin. (1) garantează că serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați cu sediul în Republica Moldova sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță cu care a fost încheiat acordul.		Compatibil		
Articolul 15 Accesibilitatea pentru persoanele cu dizabilități și cu nevoi speciale	**Article 15 Accessibility for persons with disabilities and special needs**	**Articolul 19. Accesibilitatea pentru persoanele cu dizabilități și cu nevoi speciale**				
Mijloacele de identificare electronică, prestarea serviciilor de încredere și furnizarea produselor destinate utilizatorului final care sunt utilizate pentru prestarea serviciilor respective sunt furnizate într-un limbaj clar și inteligibil și în conformitate	The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations	Mijloacele de identificare electronică, prestarea serviciilor de încredere și furnizarea produselor destinate utilizatorului final care sunt utilizate pentru prestarea serviciilor respective sunt furnizate într-un limbaj clar și inteligibil și în conformitate cu Convenția		Compatibil		

cu Convenția Națiunilor Unite privind drepturile persoanelor cu handicap și cu cerințele de accesibilitate prevăzute în Directiva (UE) 2019/882, fiind astfel accesibile și persoanelor care se confruntă cu limitări funcționale, cum ar fi persoanele în vârstă, și persoanelor cu acces limitat la tehnologiile digitale.	Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.	Națiunilor Unite privind drepturile persoanelor cu handicap, fiind astfel accesibile și persoanelor care se confruntă cu limitări funcționale, cum ar fi persoanele în vârstă, și persoanelor cu acces limitat la tehnologiile digitale.				
Articolul 16 **Sancțiuni**	**Article 16** **Penalties**	**Articolul 68.** **Sancțiuni**				
(1) Statele membre stabilesc normele referitoare la sancțiunile aplicabile în cazul încălcării prezentului regulament. Sancțiunile respective trebuie să fie eficace, proporționale și cu efect de descurajare.	(1) Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.	(1) Încălcarea prevederilor prezentei legi de către prestatorii de servicii de încredere, calificați sau necalificați, atrage răspunderea acestora și aplicarea amenzilor, de către organismul de supraveghere competent.		Compatibil		
(2) Statele membre se asigură că încălcările prezentului regulament de către prestatorii de servicii de încredere calificați și necalificați fac obiectul unor amenzi administrative în valoare de cel puțin: (a) 5 000 000 EUR, în cazul în care prestatorul de servicii de încredere este o persoană fizică; sau (b) în cazul în care prestatorul de servicii de încredere este o persoană juridică, 5 000 000 EUR sau 1 % din cifra de afaceri anuală totală la nivel mondial a întreprinderii	(2) Member States shall ensure that infringements of this Regulation are subject to administrative fines of at least: (a) EUR 5 000 000, where the trust service provider is a natural person; or (b) where the trust service provider is a legal person, EUR 5 000 000 or 1% of the total annual worldwide turnover of the undertaking to which the trust service provider belonged in the	(2) Încălcările prevederilor prezentei legi de către prestatorii de servicii de încredere calificați și necalificați fac obiectul aplicării unor amenzi în următoarele limite: a) echivalentul în lei al sumei de 5 000 000 EUR, în cazul în care prestatorul de servicii de încredere este o persoană fizică; sau b) în cazul persoanelor juridice, echivalentul în lei al sumei de 5 000 000 EUR sau până la 1% din cifra de afaceri anuală totală la nivel mondial a întreprinderii din		Compatibil		

căreia i-a aparținut prestatorul de servicii de încredere în exercițiul financiar anterior anului în care a avut loc încălcarea, luându-se în considerare valoarea cea mai mare.	preceding financial year, whichever is greater.	care face parte prestatorul de servicii de încredere, realizată în exercițiul financiar anterior anului în care a fost constatată încălcarea, luându-se în considerare valoarea cea mai mare.				
(3) În funcție de sistemul juridic al statelor membre, normele privind amenzile administrative pot fi aplicate astfel încât amenda să fie inițiată de organismul de supraveghere competent și aplicată de instanțele naționale competente. Aplicarea acestor norme în statele membre respective garantează faptul că respectivele măsuri juridice sunt eficiente și au un efect echivalent cu cel al amenzilor administrative aplicate direct de autoritățile de supraveghere.	3. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory body and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.	(3) Constatarea încălcărilor și aplicarea sancțiunilor se realizează de către organismul de supraveghere, în conformitate cu prezenta lege. (4) Deciziile organismului de supraveghere pot fi contestate în instanța de judecată competentă, în condițiile legii.		Compatibil		
SECȚIUNEA 2 Servicii de încredere necalificate	**SECTION 2 Non-qualified trust services**	**Secțiunea a 2-a Servicii de încredere necalificate**				
Articolul 19a Cerințe pentru prestatorii de servicii de încredere necalificați	**Article 19a Requirements for non-qualified trust service providers**	**Articolul 20. Cerințe pentru prestatorii de servicii de încredere necalificați**				
(1) Un prestator de servicii de încredere necalificat care prestează servicii de încredere necalificate: (a) dispune de politici adecvate și ia măsurile corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau	1. A non-qualified trust service provider providing non-qualified trust services shall: (a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or	Un prestator de servicii de încredere necalificat care prestează servicii de încredere necalificate: 1) dispune de politici adecvate și ia măsurile corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau		Compatibil		

indirecte legate de prestarea serviciului de încredere necalificat, care, în pofida articolului 21 din Directiva (UE) 2022/2555, includ cel puțin măsuri referitoare la: (i) procedurile de înregistrare și de integrare legate de un serviciu de încredere; (ii) controalele procedurale sau administrative necesare pentru prestarea de servicii de încredere; (iii) gestionarea și implementarea serviciilor de încredere; (b) notificarea organismului de supraveghere, persoanelor afectate care pot fi identificate, publicului – dacă chestiunea este de interes public –, și, după caz, altor autorități competente relevante, cu privire la orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (a) punctul (i), (ii) sau (iii) care are impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore din momentul în care a luat cunoștință de orice încălcare a securității sau perturbare.	indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of Directive (EU) 2022/2555, include at least measures relating to: (i) registration and onboarding procedures for a trust service; (ii) procedural or administrative checks needed to provide trust services; (iii) the management and implementation of trust services; (b) notifying the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (a) (i), (ii) or (iii), that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.	indirecte legate de prestarea serviciului de încredere necalificat, care, includ cel puțin măsuri referitoare la: a) procedurile de înregistrare și de integrare legate de un serviciu de încredere; b) controalele procedurale sau administrative necesare pentru prestarea de servicii de încredere; c) gestionarea și implementarea serviciilor de încredere; 2) notificarea organismului de supraveghere, persoanelor afectate care pot fi identificate, publicului – dacă chestiunea este de interes public –, și, după caz, altor autorități competente relevante, cu privire la orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la alin. 1) care are impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore din momentul în care a luat cunoștință de orice încălcare a securității sau perturbare.				

(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri în scopul alineatului (1) litera (a) de la prezentul articol. În cazul în care standardele, specificațiile și procedurile respective sunt respectate, se prezumă că sunt respectate 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).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 1, point (a), of this Article. Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
SECȚIUNEA 3 **Servicii de încredere calificate**	**SECTION 3** **Qualified trust services**	**Secțiunea a 3-a** **Servicii de încredere calificate**				
Articolul 20 **Supravegherea prestatorilor de servicii de încredere calificați**	**Article 20** **Supervision of qualified trust service providers**	**Articolul 21.** **Supravegherea prestatorilor de servicii de încredere calificați**				
(1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin la fiecare 24 de luni, de către un organism de evaluare a conformității. Auditul confirmă că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament.	1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in	(1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin la fiecare 24 de luni, de către un organism de evaluare a conformității. Auditul confirmă că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezenta lege și la art. 11 din Legea nr. 48/2023		Compatibil		

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.	Article 21 of Directive (EU) 2022/2555. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.	privind securitatea cibernetică. 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.				
(1a) Prestatorii de servicii de încredere calificați informează organismul de supraveghere cu cel puțin o lună înainte de un audit planificat și, la cerere, îi permit organismului de supraveghere să participe în calitate de observator.	1a. Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request.	(2) Prestatorii de servicii de încredere calificați informează organismul de supraveghere cu cel puțin o lună înainte de un audit planificat și, la cerere, îi permit organismului de supraveghere să participe în calitate de observator.		Compatibil		
(1b) Statele membre notifică Comisiei, fără întârzieri nejustificate, denumirile, adresele și detaliile de acreditare ale organismelor de evaluare a conformității menționate la alineatul (1), precum și orice modificări ulterioare ale acestora. Comisia pune informațiile respective la dispoziția tuturor statelor membre.	1b. Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.			Prevederi UE neaplicabile		
(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	2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to	(3) Fără a aduce atingere alin. (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		Compatibil		

servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere 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, fără întârzieri nejustificate, autoritățile de supraveghere competente înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679.	confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.	servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezenta lege. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează, fără întârzieri nejustificate, autoritatea națională pentru protecția datelor cu caracter personal.				
(3) În cazul în care prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în prezentul regulament, organismul de supraveghere îi solicită să remedieze situația într-un termen stabilit, dacă este cazul. În cazul în care prestatorul respectiv nu remediază situația, dacă este cazul în termenul stabilit de organismul de supraveghere, acesta din urmă, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.	3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable. Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.	(4) În cazul în care prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în prezenta lege, organismul de supraveghere îi solicită să remedieze situația într-un termen stabilit, dacă este cazul. În cazul în care prestatorul respectiv nu remediază situația, dacă este cazul în termenul stabilit de organismul de supraveghere, acesta din urmă, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.		Compatibil		
(3a) În cazul în care autoritățile competente desemnate sau înființate în	3a. Where the competent authorities designated or	(6) În cazul în care autoritatea competentă la nivel național în domeniul securității		Compatibil		

temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute la articolul 21 din respectiva directivă, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.	established pursuant to Article 8(1) of Directive (EU) 2022/2555 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in Article 21 of that Directive, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service that it provides.	cibernetice informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.				
(3b) În cazul în care autoritățile de supraveghere înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679 informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în regulamentul menționat, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.	3b. Where the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in that Regulation, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.	(7) În cazul în care autoritatea națională pentru protecția datelor cu caracter personal informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în Legea nr. 195/2024 privind protecția datelor cu caracter personal, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei încălcări, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.		Compatibil		
(3c) Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire	3c. The supervisory body shall inform the qualified trust service provider of the	(8) Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la		Compatibil		

la retragerea statutului de calificat, al său sau al serviciului în cauză. Organismul de supraveghere informează organismul notificat în temeiul articolului 22 alineatul (3) din prezentul regulament în scopul actualizării listelor sigure menționate la alineatul (1) de la articolul respectiv, precum și autoritatea competentă desemnată sau înființată în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555.	withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body notified pursuant to Article 22(3) of this Regulation for the purposes of updating the trusted lists referred to in paragraph 1 of that Article and the competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555.	retragerea statutului de calificat, al său sau al serviciului în cauză.				
(4) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru: (a) acreditarea organismelor de evaluare a conformității și pentru raportul de evaluare a conformității menționat la alineatul (1); (b) cerințele de audit pe baza cărora organismele de evaluare a conformității își desfășoară evaluarea conformității, inclusiv evaluarea compozită, a prestatorilor de servicii de încredere calificați, astfel cum se menționează la alineatul (1); (c) sistemele de evaluare a conformității utilizate de organismele de evaluare a conformității pentru efectuarea evaluării	4. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the following: (a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1; (b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment, including composite assessment, of the qualified trust service providers as referred to in paragraph 1; (c) the conformity assessment schemes for	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

conformității prestatorilor de servicii de încredere calificați și pentru furnizarea raportului menționat la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the report referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 21 **Inițierea unui serviciu de încredere calificat**	**Article 21** **Initiation of a qualified trust service**	**Articolul 22.** **Inițierea unui serviciu de încredere calificat**				
(1) În cazul în care prestatorii de servicii de încredere intenționează să înceapă prestarea unui serviciu de încredere calificat, aceștia informează organismul de supraveghere cu privire la intenția lor, însoțită de un raport de evaluare a conformității emis de un organism de evaluare a conformității, care confirmă îndeplinirea cerințelor prevăzute în prezentul regulament și la articolul 21 din Directiva (UE) 2022/2555.	1. Where trust service providers intend to start providing a qualified trust service, they shall notify the supervisory body of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.	(1) În cazul în care prestatorii de servicii de încredere intenționează să înceapă prestarea unui serviciu de încredere calificat, aceștia informează organismul de supraveghere cu privire la intenția lor, însoțită de un raport de evaluare a conformității emis de un organism de evaluare a conformității, care confirmă îndeplinirea cerințelor prevăzute în prezenta lege și la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică.		Compatibil		
(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	2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation and, in particular, with the	(2) Organismul de supraveghere verifică dacă prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezenta lege și, în special, cerințele pentru prestatorii de servicii de încredere calificați		Compatibil		

încredere calificați și pentru serviciile de încredere calificate prestate de aceștia. Pentru a verifica respectarea de către prestatorul de servicii de încredere a cerințelor prevăzute la articolul 21 din Directiva (UE) 2022/2555, organismul de supraveghere solicită autorităților competente desemnate sau înființate în temeiul articolului 8 alineatul (1) din respectiva directivă să desfășoare acțiuni de supraveghere în această privință și să furnizeze informații cu privire la rezultat fără întârzieri nejustificate și, în orice caz, în termen de două luni de la primirea cererii respective. În cazul în care verificarea nu este încheiată în termen de două luni de la notificare, autoritățile competente respective informează organismul de supraveghere, specificând motivele întârzierii și termenul în care urmează să se încheie verificarea. 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 prevăzute în prezentul regulament, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta	requirements for qualified trust service providers and for the qualified trust services they provide. In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities designated or established pursuant to Article 8(1) of that Directive to carry out supervisory actions in that regard and to provide information about the outcome without undue delay and in any event within two months of receipt of that request. If the verification is not concluded within two months of the notification, those competent authorities shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded. Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this	și pentru serviciile de încredere calificate prestate de aceștia. (3) În cazul în care organismul de supraveghere constată că prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezenta lege, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta și publică informațiile referitoare la prestatorul respectiv în lista sigură. (4) 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 urmează să se încheie verificarea.				

și informează în consecință organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1), în termen de trei luni de la notificare, în conformitate cu alineatul (1) de la prezentul articol. 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 urmează să se încheie verificarea.	Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article. Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.					
(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).	3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).	(3) Prestatorii de servicii de încredere calificați pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în lista sigură.		Compatibil		
		(4) Prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene obțin statutul de prestator de servicii de încredere calificat în Republica Moldova în baza notificării privind intenția de a presta servicii de încredere calificate pe teritoriul Republicii Moldova,		Compatibil	Republica Moldova păstrează aceste prevederi și în viitoarea lege pentru a asigura un mecanism de recunoaștere unilaterală a prestatorilor de servicii de încredere calificați din statele	

		expediată organismul de supraveghere, fără necesitatea de a fi supuși verificărilor prevăzute pentru prestatorii naționali. (5) Organismul de supraveghere, în termen de 10 zile lucrătoare de la data recepționării notificării, verifică statutul prestatorului de servicii de încredere în lista sigură a statului membru al Uniunii Europene și, în cazul confirmării statutului, asigură includerea prestatorului în lista respectivă. (6) În cazul retragerii statutului de prestator de servicii de încredere calificat într-un stat membru al Uniunii Europene, organismul de supraveghere radiază înregistrarea acestuia din Registrul de evidență a prestatorilor de servicii de încredere calificați.			membre ale Uniunii Europene, având în vedere că aceștia sunt deja supuși cadrului de supraveghere și conformitate prevăzut de Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere (eIDAS), astfel cum a fost modificat prin Regulamentul (UE) 2024/1183 (eIDAS 2). În acest context, prestatorii din UE sunt considerați implicit conformi și cu cadrul normativ al Republicii Moldova care transpune regulamentul european, ceea ce permite evitarea duplicării procedurilor de evaluare și facilitează interoperabilitatea transfrontalieră a serviciilor de încredere.	
(4) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile de notificare și verificare în vederea aplicării alineatelor (1) și (2) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	4. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

	referred to in Article 48(2).					
Articolul 22 **Listele sigure**	**Article 22** **Trusted lists**	**Articolul 23.** **Lista sigură**				
(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.	1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.	(1) Organismul de supraveghere instituie, menține și publică o listă sigură care include informații referitoare la prestatorii de servicii de încredere calificați și la serviciile de încredere calificate prestate de aceștia.		Compatibil		
(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.	2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.	(2) Lista sigură este instituită, menținută și publicată într-un mod securizat, fiind semnată sau sigilată electronic și pusă la dispoziție publicului într-un format adecvat prelucrării automate a datelor.		Compatibil		
(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.	3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.			Prevederi UE neaplicabile		
(4) Comisia pune la dispoziția publicului, printr-un canal sigur, informațiile menționate la alineatul (3)	4. The Commission shall make available to the public, through a secure channel, the	(2) Lista sigură este instituită, menținută și publicată într-un mod securizat, fiind semnată sau sigilată electronic și pusă				

într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.	information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.	la dispoziție publicului într-un format adecvat prelucrării automate a datelor.				
(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). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
Articolul 23 Marca de încredere a UE pentru serviciile de încredere calificate	**Article 23 EU trust mark for qualified trust services**					
(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.	1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.			Prevederi UE neaplicabile		

(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.	2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.			Prevederi UE neaplicabile		
(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).	3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			Prevederi UE neaplicabile		
Articolul 24 **Cerințe pentru prestatorii de servicii de încredere calificați**	**Article 24** **Requirements for qualified trust service providers**	**Articolul 24.** **Cerințe pentru prestatorii de servicii de încredere calificați**				
(1) Atunci când emite un certificat calificat sau un atestat electronic calificat al atributelor, un prestator de servicii de încredere calificat verifică identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia urmează să i se emită certificatul calificat sau atestatul	1. When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate	(1) Atunci când emite un certificat calificat sau un atestat electronic calificat al atributelor, un prestator de servicii de încredere calificat verifică identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia urmează să i se emită certificatul calificat		Compatibil		

electronic calificat al atributelor.	or the qualified electronic attestation of attributes is to be issued.	sau atestatul electronic calificat al atributelor.				
(1a) Verificarea identității menționată la alineatul (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora atunci când este necesar, în conformitate cu actele de punere în aplicare menționate la alineatul (1c): (a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la articolul 8 în ceea ce privește nivelul de asigurare ridicat; (b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu litera (a), (c) sau (d); (c) prin utilizarea altor metode de identificare care asigură identificarea persoanei cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității; (d) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin	1a. The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c: (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high; (b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d); (c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a	(2) Verificarea identității menționată la alin. (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora atunci când este necesar, în conformitate cu actele de punere în aplicare aprobate de Guvern: a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la art. 12 în ceea ce privește nivelul de asigurare ridicat; b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu lit. (a), (c) sau (d); c) prin utilizarea altor metode de identificare care asigură identificarea persoanei cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității; d) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în		Compatibil		

utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern.	conformity assessment body; (d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.	conformitate cu cadrul normativ aplicabil.				
(1b) Verificarea atributelor menționată la alineatul (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, atunci când este necesar, în conformitate cu actele de punere în aplicare menționate la alineatul (1c): (a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la articolul 8 în ceea ce privește nivelul de asigurare ridicat; (b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu alineatul (1a) litera (a), (c) sau (d); (c) prin intermediul unui atestat electronic calificat al atributelor;	1b. The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c: (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high; (b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with	(3) Verificarea atributelor menționată la alin. (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, atunci când este necesar, în conformitate cu actele de punere în aplicare stabilite de Guvern: a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la art. 12 în ceea ce privește nivelul de asigurare ridicat; b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu alin. (3) lit. (a), (c) sau (d); c) prin intermediul unui atestat electronic calificat al atributelor; d) prin utilizarea altor metode, care asigură		Compatibil		

(d) prin utilizarea altor metode, care asigură verificarea atributelor cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității; (e) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern.	paragraph 1a, point (a), (c) or (d); (c) by means of a qualified electronic attestation of attributes; (d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body; (e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.	verificarea atributelor cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității; e) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cadrul normativ aplicabil.				
(1c) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru verificarea identității și a atributelor în conformitate cu alineatele (1), (1a) și (1b) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	1c. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

(2) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate: (a) informează organismul de supraveghere cu cel puțin o lună înainte de punerea în aplicare a oricărei modificări în prestarea serviciilor sale de încredere calificate sau cu cel puțin trei luni înainte în cazul în care intenționează să înceteze activitățile respective; (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; (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; (d) înainte de stabilirea unei relații contractuale, informează, în mod clar, cuprinzător și ușor accesibil, într-un spațiu accesibil publicului și în mod individual, orice persoană care dorește să utilizeze un	2. A qualified trust service provider providing qualified trust services shall: (a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities; (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards; (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law; (d) before entering into a contractual relationship, inform, in a clear, comprehensive and	(4) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate: 1) informează organismul de supraveghere cu cel puțin o lună înainte de punerea în aplicare a oricărei modificări în prestarea serviciilor sale de încredere calificate sau cu cel puțin trei luni înainte în cazul în care intenționează să înceteze activitățile respective; 2) 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; 3) în ceea ce privește riscul de răspundere pentru daune în conformitate cu art. 17, menține suficiente resurse financiare și/sau obține o asigurare de răspundere adecvată, în conformitate cu dreptul intern; 4) înainte de stabilirea unei relații contractuale, informează, în mod clar, cuprinzător și ușor accesibil, într-un spațiu accesibil publicului și în mod individual, orice persoană care dorește să utilizeze un serviciu de încredere calificat în ceea ce privește clauzele și		Compatibil		

serviciu de încredere calificat în ceea ce privește clauzele și condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia; (e) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea, inclusiv prin folosirea unor tehnici criptografice adecvate; (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; (fa) în pofida articolului 21 din Directiva (UE) 2022/2555, dispune de politici adecvate și ia măsuri corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere calificat, inclusiv cel puțin măsuri referitoare la următoarele aspecte:	easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use; (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques; (f) use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity; (fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business,	condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia; 5) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea, inclusiv prin folosirea unor tehnici criptografice adecvate; 6) utilizează sisteme demne de încredere pentru a stoca datele care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât: a) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul persoanei la care se referă datele; b) numai persoanele autorizate să poată introduce și modifica datele stocate; c) autenticitatea datelor să poată fi controlată; 7) dispune de politici adecvate și ia măsuri corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere calificat, inclusiv cel puțin măsuri referitoare la următoarele aspecte: a) procedurile de înregistrare și de integrare legate de un serviciu;				

(i) procedurile de înregistrare și de integrare legate de un serviciu; (ii) controalele procedurale sau administrative; (iii) gestionarea și implementarea serviciilor; (fb) notifică organismului de supraveghere, persoanelor afectate care pot fi identificate, altor organisme competente relevante, după caz, și, la cererea organismului de supraveghere, publicului, dacă chestiunea este de interes public, orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (fa) punctul (i), (ii) sau (iii) care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la producerea incidentului; (g) ia măsuri adecvate împotriva falsificării, furtului sau însușirii ilegale de date ori împotriva ștergerii sau modificării neautorizate a datelor sau a acțiunii neautorizate de a le face inaccesibile; (h) înregistrează și menține accesibile atât timp cât este necesar, după încetarea activității prestatorului de	operational and other direct or indirect risks to the provision of the qualified trust service, including at least measures related to the following: (i) registration and onboarding procedures for a service; (ii) procedural or administrative checks; (iii) the management and implementation of services; (fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa)(i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident; (g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or	b) controalele procedurale sau administrative; c) gestionarea și implementarea serviciilor; 8) notifică organismului de supraveghere, persoanelor afectate care pot fi identificate, altor organisme competente relevante, după caz, și, la cererea organismului de supraveghere, publicului, dacă chestiunea este de interes public, orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la pct. 7 care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la producerea incidentului; 9) ia măsuri adecvate împotriva falsificării, furtului sau însușirii ilegale de date ori împotriva ștergerii sau modificării neautorizate a datelor sau a acțiunii neautorizate de a le face inaccesibile; 10) înregistrează și menține accesibile atât timp cât este necesar, după încetarea activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către acesta, în scopul de a furniza dovezi în				

servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către acesta, în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic; (i) are un plan actualizat pentru a asigura, în cazul încetării serviciului, continuitatea serviciului conform dispozițiilor verificate de organismul de supraveghere în conformitate cu articolul 46b alineatul (4) litera (i); (k) în cazul prestatorilor de servicii de încredere calificați care eliberează certificate calificate, instituie și actualizează permanent o bază de date a certificatelor. Organismul de supraveghere poate solicita informații în plus față de informațiile notificate în temeiul primului paragraf litera (a) sau rezultatul unei evaluări a conformității și poate stabili anumite condiții pentru acordarea permisiunii de a pune în aplicare modificările preconizate ale serviciilor de încredere calificate. 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,	rendering data inaccessible; (h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically; (i) have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i); (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database. The supervisory body may request information in addition to the information notified pursuant to point (a) of the first subparagraph or the result of a conformity assessment and may condition the granting of the	procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic; 11) are un plan actualizat pentru a asigura, în cazul încetării serviciului, continuitatea serviciului conform dispozițiilor verificate de organismul de supraveghere în conformitate cu art. 64 alin. (3) pct. 2) lit. f); 12) în cazul prestatorilor de servicii de încredere calificați care eliberează certificate calificate, instituie și actualizează permanent o bază de date a certificatelor. (5) Organismul de supraveghere poate solicita informații în plus față de informațiile notificate în temeiul alin. (4) sau rezultatul unei evaluări a conformității și poate stabili anumite condiții pentru acordarea permisiunii de a pune în aplicare modificările preconizate ale serviciilor de încredere calificate. 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 urmează să se încheie verificarea.				

specificând motivele întârzierii și termenul în care urmează să se încheie verificarea.	permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.					
(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.	3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.	(6) 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.		Compatibil		
(4) Cu privire la alineatul (3), prestatorii de servicii de încredere calificați care emit certificate calificate 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	4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per	(7) Prestatorii de servicii de încredere calificați care emit certificate calificate 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		Compatibil		

moment și după expirarea perioadei de valabilitate a certificatului, în mod automat, fiabil, gratuit și eficient.	certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.	valabilitate a certificatului, în mod automat, fiabil, gratuit și eficient.				
(4a) Alineatele (3) și (4) se aplică în mod corespunzător revocării atestatelor electronice calificate ale atributelor.	4a. Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.	Alin. (6) și (7) se aplică în mod corespunzător revocării atestatelor electronice calificate ale atributelor.		Compatibil		
(4b) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47, pentru a stabili măsurile suplimentare menționate la alineatul (2) litera (fa) de la prezentul articol.	4b. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2, point (fa), of this Article.			Prevederi UE neaplicabile		
(5) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatul (2) de la prezentul articol. În cazul în care standardele, specificațiile și procedurile respective sunt respectate, se prezumă că sunt respectate cerințele prevăzute la prezentul alineat. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	5. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 2 of this Article. Compliance with the requirements laid down in this paragraph shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				

Articolul 24a **Recunoașterea serviciilor de încredere calificate**	**Article 24a** **Recognition of qualified trust services**	**Articolul 25. Recunoașterea serviciilor de încredere calificate furnizate de prestatori de servicii calificate din statele membre ale Uniunii Europene**				
(1) Semnăturile electronice calificate bazate pe un certificat calificat emis într-un stat membru și sigiliile electronice calificate bazate pe un certificat calificat emis într-un stat membru sunt recunoscute drept semnături electronice calificate și, respectiv, drept sigilii electronice calificate în toate celelalte state membre.	1. Qualified electronic signatures based on a qualified certificate issued in one Member State and qualified electronic seals based on a qualified certificate issued in one Member State shall be recognised, respectively, as qualified electronic signatures and qualified electronic seals in all other Member States.	(1) Semnăturile electronice calificate bazate pe un certificat calificat emis într-un stat membru al Uniunii Europene și sigiliile electronice calificate bazate pe un certificat calificat emis într-un stat membru al Uniunii Europene sunt recunoscute drept semnături electronice calificate și, respectiv, drept sigilii electronice calificate în Republica Moldova.		Compatibil		
(2) Dispozitivele de creare a semnăturilor electronice calificate și dispozitivele de creare a sigiliilor electronice calificate certificate într-un stat membru sunt recunoscute drept dispozitive de creare a semnăturilor electronice calificate și, respectiv, drept dispozitive de creare a sigiliilor electronic calificate în toate celelalte state membre.	2. Qualified electronic signature creation devices and qualified electronic seal creation devices certified in one Member State shall be recognised, respectively, as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States.	(2) Dispozitivele de creare a semnăturilor electronice calificate și dispozitivele de creare a sigiliilor electronice calificate certificate într-un stat membru al Uniunii Europene sunt recunoscute drept dispozitive de creare a semnăturilor electronice calificate și, respectiv, drept dispozitive de creare a sigiliilor electronic calificate în Republica Moldova.		Compatibil		
(3) Un certificat calificat pentru semnăturile electronice, un certificat calificat pentru sigilii electronice, un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a	3. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic	(3) Un certificat calificat pentru semnăturile electronice, un certificat calificat pentru sigilii electronice, un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a		Compatibil		

semnăturii electronice la distanță și un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță furnizat într-un stat membru este recunoscut drept certificat calificat pentru semnăturile electronice, drept certificat calificat pentru sigilii electronice, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și, respectiv, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță în toate celelalte state membre.	signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices provided in one Member State shall be recognised, respectively, as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States.	semnăturii electronice la distanță și un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță furnizat într-un stat membru al Uniunii Europene este recunoscut drept certificat calificat pentru semnăturile electronice, drept certificat calificat pentru sigilii electronice, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și, respectiv, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță în Republica Moldova.				
(4) Un serviciu de validare calificat pentru semnături electronice calificate și un serviciu de validare calificat pentru sigilii electronice calificate furnizat într-un stat membru este recunoscut drept serviciu de validare calificat pentru semnături electronice calificate și, respectiv, drept serviciu de validare calificat pentru sigilii electronice calificate în toate celelalte state membre.	4. A qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States.	(4) Un serviciu de validare calificat pentru semnături electronice calificate și un serviciu de validare calificat pentru sigilii electronice calificate furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu de validare calificat pentru semnături electronice calificate și, respectiv, drept serviciu de validare calificat pentru sigilii electronice calificate în Republica Moldova.		Compatibil		
(5) Un serviciu calificat de păstrare a semnăturilor electronice calificate și un	5. A qualified preservation service for qualified electronic	(5) Un serviciu calificat de păstrare a semnăturilor electronice calificate și un		Compatibil		

serviciu calificat de păstrare a sigiliilor electronice calificate furnizat într-un stat membru este recunoscut drept serviciu calificat de păstrare a semnăturilor electronice calificate și, respectiv, drept serviciu calificat de păstrare a sigiliilor electronice calificate în toate celelalte state membre.	signatures and a qualified preservation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States.	serviciu calificat de păstrare a sigiliilor electronice calificate furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu calificat de păstrare a semnăturilor electronice calificate și, respectiv, drept serviciu calificat de păstrare a sigiliilor electronice calificate în Republica Moldova.				
(6) O marcă temporală electronică calificată furnizată într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate celelalte state membre.	6. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States.	(6) O marcă temporală electronică calificată furnizată într-un stat membru al Uniunii Europene este recunoscută drept marcă temporală electronică calificată în Republica Moldova.		Compatibil		
(7) Un certificat calificat pentru autentificarea unui site internet emis într-un stat membru este recunoscut drept certificat calificat pentru autentificarea unui site internet în toate celelalte state membre.	7. A qualified certificate for website authentication issued in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States.	(7) Un certificat calificat pentru autentificarea unui site internet emis într-un stat membru al Uniunii Europene este recunoscut drept certificat calificat pentru autentificarea unui site internet în Republica Moldova.		Compatibil		
(8) Un serviciu de distribuție electronică înregistrată calificat furnizat într-un stat membru este recunoscut drept serviciu de distribuție electronică înregistrată calificat în toate celelalte state membre.	8. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States.	(8) Un serviciu de distribuție electronică înregistrată calificat furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu de distribuție electronică înregistrată calificat în Republica Moldova.		Compatibil		
(9) Un atestat electronic calificat al atributelor emis într-un stat membru este recunoscut drept atestat electronic calificat al	9. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified	(9) Un atestat electronic calificat al atributelor emis într-un stat membru al Uniunii Europene este recunoscut drept atestat electronic		Compatibil		

atributelor în toate celelalte state membre.	electronic attestation of attributes in all other Member States.	calificat al atributelor în Republica Moldova.				
(10) Un serviciu calificat de arhivare electronică furnizat într-un stat membru este recunoscut drept serviciu calificat de arhivare electronică în toate celelalte state membre.	10. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.	(10) Un serviciu calificat de arhivare electronică furnizat într-un stat membru al Uniunii Europene este recunoscut drept serviciu calificat de arhivare electronică în Republica Moldova.		Compatibil		
(11) Un registru electronic calificat furnizat într-un stat membru este recunoscut drept registru electronic calificat în toate celelalte state membre.	11. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.	(11) Un registru electronic calificat furnizat într-un stat membru al Uniunii Europene este recunoscut drept registru electronic calificat în Republica Moldova.		Compatibil		
SECȚIUNEA 4 **Semnătura electronică**	**SECTION 4** **Electronic signatures**	**Secțiunea a 4-a** **Semnătura electronică**				
Articolul 25 **Efectele juridice ale semnăturilor electronice**	**Article 25** **Legal effects of electronic signatures**	**Articolul 26.** **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.	1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.	(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.		Compatibil		
(2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.	2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.	(2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.		Compatibil		
Articolul 26	**Article 26**	**Articolul 27.** **Cerințe pentru semnături electronice avansate**				

Cerințe pentru semnături electronice avansate	**Requirements for advanced electronic signatures**					
1. O semnătură electronică avansată îndeplinește următoarele cerințe: (a) face trimitere exclusiv la semnatar; (b) permite identificarea semnatarului; (c) este creată utilizând date de creare a semnăturilor 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.	1. An advanced electronic signature shall meet the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.	(1) 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 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.		Compatibil		
2. Până la 21 mai 2026, Comisia evaluează dacă este necesar să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru semnăturile electronice avansate. Pe baza rezultatului evaluării respective, Comisia poate adopta astfel de acte de punere în aplicare. În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele	2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic signatures. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic	(2) În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele referitoare la semnăturile electronice avansate prevăzute la alin. (1).		Compatibil		

referitoare la semnăturile electronice avansate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	signature complies with the standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 27 Semnăturile electronice în cadrul serviciilor publice	**Article 27 Electronic signatures in public services**	**Articolul 28. 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 întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).	1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.	(1) În cadrul prestării serviciilor publice electronice de către organismele din sectorul public sau în numele acestora, atunci când cadrul normativ aplicabil solicită aplicarea unei semnături electronice, aceasta se realizează prin utilizarea semnăturii electronice calificate.		Compatibil		
(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	2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures	(2) Semnătura electronică calificată utilizată în cadrul serviciilor publice produce efecte juridice echivalente semnăturii olografe și este recunoscută de către toate autoritățile și instituțiile publice.		Compatibil		

avansate bazate pe un certificat calificat și semnăturile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).	based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 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.	3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.	(3) Organismele din sectorul public nu pot solicita, pentru utilizarea serviciilor publice electronice, un nivel de securitate al semnăturii electronice mai ridicat decât cel al semnăturii electronice calificate.		Compatibil		
(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. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 28 **Certificate calificate pentru semnăturile electronice**	**Article 28** **Qualified certificates for electronic signatures**	**Articolul 29.** **Certificate calificate pentru semnăturile electronice**				
(1) Certificatele calificate pentru semnăturile electronice îndeplinesc	1. Qualified certificates for electronic signatures shall meet the	(1) Certificatele calificate pentru semnăturile		Compatibil		

cerințele prevăzute în anexa I.	requirements laid down in Annex I.	electronice îndeplinesc cerințele prevăzute la art. 30.				
(2) Certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa I.	2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.	(2) Certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la art. 30.		Compatibil		
(3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate.	3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.	(3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate.		Compatibil		
(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.	4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	(6) 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.		Compatibil		
(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	5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature: (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;	(4) Prestatorul de servicii de încredere suspendă valabilitatea certificatelor calificate pentru semnăturile electronice la cererea titularilor acestora. (5) În cazul în care un certificat calificat pentru semnătura electronică a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare, iar perioada de suspendare este		Compatibil		

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.	(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.	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) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru semnăturile electronice. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate 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).	6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(7) În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la art. 30.		Compatibil		
Articolul 29 Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate	**Article 29 Requirements for qualified electronic signature creation devices**	**Articolul 31. Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate**				
(1) Dispozitivele de creare a semnăturilor electronice calificate îndeplinesc	1. Qualified electronic signature creation devices shall meet the	(1) Dispozitivele de creare a semnăturilor electronice		Compatibil		

cerințele prevăzute în anexa II.	requirements laid down in Annex II.	calificate îndeplinesc cerințele prevăzute la alin. (2) și (3).				
(1a) Generarea sau gestionarea datelor de creare a semnăturii electronice sau duplicarea unor astfel de date de creare a semnăturii în scopul creării unei copii de rezervă se realizează numai în numele semnatarului și la cererea acestuia și de către un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a semnăturii electronice la distanță.	1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.	Generarea sau gestionarea datelor de creare a semnăturii electronice sau duplicarea unor astfel de date de creare a semnăturii în scopul creării unei copii de rezervă se realizează numai în numele semnatarului și la cererea acestuia și de către un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a semnăturii electronice la distanță.		Compatibil		
(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).	2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(5) În cazul în care un dispozitiv de creare a semnăturilor electronice calificat îndeplinește standardele stabilite de Guvern, se presupune că acesta respectă cerințele prevăzute la alin. (2) și (3).		Compatibil		
Articolul 29a Cerințe privind un serviciu calificat pentru	**Article 29a Requirements for a qualified service for**	**Articolul 32. Cerințe privind un serviciu calificat pentru gestionarea**				

gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță	**the management of remote qualified electronic signature creation devices**	**dispozitivelor calificate de creare a semnăturii electronice la distanță**				
(1) Gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță în calitate de serviciu calificat se efectuează numai de către un prestator de servicii de încredere calificat care: (a) generează sau gestionează datele de creare a semnăturilor electronice în numele semnatarului; (b) în pofida punctului 1 litera (d) din anexa II, duplică datele de creare a semnăturilor electronice numai în scopul creării unei copii de rezervă, cu condiția să fie îndeplinite următoarele cerințe: (i) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale; (ii) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului; (c) respectă toate cerințele identificate în raportul de certificare a dispozitivului calificat specific de creare a semnăturii electronice la distanță, emis în temeiul articolului 30.	1. The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that: (a) generates or manages electronic signature creation data on behalf of the signatory; (b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met: (i) the security of the duplicated datasets must be at the same level as for the original datasets; (ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service; (c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30.	Gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță în calitate de serviciu calificat se efectuează numai de către un prestator de servicii de încredere calificat care: 1) generează sau gestionează datele de creare a semnăturilor electronice în numele semnatarului; 2) duplică datele de creare a semnăturilor electronice numai în scopul creării unei copii de rezervă, cu condiția să fie îndeplinite următoarele cerințe: a) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale; b) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului; 3) respectă toate cerințele identificate în raportul de certificare a dispozitivului calificat specific de creare a semnăturii electronice la distanță, emis în temeiul art. 33.		Compatibil		
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi:		Compatibil		

standarde de referință și, dacă este necesar, specificații și proceduri în scopul aplicării alineatului (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	reference standards and, where necessary, specifications and procedures for the purposes of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
Articolul 30 Certificarea dispozitivelor de creare a semnăturilor electronice calificate	**Article 30 Certification of qualified electronic signature creation devices**	**Articolul 33. Certificarea dispozitivelor de creare a semnăturilor 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.	1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.	(1) Conformitatea dispozitivelor de creare a semnăturii electronice calificate cu cerințele prevăzute la alin. (2) și (3) din art. 31 este certificată de organisme de evaluare a conformității.		Compatibil		
(2) Statele membre notifică Comisiei denumirile și adresele organismului public sau privat menționat la alineatul (1). Comisia pune informațiile respective la dispoziția statelor membre.	2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.			Prevederi UE neaplicabile		
(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	3. The certification referred to in paragraph 1 shall be based on one of the following: (a) a security evaluation process carried out in accordance with one of	(2) Certificarea menționată la alin. (1) se bazează pe unul dintre următoarele elemente: a) un proces de evaluare de securitate efectuat în conformitate cu unul dintre		Compatibil		

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).	the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or (b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing. The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	standardele pentru evaluarea securității produselor din domeniul tehnologiei informației stabilite de Guvern; sau b) un alt proces decât procesul prevăzut la lit. a), cu condiția ca acest proces să utilizeze niveluri de securitate comparabile și ca organisme de evaluare a conformității să notifice organismului de supraveghere respectivul proces. Procesul respectiv poate fi utilizat numai în absența standardelor menționate la lit. a) sau dacă un proces de evaluare de securitate menționat la lit. a) este în curs de desfășurare.				
(3a) Perioada de valabilitate a certificării menționate la alineatul (1) nu depășește cinci ani, cu condiția efectuării unei evaluări a vulnerabilităților	3a The validity of a certification referred to in paragraph 1 shall not exceed five years, provided that vulnerabilities	(3) Perioada de valabilitate a certificării menționate la alin. (1) nu depășește cinci ani, cu condiția efectuării unei evaluări a vulnerabilităților la fiecare doi		Compatibil		

la fiecare doi ani. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate, certificarea este anulată.	assessments are carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.	ani. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate, certificarea este anulată.				
(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.	4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 31 Publicarea unei liste a dispozitivelor de creare a semnăturilor electronice certificate și calificate	**Article 31 Publication of a list of certified qualified electronic signature creation devices**	**Articolul 33. Certificarea dispozitivelor de creare a semnăturilor electronice 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 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.	1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature	(4) Organismul de supraveghere publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate.		Compatibil		

	creation devices that are no longer certified.					
(2) Pe baza informațiilor primite, Comisia stabilește, publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate.	2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.			Compatibil		
(3) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile aplicabile în vederea îndeplinirii cerințelor prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	3. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purpose of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 32 **Cerințe pentru validarea semnăturilor electronice calificate**	**Article 32** **Requirements for the validation of qualified electronic signatures**	**Articolul 34.** **Cerințe pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate calificate**				
(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții: (a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu anexa I; (b) certificatul calificat a fost emis de un prestator de	1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that: (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	(1) Procesul de validare a unei semnături electronice calificate sau a unei semnături electronice avansate bazate pe un certificat calificat confirmă validitatea unei semnături electronice cu următoarele condiții: a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu art. 30;		Compatibil		

servicii de încredere calificat și a fost valabil în momentul semnării; (c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar; (d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului; (e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim; (f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat; (g) integritatea datelor semnate nu a fost compromisă; (h) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării. În cazul în care validarea semnăturilor electronice calificate respectă standardele, specificațiile și procedurile menționate la alineatul (3), se prezumă că sunt respectate cerințele prevăzute la primul paragraf de la prezentul alineat.	(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; (c) the signature validation data corresponds to the data provided to the relying party; (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party; (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; (f) the electronic signature was created by a qualified electronic signature creation device; (g) the integrity of the signed data has not been compromised; (h) the requirements provided for in Article 26 were met at the time of signing. Compliance with the requirements laid down in the first subparagraph of this paragraph shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3.	b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării; c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar; d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului; e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim; f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat; g) integritatea datelor semnate nu a fost compromisă; h) cerințele prevăzute la art. 27 au fost îndeplinite la momentul semnării. (2) Suplimentar cerințelor prevăzute la alin. (1), procesul de validare a unei semnături electronice calificate include verificarea faptului că semnătura electronică a fost creată prin intermediul unui dispozitiv calificat de creare a semnăturilor electronice.				

(2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.	2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	(3) Sistemul utilizat pentru validarea semnăturii electronice calificate sau a semnăturii electronice avansate bazate pe un certificat calificat furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.		Compatibil		
(3) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru validarea semnăturilor electronice calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	În cazul în care validarea semnăturilor electronice calificate sau a sau a semnăturilor electronice avansate bazate pe certificate calificate respectă standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1), inclusiv și a celei prevăzute la alin. (2) în cazul semnăturilor electronice calificate .		Compatibil		
Articolul 32a Cerințe pentru validarea semnăturilor electronice avansate bazate pe certificate calificate	**Article 32a Requirements for the validation of advanced electronic signatures based on qualified certificates**	**Articolul 34. Cerințe pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate calificate**				
(1) Prin procesul de validare a unei semnături electronice avansate bazate pe un certificat calificat se confirmă validitatea semnăturii electronice avansate bazate pe un certificat calificat în următoarele condiții: (a) certificatul care stă la baza semnăturii să fi fost, la	1. The process for the validation of an advanced electronic signature based on a qualified certificate shall confirm the validity of an advanced electronic signature based on a qualified certificate, provided that:	(1) Procesul de validare a unei semnături electronice calificate sau a unei semnături electronice avansate bazate pe un certificat calificat confirmă validitatea unei semnături electronice cu următoarele condiții: a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un		Compatibil		

momentul semnării, un certificat calificat pentru semnătura electronică conform cu anexa I; (b) certificatul calificat să fi fost emis de un prestator de servicii de încredere calificat și să fi fost valabil la momentul semnării; (c) datele de validare a semnăturii să corespundă datelor furnizate de beneficiar; (d) setul unic de date care reprezintă semnatarul în certificat să fie furnizat corect beneficiarului; (e) în cazul în care la momentul semnării s-a folosit un pseudonim, utilizarea acestuia să fie indicată clar beneficiarului; (f) integritatea datelor semnate să nu fi fost compromisă; (g) cerințele prevăzute la articolul 26 să fi fost îndeplinite la momentul semnării.	(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I; (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; (c) the signature validation data corresponds to the data provided to the relying party; (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party; (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; (f) the integrity of the signed data has not been compromised; (g) the requirements provided for in Article 26 were met at the time of signing.	certificat calificat pentru semnătura electronică în conformitate cu art. 30; b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării; c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar; d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului; e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim; f) integritatea datelor semnate nu a fost compromisă; g) cerințele prevăzute la art. 27 au fost îndeplinite la momentul semnării.				
(2) Sistemul utilizat pentru validarea semnăturii electronice avansate bazate pe un certificat calificat furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să	2. The system used for validating the advanced electronic signature based on qualified certificate shall provide to the relying party the correct result of the validation process and shall allow the relying	(3) Sistemul utilizat pentru validarea semnăturii electronice calificate sau a semnăturii electronice avansate bazate pe un certificat calificat furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să		Compatibil		

detecteze orice aspect relevant pentru securitate.	party to detect any security relevant issues.	detecteze orice aspect relevant pentru securitate.				
(3) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru validarea semnăturilor electronice avansate bazate pe certificate calificate. În cazul în care validarea semnăturii electronice avansate bazate pe certificate calificate îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of advanced electronic signatures based on qualified certificates. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the validation of advanced electronic signature based on qualified certificates complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(4) În cazul în care validarea semnăturilor electronice calificate sau a sau a semnăturilor electronice avansate bazate pe certificate calificate respectă standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1), inclusiv și a celei prevăzute la alin. (2) în cazul semnăturilor electronice calificate .		Compatibil		
Articolul 33 Serviciul calificat de validare a semnăturilor electronice calificate	**Article 33 Qualified validation service for qualified electronic signatures**	**Articolul 35. Serviciul calificat de validare a semnăturilor electronice calificate**				
(1) Un serviciu calificat de validare a semnăturilor 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	1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:	(1) Un serviciu calificat de validare a semnăturilor electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care: a) realizează validarea în conformitate cu art. 34 alin. (1) și alin. (2); și		Compatibil		

(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.	(a) provides validation in compliance with Article 32(1); and (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	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.				
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru serviciul calificat de validare menționat la alineatul (1) de la prezentul articol. În cazul în care serviciul calificat de validare pentru semnături electronice calificate îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele de la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1 of this Article. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(2) În cazul în care serviciul calificat de validare pentru semnături electronice calificate îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele de la alin. (1).		Compatibil		
Articolul 34	**Article 34**	**Articolul 36.**				

Serviciul calificat de păstrare a semnăturilor electronice calificate	**Qualified preservation service for qualified electronic signatures**	**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 semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.	1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.	(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 semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.		Compatibil		
(1a) În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).	1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 2.	(2) În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).		Compatibil		
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru serviciul calificat de păstrare a semnăturilor electronice calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

	referred to in Article 48(2).					
SECȚIUNEA 5 **Sigiliile electronice**	**SECTION 5** **Electronic seals**	**Secțiunea a 5-a** **Sigiliile electronice**				
Articolul 35 **Efectele juridice ale sigiliilor electronice**	**Article 35** **Legal effects of electronic seals**	**Articolul 37.** **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.	1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.	(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.		Compatibil		
(2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.	2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.	(2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.		Compatibil		
Articolul 36 **Cerințele pentru sigiliile electronice avansate**	**Article 36** **Requirements for advanced electronic seals**	**Articolul 38.** **Cerințele pentru sigiliile electronice avansate**				
(1) 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	An advanced electronic seal shall meet the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high	(1) Un sigiliu electronic avansat îndeplinește următoarele cerințele: 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		Compatibil		

controlul său, cu un nivel ridicat de încredere; și (d) este legat de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată.	level of confidence, use under his control; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.	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.				
2. Până la 21 mai 2026, Comisia evaluează dacă este necesar să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru sigiliile electronice avansate. Pe baza rezultatului evaluării respective, Comisia poate adopta astfel de acte de punere în aplicare. În cazul în care un sigiliu electronic avansat îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele privind sigiliile electronice avansate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic seals. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(2) În cazul în care un sigiliu electronic avansat îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).		Compatibil		
Articolul 37 **Sigiliile electronice în cadrul serviciilor publice**	**Article 37** **Electronic seals in public services**	**Articolul 39.** **Sigiliile electronice în cadrul serviciilor publice**				
(1) În cazul în care un stat membru solicită un sigiliu electronic avansat pentru	1. If a Member State requires an advanced electronic seal in order	(1) În cadrul prestării serviciilor publice electronice de către autoritățile publice și		Compatibil		

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 întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).	to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.	instituții publice sau în numele acestora, atunci când cadrul normativ aplicabil solicită aplicarea unui sigiliu electronic, aceasta se realizează prin utilizarea sigiliului electronic calificat.				
(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 întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).	2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.					
(3) Statele membre nu solicită un sigiliu electronic la un 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.	3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.	(2) Organismele din sectorul public nu pot solicita, pentru utilizarea serviciilor publice electronice, un nivel de securitate al sigiliului electronic mai ridicat decât cel al sigiliului electronic calificat.		Compatibil		

(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).	5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 38 Certificate calificate pentru sigiliul electronic	**Article 38 Qualified certificates for electronic seals**	**Articolul 40. Certificate calificate pentru sigiliul electronic**				
(1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III.	1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.	(1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute art. 41.		Compatibil		
(2) Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa III.	2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.	(2) Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la art. 41.		Compatibil		
(3) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate.	3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.	(3) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate.		Compatibil		

(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.	4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	(6) 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.		Compatibil		
(5) Sub rezerva următoarelor condiții, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a certificatelor calificate pentru sigiliile electronice: (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; (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.	5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals: (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension; b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.	(4) Prestatorul de servicii de încredere suspendă valabilitatea certificatelor calificate pentru sigiliile electronice la cererea titularilor acestora. (5) În cazul în care un certificat calificat pentru sigiliu electronic a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare, iar 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.		Compatibil		
(6) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru sigiliul electronic. În	6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for	(7) În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la art. 41.		Compatibil		

cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate 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).	electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 39 **Dispozitive de creare a sigiliilor electronice calificate**	**Article 39** **Qualified electronic seal creation devices**	**Articolul 42.** **Dispozitive de creare a sigiliilor electronice calificate**				
(1) Articolul 29 se aplică mutatis mutandis cerințelor pentru dispozitivele de creare a sigiliilor electronice calificate.	1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.	Dispozițiile art. 31 și 33 privind cerințele aplicabile dispozitivelor de creare a semnăturilor electronice calificate, certificarea acestora și publicarea listei dispozitivelor certificate și calificate se aplică, în mod corespunzător, și dispozitivelor de creare a sigiliilor electronice calificate.		Compatibil		
(2) Articolul 30 se aplică mutatis mutandis certificării dispozitivelor de creare a sigiliilor electronice calificate.	2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.			Compatibil		
(3) Articolul 31 se aplică mutatis mutandis publicării unei liste a dispozitivelor de creare a sigiliilor electronice certificate și calificate.	3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.			Compatibil		
Articolul 39a **Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță**	**Article 39a** **Requirements for a qualified service for the management of remote qualified electronic seal creation devices**	**Articolul 43.** **Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță**				

Articolul 29a se aplică mutatis mutandis unui serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță.	Article 29a shall apply mutatis mutandis to a qualified service for the management of remote qualified electronic seal creation devices.	Dispozițiile art. 33 privind cerințele aplicabile serviciului calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță se aplică și serviciului calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță.		Compatibil		
Articolul 40 **Validarea și păstrarea sigiliilor electronice calificate**	**Article 40** **Validation and preservation of qualified electronic seals**	**Articolul 44.** **Validarea și păstrarea sigiliilor electronice calificate**				
Articolele 32, 33 și 34 se aplică mutatis mutandis validării și păstrării sigiliilor electronice calificate.	Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	Dispozițiile art. 34, 35 și 36 privind validarea și păstrarea semnăturilor electronice calificate se aplică și validării și păstrării sigiliilor electronice calificate.		Compatibil		
Articolul 40a **Cerințe pentru validarea sigiliilor electronice avansate bazate pe certificate calificate**	**Article 40a** **Requirements for the validation of advanced electronic seals based on qualified certificates**	**Articolul 45.** **Cerințe pentru validarea sigiliilor electronice avansate bazate pe certificate calificate**				
Articolul 32a se aplică mutatis mutandis validării sigiliilor electronice avansate bazate pe certificate calificate.	Article 32a shall apply mutatis mutandis to the validation of advanced electronic seals based on qualified certificates.	Dispozițiile articolului 34 privind cerințele pentru validarea semnăturilor electronice avansate bazate pe certificate calificate se aplică și validării sigiliilor electronice avansate bazate pe certificate calificate.		Compatibil		
SECȚIUNEA 6 **Mărcile temporale electronice**	**SECTION 6** **Electronic time stamps**	**Secțiunea a 6-a** **Mărcile temporale electronice**				
Articolul 41 **Efectul juridic al mărcilor temporale electronice**	**Article 41** **Legal effect of electronic time stamps**	**Articolul 46.** **Efectul juridic al mărcilor temporale electronice**				
(1) Unei mărci temporale electronice nu i se refuză	1. An electronic time stamp shall not be	(1) Unei mărci temporale electronice nu i se refuză		Compatibil		

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.	denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.	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.	2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.	(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 42 **Cerințe pentru mărcile temporale electronice calificate**	**Article 42** **Requirements for qualified electronic time stamps**	**Articolul 47.** **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.	1. A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by	(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.		Compatibil		

	some equivalent method.					
(1a) În cazul în care legătura dintre dată și oră și date și exactitatea sursei orei indicate îndeplinesc standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).	1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 2.	(2) În cazul în care legătura dintre dată și oră și date și exactitatea sursei orei indicate îndeplinesc standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).		Compatibil		
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru legătura dintre dată și oră și date și pentru stabilirea exactității surselor orei indicate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
SECȚIUNEA 7 **Serviciul de distribuție electronică înregistrată**	**SECTION 7** **Electronic registered delivery service**	**Secțiunea a 7-a** **Serviciul de distribuție electronică înregistrată**				
Articolul 43 **Efectul juridic al unui serviciu de distribuție electronică înregistrată**	**Article 43** **Legal effect of an electronic registered delivery service**	**Articolul 48.** **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	1. Data sent and received using an electronic registered delivery service shall	(1) Datelor trimise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză		Compatibil		

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 calificat.	not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.	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 calificat beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de către destinatarul identificat și a preciziei datei și orei trimiterii și primirii datelor indicate de serviciul de distribuție electronică înregistrată calificat.	2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.	(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		
Articolul 44 **Cerințe pentru serviciile de distribuție electronică înregistrată calificate**	**Article 44** **Requirements for qualified electronic registered delivery services**	**Articolul 49.** **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;	1. Qualified electronic registered delivery services shall meet the following requirements: (a) they are provided by one or more qualified trust service provider(s); (b) they ensure with a high level of confidence the identification of the sender;	(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;		Compatibil		

(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 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 literele (a)-(f) se aplică tuturor prestatorilor de servicii de încredere calificați.	(c) they ensure the identification of the addressee before the delivery of the data; (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.	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 datelor este indicată printr-o marcă temporală electronică calificată. (2) În cazul datelor transferate între doi sau mai mulți prestatori de servicii de încredere, cerințele de la alin. (1) lit. (a)-(f) se aplică tuturor prestatorilor de servicii de încredere calificați.				
(1a) În cazul în care procesul de trimitere și primire de date îndeplinește standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).	1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications	(4) În cazul în care procesul de trimitere și primire de date îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).		Compatibil		

	and procedures referred to in paragraph 2.					
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru procesele de trimitere și primire de date. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
(2a) Prestatorii de servicii de distribuție electronică înregistrată calificate pot conveni asupra interoperabilității dintre serviciile de distribuție electronică înregistrată calificate pe care le prestează. Un astfel de cadru de interoperabilitate respectă cerințele prevăzute la alineatul (1), iar respectarea acestor cerințe este confirmată de un organism de evaluare a conformității.	2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body.	(3) Prestatorii de servicii de distribuție electronică înregistrată calificate pot conveni asupra interoperabilității dintre serviciile de distribuție electronică înregistrată calificate pe care le prestează. Un astfel de cadru de interoperabilitate respectă cerințele prevăzute la alineatul (1), iar respectarea acestor cerințe este confirmată de un organism de evaluare a conformității.		Compatibil		
(2b) Comisia poate stabili, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru cadrul de interoperabilitate menționat la alineatul (2a) de la	2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative		Compatibil		

prezentul articol. Specificațiile tehnice și conținutul standardelor sunt eficiente din punctul de vedere al costurilor și proporționale. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	necesare punerii în aplicare a prevederilor prezentei legi.				
SECȚIUNEA 8 **Autentificarea unui site internet**	**SECTION 8** **Website authentication**	**Secțiunea a 8-a** **Autentificarea unui site internet**				
Articolul 45 **Cerințe pentru certificatele calificate pentru autentificarea unui site internet**	**Article 45** **Requirements for qualified certificates for website authentication**	**Articolul 50.** **Cerințe pentru certificatele calificate pentru autentificarea unui site internet**				
(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute în anexa IV. Evaluarea conformității cu aceste cerințe se efectuează în conformitate cu standardele, specificațiile și procedurile menționate la alineatul (2) de la prezentul articol.	1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.	(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute la alin. (2).		Compatibil		
(1a) Certificatele calificate pentru autentificarea unui site internet emise în conformitate cu alineatul (1) de la prezentul articol sunt recunoscute de furnizorii de browsere web. Furnizorii de browsere web asigură faptul	1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognised by providers of web-browsers.	(3) Certificatele calificate pentru autentificarea unui site internet emise în conformitate cu alin. (1) sunt recunoscute de furnizorii de browsere web. Furnizorii de browsere web asigură faptul că datele de identitate atestate		Compatibil		

că datele de identitate atestate în certificat și atributele suplimentare atestate sunt afișate într-un mod ușor de recunoscut de către utilizator. Furnizorii de browsere web asigură suport și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1) de la prezentul articol, cu excepția microîntreprinderilor sau a întreprinderilor mici, astfel cum sunt definite la articolul 2 din anexa la Recomandarea 2003/361/CE, în primii cinci ani de funcționare ca prestatori de servicii de navigare pe internet.	Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article, with the exception of microenterprises or small enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC during the first five years of operating as providers of web-browsing services.	în certificat și atributele suplimentare atestate sunt afișate într-un mod ușor de recunoscut de către utilizator. Furnizorii de browsere web asigură suport și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet menționate la alin. (1), cu excepția microîntreprinderilor sau a întreprinderilor mici, astfel cum sunt stabilite prin Legea nr. 179/2016 cu privire la întreprinderile mici şi mijlocii, în primii cinci ani de funcționare ca prestatori de servicii de navigare pe internet.				
(1b) Certificatele calificate pentru autentificarea unui site internet nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alineatul (1).	1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.	(4) Certificatele calificate pentru autentificarea unui site internet nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alin. (2).		Compatibil		
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1) de la prezentul articol. Respectivele acte de	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. Those	(5) În cazul în care un certificat calificat pentru autentificarea unui site internet îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (2).		Compatibil		

punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 45a Măsuri de precauție în materie de securitate cibernetică	**Article 45a Cybersecurity precautionary measures**	**Articolul 51. Măsuri de precauție în materie de securitate cibernetică**				
(1) Furnizorii de browsere web nu iau nicio măsură contrară obligațiilor lor prevăzute la articolul 45, în special cerințelor de recunoaștere a certificatelor calificate pentru autentificarea unui site internet și de afișare a datelor de identitate furnizate într-un mod ușor de recunoscut de către utilizator.	1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication and to display the identity data provided in a user-friendly manner.	(1) Furnizorii de browsere web nu iau nicio măsură contrară obligațiilor lor prevăzute la art. 50, în special cerințelor de recunoaștere a certificatelor calificate pentru autentificarea unui site internet și de afișare a datelor de identitate furnizate într-un mod ușor de recunoscut de către utilizator.		Compatibil		
(2) Prin derogare de la alineatul (1) și numai în cazul unor suspiciuni motivate legate de încălcări ale securității sau de pierderea integrității unui certificat identificat sau a unui set de certificate identificate, furnizorii de browsere web pot lua măsuri de precauție în legătură cu respectivul certificat sau set de certificate.	2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates.	(2) Prin derogare de la alin. (1) și numai în cazul unor suspiciuni motivate legate de încălcări ale securității sau de pierderea integrității unui certificat identificat sau a unui set de certificate identificate, furnizorii de browsere web pot lua măsuri de precauție în legătură cu respectivul certificat sau set de certificate.		Compatibil		
(3) În cazul în care un furnizor de browsere web ia măsuri de precauție conform alineatului (2), furnizorul de browsere web își notifică suspiciunile în scris, fără întârzieri nejustificate,	3. Where a provider of a web-browser takes precautionary measures pursuant to paragraph 2, the provider of the web-browser shall notify its concerns in writing,	(3) În cazul în care un furnizor de browsere web ia măsuri de precauție conform alin. (2), furnizorul de browsere web își notifică suspiciunile în scris, fără întârzieri nejustificate, împreună cu o descriere a		Compatibil		

împreună cu o descriere a măsurilor luate pentru a remedia aceste suspiciuni, Comisiei, organismului de supraveghere competent, entității căreia i-a fost emis certificatul și prestatorului de servicii de încredere calificat care a emis certificatul sau setul de certificate. La primirea unei astfel de notificări, organismul de supraveghere competent emite furnizorului de browsere web în cauză o confirmare de primire.	without undue delay, together with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory body, the entity to whom the certificate was issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question.	măsurilor luate pentru a remedia aceste suspiciuni, organismului de supraveghere, entității căreia i-a fost emis certificatul și prestatorului de servicii de încredere calificat care a emis certificatul sau setul de certificate. La primirea unei astfel de notificări, organismul de supraveghere emite furnizorului de browsere web în cauză o confirmare de primire.				
(4) Organismul de supraveghere competent investighează, în conformitate cu articolul 46b alineatul (4) litera (k), aspectele prezentate în notificare. În cazul în care rezultatul investigației respective nu are ca rezultat retragerea statutului de calificat al certificatului, organismul de supraveghere informează furnizorul de browsere web în consecință și îi solicită acestuia să pună capăt măsurilor de precauție menționate la alineatul (2) de la prezentul articol.	4. The competent supervisory body shall investigate the issues raised in the notification in accordance with Article 46b(4), point (k). Where the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate, the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end to the precautionary measures referred to in paragraph 2 of this Article.	(4) Organismul de supraveghere competent investighează, în conformitate cu art. 64 alin. (3) lit. h), aspectele prezentate în notificare. În cazul în care rezultatul investigației respective nu are ca rezultat retragerea statutului de calificat al certificatului, organismul de supraveghere informează furnizorul de browsere web în consecință și îi solicită acestuia să pună capăt măsurilor de precauție menționate la alin. (2).		Compatibil		
SECȚIUNEA 9	**SECTION 9**	**Secțiunea a 9-a**				

Atestatul electronic al atributelor	**Electronic attestation of attributes**	**Atestatul electronic al atributelor**				
Articolul 45b **Efectele juridice ale atestatului electronic al atributelor**	**Article 45b** **Legal effects of electronic attestation of attributes**	**Articolul 52.** **Efectele juridice ale atestatului electronic al atributelor**				
(1) Unui atestat electronic al atributelor nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele privind atestatele electronice calificate ale atributelor.	1. An electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes.	(1) Unui atestat electronic al atributelor nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele privind atestatele electronice calificate ale atributelor.		Compatibil		
(2) Un atestat electronic calificat al atributelor și atestatele atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism au același efect juridic ca atestatele emise în mod legal în format tipărit.	2. A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.	(2) Un atestat electronic calificat al atributelor și atestatele atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism au același efect juridic ca atestatele emise în mod legal în format tipărit.		Compatibil		
(3) Un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică într-un stat membru sau în numele unui astfel de organism este recunoscut drept un atestat al atributelor emis de un organism din sectorul public în toate statele membre.	3. An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in one Member State shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.	(3) Un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică într-un stat membru al Uniunii Europene sau în numele unui astfel de organism este recunoscut drept un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism în Republica Moldova.		Compatibil		

Articolul 45c Atestatul electronic al atributelor în serviciile publice	**Article 45c Electronic attestation of attributes in public services**	**Articolul 53. Atestatul electronic al atributelor în serviciile publice**				
Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este obligatorie în temeiul dreptului intern pentru a accesa un serviciu prestat online de un organism din sectorul public, datele de identificare personală din atestatul electronic al atributelor nu înlocuiesc identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării pentru identificarea electronică, cu excepția cazului în care acest lucru este permis în mod expres de statul membru. Într-un astfel de caz, se acceptă, de asemenea, atestatul electronic calificat al atributelor din alte state membre.	Where an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.	Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este obligatorie în temeiul dreptului intern pentru a accesa un serviciu prestat online de un organism din sectorul public, datele de identificare personală din atestatul electronic al atributelor nu înlocuiesc identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării pentru identificarea electronică, cu excepția cazului în care acest lucru este permis în mod expres de statul membru. Într-un astfel de caz, se acceptă, de asemenea, atestatul electronic calificat al atributelor din alte state membre.		Compatibil		
Articolul 45d Cerințe privind atestatul electronic calificat al atributelor	**Article 45d Requirements for qualified electronic attestation of attributes**	**Articolul 54. Cerințe privind atestatul electronic calificat al atributelor**				
(1) Atestatul electronic calificat al atributelor îndeplinește cerințele prevăzute în anexa V.	1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V.	(1) Atestatul electronic calificat al atributelor îndeplinește cerințele prevăzute la alin. (2).		Compatibil		
(2) Evaluarea conformității cu cerințele prevăzute în anexa V se efectuează în	2. The evaluation of compliance with the requirements laid down	(5) În cazul în care un atestatul electronic calificat al atributelor îndeplinește		Compatibil		

conformitate cu standardele, specificațiile și procedurile menționate la alineatul (5) de la prezentul articol.	in Annex V shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article.	standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (2).				
(3) Atestatele electronice calificate ale atributelor nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa V.	3. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.	(3) Atestatele electronice calificate ale atributelor nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alin. (2).		Compatibil		
(4) În cazul în care un atestat electronic calificat al atributelor este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se poate reveni în niciun caz la statutul său anterior.	4. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not in any circumstances be reverted.	(4) În cazul în care un atestat electronic calificat al atributelor este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se poate reveni în niciun caz la statutul său anterior.		Compatibil		
(5) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind atestatele electronice calificate ale atributelor. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura	5. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

de examinare menționată la articolul 48 alineatul (2).	shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 45e Verificarea atributelor în raport cu surse autentice	**Article 45e Verification of attributes against authentic sources**	**Articolul 55. Verificarea atributelor în raport cu surse autentice**				
(1) În termen de 24 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la articolul 5a alineatul (23) și la articolul 5c alineatul (6), statele membre se asigură că, cel puțin în cazul atributelor enumerate în anexa VI, ori de câte ori respectivele atribute se bazează pe surse autentice din sectorul public, se iau măsuri pentru a permite prestatorilor de servicii de încredere calificați care pun la dispoziție atestate electronice ale atributelor să verifice respectivele atribute prin mijloace electronice, la cererea utilizatorului, în conformitate cu dreptul Uniunii sau cu dreptul intern.	1. Member States shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c(6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector, measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify those attributes by electronic means at the request of the user, in accordance with Union or national law.	(1) Organismele din sectorul public care gestionează registre de stat sau alte sisteme informaționale ce constituie surse autentice de date asigură, în limitele competențelor și în conformitate cu cadrul normativ aplicabil, disponibilitatea mecanismelor electronice care permit verificarea atributelor persoanelor fizice și juridice de către prestatorii de servicii de încredere calificați ce emit atestate electronice ale atributelor, la cererea expresă a utilizatorului.		Compatibil		
(2) Până la 21 noiembrie 2024, ținând seama de standardele internaționale relevante, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru catalogul de atribute, precum și	2. By 21 November 2024, the Commission shall, taking into account relevant international standards, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		

sisteme pentru atestarea atributelor și procedurile de verificare pentru atestatele electronice calificate ale atributelor în sensul alineatului (1) de la prezentul articol. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală și se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	and procedures for the catalogue of attributes, as well as schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes for the purposes of paragraph 1 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
Articolul 45f Cerințe privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism	**Article 45f Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source**	**Articolul 56. Cerințe privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism**				
(1) Un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește următoarele cerințe: (a) cerințele prevăzute în anexa VII; (b) cerința ca certificatul calificat care stă la baza semnăturii electronice	1. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements: (a) those set out in Annex VII; (b) the qualified certificate supporting the qualified electronic	(1) Un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește următoarele cerințe: 1) cerințele prevăzute la alin. (2); 2) cerința ca certificatul calificat care stă la baza semnăturii electronice		Compatibil		

calificate sau a sigiliului electronic calificat al organismului din sectorul public menționat la articolul 3 punctul 46, identificat drept emitentul menționat la litera (b) din anexa VII, să conțină un set specific de atribute certificate într-o formă adecvată pentru prelucrarea automată, care: (i) indică faptul că organismul emitent este înființat în conformitate cu dreptul Uniunii sau cu dreptul intern ca fiind responsabil de sursa autentică pe baza căreia este emis atestatul electronic al atributelor sau ca organism desemnat să acționeze în numele acestuia; (ii) furnizează un set de date care reprezintă fără ambiguitate sursa autentică menționată la punctul (i); și (iii) identifică dreptul Uniunii sau dreptul intern menționat la punctul (i).	signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and: (i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf; (ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and (iii) identifying the Union or national law referred to in point (i).	calificate sau a sigiliului electronic calificat al organismului din sectorul public să conțină un set specific de atribute certificate într-o formă adecvată pentru prelucrarea automată, care: a) indică faptul că organismul emitent este înființat în conformitate cu cadrul normativ aplicabil ca fiind responsabil de sursa autentică pe baza căreia este emis atestatul electronic al atributelor sau ca organism desemnat să acționeze în numele acestuia; b) furnizează un set de date care reprezintă fără ambiguitate sursa autentică menționată la lit. a); și c) identifică cadrul normativ menționat la lit. a).				
(2) Statul membru în care sunt stabilite organismele din sectorul public menționate la articolul 3 punctul 46 se asigură că organismele din sectorul public care emit atestate electronice ale atributelor au un nivel de fiabilitate și încredere echivalent cu cel al prestatorilor de servicii de încredere calificați, în conformitate cu articolul 24.	2. The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in			Prevederi UE neaplicabile		

	accordance with Article 24.					
(3) Statele membre notifică Comisiei organismele din sectorul public menționate la articolul 3 punctul 46. Notificarea respectivă include un raport de evaluare a conformității emis de un organism de evaluare a conformității care confirmă că sunt îndeplinite cerințele prevăzute la alineatele (1), (2) și (6) de la prezentul articol. Comisia pune la dispoziția publicului, printr-un canal sigur, lista organismelor din sectorul public menționate la articolul 3 punctul 46, într-o formă purtând o semnătură electronică sau un sigiliu electronic, adecvată pentru prelucrarea automată.	3. Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of public sector bodies referred to in Article 3, point (46), in electronically signed or sealed form suitable for automated processing.			Prevederi UE neaplicabile		
(4) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se mai poate reveni la statutul anterior revocării.	4. Where an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted.	(4) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se mai poate reveni la statutul anterior revocării.		Compatibil		
(5) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui	5. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be	(5) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism		Compatibil		

astfel de organism îndeplinește standardele, specificațiile și procedurile menționate la alineatul (6), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).	deemed to be compliant with the requirements laid down in paragraph 1, where it complies with the standards, specifications and procedures referred to in paragraph 6.	îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).				
(6) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
(7) Până la 21 noiembrie 2024, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri în sensul alineatului (3) de la prezentul articol. Actele de punere în aplicare respective	7. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the purposes of paragraph 3	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative				

sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).	necesare punerii în aplicare a prevederilor prezentei legi.				
(8) Organismele din sectorul public menționate la articolul 3 punctul 46 care emit atestate electronice ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu articolul 5a.	8. Public sector bodies referred to in Article 3, point (46), issuing electronic attestation of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance with Article 5a.	(4) Organismele din sectorul public care emit atestate electronice ale atributelor pun la dispoziție o interfață cu portofelele pentru identitatea digitală care sunt furnizate în conformitate cu art. 5.		Compatibil		
Articolul 45g Emiterea atestatului electronic al atributelor pentru portofelele europene pentru identitatea digitală	**Article 45g Issuing of electronic attestation of attributes to European Digital Identity Wallets**	**Articolul 57. Emiterea atestatului electronic al atributelor pentru portofelele pentru identitatea digitală**				
(1) Furnizorii de atestate electronice ale atributelor oferă utilizatorilor portofelului european pentru identitatea digitală posibilitatea de a solicita, de a obține, de a stoca și de a gestiona atestatul electronic al atributelor indiferent de statele membre în care este furnizat portofelul european pentru identitatea digitală.	1. Providers of electronic attestations of attributes shall provide European Digital Identity Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the European Digital Identity Wallet is provided.	(1) Furnizorii de atestate electronice ale atributelor oferă utilizatorilor portofelului pentru identitatea digitală posibilitatea de a solicita, de a obține, de a stoca și de a gestiona atestatul electronic al atributelor prin intermediul oricărui portofel pentru identitatea digitală furnizat în conformitate cu art. 5, fără restricții nejustificate legate de furnizorul portofelului, cu respectarea cerințelor de		Compatibil		

		interoperabilitate, securitate și protecție a datelor stabilite de cadrul normativ aplicabil.				
(2) Furnizorii de atestate electronice calificate ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu articolul 5a.	2. Providers of qualified electronic attestations of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance in Article 5a.	(2) Furnizorii de atestate electronice calificate ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu art. 5.		Compatibil		
Articolul 45h Norme suplimentare privind prestarea serviciilor de atestare electronică a atributelor	**Article 45h Additional rules for the provision of electronic attestation of attributes services**	**Articolul 58. Norme suplimentare privind prestarea serviciilor de atestare electronică a atributelor**				
(1) Prestatorii serviciilor de atestare electronică calificată și necalificată a atributelor nu combină datele cu caracter personal referitoare la prestarea serviciilor respective cu datele cu caracter personal care provin din orice alte servicii oferite de ei sau de partenerii lor comerciali.	1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners.	(1) Prestatorii serviciilor de atestare electronică calificată și necalificată a atributelor nu combină datele cu caracter personal referitoare la prestarea serviciilor respective cu datele cu caracter personal care provin din orice alte servicii oferite de ei sau de partenerii lor comerciali.		Compatibil		
(2) Datele cu caracter personal referitoare la prestarea serviciilor de atestare electronică a atributelor sunt păstrate separate logic de alte date deținute de furnizorul atestatului electronic al atributelor.	2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes.	(2) Datele cu caracter personal referitoare la prestarea serviciilor de atestare electronică a atributelor sunt păstrate separate logic de alte date deținute de furnizorul atestatului electronic al atributelor.		Compatibil		
(3) Prestatorii de servicii de atestare electronică calificată a atributelor pun în aplicare prestarea unor astfel de servicii de încredere calificate într-un mod care este separat din punct de	3. Providers of qualified electronic attestation of attributes' services shall implement the provision of such qualified trust services in a manner that is	(3) Prestatorii de servicii de atestare electronică calificată a atributelor pun în aplicare prestarea unor astfel de servicii de încredere calificate într-un mod care este separat din punct de vedere funcțional		Compatibil		

vedere funcțional de alte servicii pe care le prestează.	functionally separate from other services provided by them.	de alte servicii pe care le prestează.				
SECȚIUNEA 10 **Servicii de arhivare electronică**	**SECTION 10** **Electronic archiving services**	**Secțiunea a 10-a** **Servicii de arhivare electronică**				
Articolul 45i **Efectul juridic al serviciilor de arhivare electronică**	**Article 45i** **Legal effect of electronic archiving services**	**Articolul 59.** **Efectul juridic al serviciilor de arhivare electronică**				
(1) Datelor electronice și documentelor electronice păstrate prin utilizarea unui serviciu de arhivare electronică nu li se refuză efectul juridic sau posibilitatea de a fi acceptate ca probă în procedurile judiciare doar pentru motivul că acestea sunt în format electronic sau că nu sunt păstrate prin utilizarea unui serviciu calificat de arhivare electronică.	1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form or that they are not preserved using a qualified electronic archiving service.	(1) Datelor electronice și documentelor electronice păstrate prin utilizarea unui serviciu de arhivare electronică nu li se refuză efectul juridic sau posibilitatea de a fi acceptate ca probă în procedurile judiciare doar pentru motivul că acestea sunt în format electronic sau că nu sunt păstrate prin utilizarea unui serviciu calificat de arhivare electronică.		Compatibil		
(2) Datele electronice și documentele electronice păstrate prin utilizarea unui serviciu calificat de arhivare electronică beneficiază de prezumția de integritate și de acuratețea originii pe toată durata perioadei de păstrare de către prestatorul de servicii de încredere calificat.	2. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider.	Datele electronice și documentele electronice păstrate prin utilizarea unui serviciu calificat de arhivare electronică beneficiază de prezumția de integritate și de acurateț̦e a originii pe toată durata perioadei de păstrare de către prestatorul de servicii de încredere calificat.		Compatibil		
Articolul 45j **Cerințe privind serviciile calificate de arhivare electronică**	**Article 45j** **Requirements for qualified electronic archiving services**	**Articolul 60.** **Cerințe privind serviciile calificate de arhivare electronică**				

(1) Serviciile calificate de arhivare electronică îndeplinesc următoarele cerințe: (a) sunt prestate de prestatori de servicii de încredere calificați; (b) utilizează proceduri și tehnologii capabile să asigure durabilitatea și lizibilitatea datelor electronice și a documentelor electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținându-le totodată integritatea și acuratețea originii; (c) garantează că respectivele date electronice și documente electronice sunt păstrate astfel încât să fie protejate împotriva pierderii și modificării, cu excepția modificărilor privind suportul lor sau formatul lor electronic; (d) permit beneficiarilor autorizați să primească în mod automat un raport care confirmă faptul că datele electronice și documentele electronice extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate a datelor de la începutul perioadei de păstrare până în momentul extragerii. Raportul menționat la litera (d) de la primul paragraf este furnizat într-un mod fiabil și eficient și poartă semnătura	1. Qualified electronic archive services shall meet the following requirements: (a) they are provided by qualified trust service providers; (b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin; (c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format; (d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the	(1) Serviciile calificate de arhivare electronică îndeplinesc următoarele cerințe: a) sunt prestate de prestatori de servicii de încredere calificați; b) utilizează proceduri și tehnologii capabile să asigure durabilitatea și lizibilitatea datelor electronice și a documentelor electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținându-le totodată integritatea și acuratețea originii; c) garantează că respectivele date electronice și documente electronice sunt păstrate astfel încât să fie protejate împotriva pierderii și modificării, cu excepția modificărilor privind suportul lor sau formatul lor electronic; d) permit beneficiarilor autorizați să primească în mod automat un raport care confirmă faptul că datele electronice și documentele electronice extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate a datelor de la începutul perioadei de păstrare până în momentul extragerii. (2) Raportul menționat la alin. (1) lit. d) este furnizat într-un mod fiabil și eficient și poartă semnătura electronică calificată sau sigiliul electronic calificat al				

electronică calificată sau sigiliul electronic calificat al prestatorului serviciului calificat de arhivare electronică.	preservation period to the moment of retrieval. The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.	prestatorului serviciului calificat de arhivare electronică.				
(2) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind serviciile calificate de arhivare electronică. În cazul în care un serviciu calificat de arhivare electronică îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele privind serviciile calificate de arhivare electronică. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	(3) În cazul în care un serviciu calificat de arhivare electronică îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele privind serviciile calificate de arhivare electronică.		Compatibil		
SECȚIUNEA 11 **Registre electronice**	**SECTION 11** **Electronic ledgers**	**Secțiunea a 11-a** **Registre electronice**				
Articolul 45k	**Article 45k**	**Articolul 61.**				

Efectele juridice ale registrelor electronice	**Legal effects of electronic ledgers**	**Efectele juridice ale registrelor electronice**				
(1) Unui registru electronic nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele pentru registrele electronice calificate.	1. An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.	(1) Unui registru electronic nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele pentru registrele electronice calificate.		Compatibil		
(2) Înregistrările de date cuprinse într-un registru electronic calificat beneficiază de prezumția ordonării lor cronologice secvențiale unice și exacte și de prezumția de integritate.	2. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.	(2) Înregistrările de date cuprinse într-un registru electronic calificat beneficiază de prezumția ordonării lor cronologice secvențiale unice și exacte și de prezumția de integritate.		Compatibil		
Articolul 45l **Cerințe privind registrele electronice calificate**	**Article 45l** **Requirements for qualified electronic ledgers**	**Articolul 62.** **Cerințe privind registrele electronice calificate**				
(1) Registrele electronice calificate îndeplinesc următoarele cerințe: (a) sunt create și gestionate de unul sau mai mulți prestatori de servicii de încredere calificați; (b) stabilesc originea înregistrărilor de date din registru; (c) asigură ordonarea cronologică secvențială unică a înregistrărilor de date din registru; (d) înregistrează datele astfel încât orice modificare a lor ulterioară să poată fi detectată imediat, asigurând integritatea datelor în timp.	1. Qualified electronic ledgers shall meet the following requirements: (a) they are created and managed by one or more qualified trust service providers; (b) they establish the origin of data records in the ledger; (c) they ensure the unique sequential chronological ordering of data records in the ledger; (d) they record data in such a way that any subsequent change to the data is immediately	(1) Registrele electronice calificate îndeplinesc următoarele cerințe: a) sunt create și gestionate de unul sau mai mulți prestatori de servicii de încredere calificați; b) stabilesc originea înregistrărilor de date din registru; c) asigură ordonarea cronologică secvențială unică a înregistrărilor de date din registru; d) înregistrează datele astfel încât orice modificare a lor ulterioară să poată fi		Compatibil		

	detectable, ensuring their integrity over time.	detectată imediat, asigurând integritatea datelor în timp.				
(2) În cazul în care registrul electronic îndeplinește standardele, specificațiile și procedurile menționate la alineatul (3), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).	2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger complies with the standards, specifications and procedures referred to in paragraph 3.	(2) În cazul în care registrul electronic îndeplinește standardele, specificațiile și procedurile stabilite de Guvern, se prezumă că sunt respectate cerințele prevăzute la alin. (1).		Compatibil		
(3) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
CAPITOLUL IV **DOCUMENTE ELECTRONICE**	**CHAPTER IV** **ELECTRONIC DOCUMENTS**	**Capitolul IV** **DOCUMENTE ELECTRONICE**				
Articolul 46 **Efectele juridice ale documentelor electronice**	**Article 46** **Legal effects of electronic documents**	**Articolul 63.** **Efectele juridice ale documentelor electronice**				
		(1) Documentul electronic semnat cu semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat este asimilat, după efectele acestuia, cu documentul similar pe suport de hârtie, semnat cu semnătură olografă.		Compatibil		

		(2) Documentul electronic emis de către o autoritate sau o instituţie publică sau de către o persoană în exercitarea şi în limitele atribuţiilor sale de putere publică, semnat cu o semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat este asimilat unui înscris autentic.		Compatibil		
		(3)Documentul electronic semnat cu un tip de semnătură electronică diferit de semnătura electronică calificată produce efecte juridice echivalente cu cele ale documentului similar pe suport de hârtie semnat olograf doar în cazurile prevăzute expres de actele normative sau atunci când părţile au convenit în mod explicit utilizarea semnăturilor electronice, printr-un înscris distinct semnat olograf sau cu semnătură electronică calificată.		Compatibil		
		(4) Actele normative sau acordul părților privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaștere a documentelor electronice, semnate cu alt tip de semnătură electronică decât cea calificată, asimilate, după efectele lor, cu documente similare pe suport de hârtie, semnate cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum și obligațiile părților		Compatibil		

		privind confidențialitatea și răspunderea materială.				
		(5)În cazul în care, conform legislației, se cere ca documentul să fie perfectat sau prezentat pe suport de hârtie și semnat cu semnătură olografă, documentul electronic se consideră corespunzător cerințelor respective.		Compatibil		
		(6) În cazul în care, conform legislației, se cere ca documentul pe suport de hârtie să fie autentificat cu ștampilă, documentul electronic se consideră a fi corespunzător cerinței respective.				
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.	An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form.	(7) 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.		Compatibil		
CAPITOLUL IVa CADRUL DE GUVERNANȚĂ	**CHAPTER IVa GOVERNANCE FRAMEWORK**	**Capitolul V CADRUL DE GUVERNANȚĂ**				
Articolul 46a Supravegherea cadrului pentru portofelul european pentru identitatea digitală	**Article 46a Supervision of the European Digital Identity Wallet Framework**	**Articolul 64. Supravegherea cadrului pentru portofelul european pentru identitatea digitală și a serviciilor de încredere**				
(1) Statele membre desemnează unul sau mai multe organisme de supraveghere stabilite pe teritoriul lor. Organismelor de supraveghere desemnate în temeiul primului paragraf li se conferă competențele necesare și resursele adecvate pentru a-și	1. Member States shall designate one or more supervisory bodies established in their territory. The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for	(1) Organismul de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere este Serviciul de Informații și Securitate al Republicii Moldova.		Compatibil		

îndeplini sarcinile în mod eficace, eficient și independent.	the exercise of their tasks in an effective, efficient and independent manner.					
(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate în temeiul alineatului (1), precum și orice modificări ulterioare ale acestora. Comisia publică o listă a organismelor de supraveghere notificate.	2. Member States shall notify to the Commission the names and the addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.			Prevederi UE neaplicabile		
(3) Rolul organismelor de supraveghere desemnate în temeiul alineatului (1) constă în: (a) supravegherea furnizorilor de portofele europene pentru identitatea digitală stabiliți pe teritoriul statului membru care a desemnat organismele de supraveghere și asigurarea, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii furnizori și de către portofelele europene pentru identitatea digitală furnizate de aceștia a cerințelor stabilite în prezentul regulament; (b) a lua măsuri, dacă este necesar, în ceea ce îi privește pe furnizorii de portofele europene pentru identitatea digitală stabiliți pe teritoriul statului membru care a desemnat organismele de supraveghere, prin	3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be: (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, by means of ex ante and ex post supervisory activities, that those providers and European Digital Identity Wallets they provide meet the requirements laid down in this Regulation; (b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, by means of ex post supervisory activities, when	(2) Rolul organismului de supraveghere desemnate în temeiul alin. (1) constă în: a) supravegherea furnizorilor de portofele pentru identitatea digitală cu sediul în Republica Moldova, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii furnizori și de către portofelele pentru identitatea digitală furnizate de aceștia a cerințelor stabilite de prezenta lege; c) a lua măsuri, dacă este necesar, în ceea ce îi privește pe furnizorii de portofele pentru identitatea digitală cu sediul în Republica Moldova, prin intermediul unor activități de supraveghere ex post, atunci când sunt informate că furnizorii sau portofelele pentru identitatea digitală furnizate de aceștia încalcă prezenta lege;		Compatibil		

intermediul unor activități de supraveghere ex post, atunci când sunt informate că furnizorii sau portofelele europene pentru identitatea digitală furnizate de aceștia încalcă prezentul regulament.	informed that providers or European Digital Identity Wallets that they provide infringe this Regulation.					
(4) Printre sarcinile organismelor de supraveghere desemnate în temeiul alineatului (1) se numără, în special, următoarele: (a) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolele 46c și 46e; (b) să solicite informațiile necesare pentru monitorizarea conformității cu prezentul regulament; (c) să informeze autoritățile competente relevante ale statelor membre în cauză, desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cu privire la orice încălcare semnificativă a securității sau pierdere a integrității de care iau cunoștință în îndeplinirea sarcinilor lor și, în cazul unei încălcări semnificative a securității sau al pierderii integrității care privește alte state membre, să informeze punctul unic de contact din statul membru în cauză, desemnat sau înființat în temeiul articolului 8 alineatul (3) din Directiva	4. The tasks of the supervisory bodies designated pursuant to paragraph 1 shall include, in particular, the following: (a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e; (b) to request information necessary to monitor compliance with this Regulation; (c) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breaches or loss of integrity of which they become aware in the performance of their tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to	(3) În îndeplinirea rolului prevăzut la alin. (2), organismul de supraveghere: 1) în domeniul cadrului pentru portofelul european pentru identitatea digitală: a) solicită furnizorilor de portofele pentru identitatea digitală să remedieze orice încălcare a cerințelor prevăzute de prezenta lege; b) suspendă sau anulează înregistrarea și includerea beneficiarilor în mecanismul menționat la art. 6 în cazul utilizării ilegale sau frauduloase a portofelului pentru identitatea digitală; c) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal; d) realizează activități de verificare a furnizorilor de portofele pentru identitatea digitală;		Compatibil		

(UE) 2022/2555, și punctele unice de contact din celelalte state membre în cauză, desemnate în temeiul articolului 46c alineatul (1) din prezentul regulament, și să informeze publicul sau să solicite furnizorilor de portofele europene pentru identitatea digitală să facă acest lucru în cazul în care organismul de supraveghere consideră că divulgarea încălcării securității sau a pierderii integrității ar fi de interes public; (d) să efectueze inspecții la fața locului și supraveghere ex situ; (e) să solicite furnizorilor de portofele europene pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament; (f) să suspende sau să anuleze înregistrarea și includerea beneficiarilor în mecanismul menționat la articolul 5b alineatul (7) în cazul utilizării ilegale sau frauduloase a portofelului european pentru identitatea digitală; (g) să coopereze cu autoritățile de supraveghere competente înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679, în special prin informarea acestora, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu	Article 8(3) of Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require providers of European Digital Identity Wallet to do so where the supervisory body determines that disclosure of the security breach or of the loss of integrity would be in the public interest; (d) to carry out on-site inspections and off-site supervision; (e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation; (f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 5b(7) in the case of illegal or fraudulent use of the European Digital Identity Wallet; (g) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular,	e) solicită informațiile necesare pentru monitorizarea conformității cu prezentat lege.				

caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal.	by informing them without undue delay, where personal data protection rules appear to have been infringed and about security breaches which appear to constitute personal data breaches.					
(5) În cazul în care organismul de supraveghere desemnat în temeiul alineatului (1) solicită furnizorului unui portofel european pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament în temeiul alineatului (4) litera (e), iar furnizorul respectiv nu acționează în consecință și, dacă este cazul, într-un termen stabilit de organismul de supraveghere, organismul de supraveghere desemnat în temeiul alineatului (1) poate, ținând seama, în special, de amploarea, durata și consecințele respectivei neîndepliniri, să dispună ca furnizorul să suspende sau să înceteze furnizarea portofelului european pentru identitatea digitală. Organismul de supraveghere informează fără întârzieri nejustificate organismele de supraveghere ale altor state membre, Comisia, beneficiarii și utilizatorii portofelului european pentru identitatea digitală cu privire la decizia de a solicita	5. Where the supervisory body designated pursuant to paragraph 1 requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to paragraph 4, point (e), and that provider does not act accordingly and, if applicable, within a time limit set by that supervisory body, the supervisory body designated pursuant to paragraph 1 may, taking into account, in particular, the extent, duration and consequences of that failure, order the provider to suspend or to cease the provision of the European Digital Identity Wallet. The supervisory body shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the	(4) În cazul în care organismul de supraveghere, în temeiul alin. (4) pct. 1) lit. a), solicită furnizorului unui portofel pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute de lege, iar furnizorul nu ia măsurile corespunzătoare, organismul de supraveghere poate dispune, ținând seama, în special, de amploarea, durata și consecințele respectivei neîndepliniri, suspendarea sau încetarea furnizării portofelului pentru identitatea digitală. (5) Organismul de supraveghere informează fără întârzieri nejustificate beneficiarii și utilizatorii portofelului pentru identitatea digitală cu privire la decizia de suspendare sau încetare a furnizării acestuia.		Compatibil		

suspendarea sau încetarea furnizării portofelului european pentru identitatea digitală.	decision to require the suspension or cessation of the provision of the European Digital Identity Wallet.					
(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere desemnat în temeiul alineatului (1) prezintă Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior. Comisia pune la dispoziția Parlamentului European și a Consiliului rapoartele anuale respective.	6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.	(6) Organismul de supraveghere transmite Parlamentului Republicii Moldova, până la 31 martie a fiecărui an, un raport cu privire la principalele activități desfășurate în anul calendaristic anterior în domeniul portofelului european pentru identitatea digitală și al serviciilor de încredere.		Compatibil		
(7) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile privind raportul menționat la alineatul (6) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.		Compatibil		
Articolul 46b Supravegherea serviciilor de încredere	**Article 46b Supervision of trust services**	**Articolul 65. Supravegherea cadrului pentru portofelul european pentru identitatea digitală și a serviciilor de încredere**				
(1) Statele membre desemnează un organism de supraveghere înființat pe teritoriul lor sau desemnează, de comun acord cu un alt stat membru, un organism de	1. Member States shall designate a supervisory body established in their territory or designate, upon mutual agreement with another Member State, a supervisory	(1) Organismul de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere este Serviciul de Informații și Securitate al Republicii Moldova.		Compatibil		

supraveghere înființat în acel alt stat membru. Organismul de supraveghere respectiv este responsabil de sarcinile de supraveghere în statul membru care l-a desemnat în ceea ce privește serviciile de încredere. Organismelor de supraveghere desemnate în temeiul primului paragraf li se acordă competențele necesare și resursele adecvate pentru a-și îndeplini sarcinile.	body established in that other Member State. That supervisory body shall be responsible for supervisory tasks in the designating Member State as regards trust services. The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks.					
(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate în temeiul alineatului (1), precum și orice modificări ulterioare ale acestora. Comisia publică o listă a organismelor de supraveghere notificate.	2. Member States shall notify to the Commission the names and addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.			Prevederi UE neaplicabile		
(3) Rolul organismelor de supraveghere desemnate în temeiul alineatului (1) constă în: (a) supravegherea prestatorilor de servicii de încredere calificați stabiliți pe teritoriul statului membru care le-a desemnat și asigurarea, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii prestatori de servicii de încredere calificați și de către	3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be: (a) to supervise qualified trust service providers established in the territory of the designating Member State and to ensure, by means of ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services	(2) Rolul organismului de supraveghere desemnate în temeiul alin. (1) constă în: b) supravegherea prestatorilor de servicii de încredere calificați cu sediul în Republicii Moldova, prin intermediul unor activități de supraveghere ex ante și ex post, îndeplinirii de către respectivii prestatori de servicii de încredere calificați și de către serviciile de încredere calificate prestate de aceștia a cerințelor stabilite în prezenta lege;		Compatibil		

serviciile de încredere calificate prestate de aceștia a cerințelor 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 le-a desemnat, prin intermediul activităților de supraveghere ex post, atunci când sunt informate că respectivii prestatori de servicii de încredere necalificați sau serviciile de încredere prestate de aceștia nu ar îndeplini cerințele stabilite în prezentul regulament.	that they provide meet the requirements laid down in this Regulation; (b) to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, by means of ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.	d) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați cu sediul în Republica Moldova, prin intermediul activităților de supraveghere ex post, atunci când sunt informate că respectivii prestatori de servicii de încredere necalificați sau serviciile de încredere prestate de aceștia nu ar îndeplini cerințele stabilite de prezenta lege.				
(4) Printre sarcinile organismelor de supraveghere desemnate în temeiul alineatului (1) se numără, în special, următoarele: (a) să informeze autoritățile competente relevante ale statelor membre în cauză, desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cu privire la orice încălcare semnificativă a securității sau pierdere a integrității de care iau cunoștință în îndeplinirea sarcinilor lor și, în cazul unei încălcări semnificative a securității sau al pierderii integrității care privește alte state membre, să informeze punctul unic de contact din statul membru în cauză,	4. The tasks of the supervisory body designated pursuant to paragraph 1 shall include in particular the following: (a) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point	(3) În îndeplinirea rolului prevăzut la alin. (2), organismul de supraveghere: 2) în domeniul serviciilor de încredere: a) analizează rapoartele de evaluare a conformității menționate la art. 21 alin. (1) și la art. 22 alin. (1); b) realizează audituri sau solicită unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați, în conformitate cu art. 21 alin. (3); c) acordă sau retrage statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează;		Compatibil		

desemnat sau înființat în temeiul articolului 8 alineatul (3) din Directiva (UE) 2022/2555, și punctele unice de contact din celelalte state membre în cauză, desemnate în temeiul articolului 46c alineatul (1) din prezentul regulament, și să informeze publicul sau să solicite prestatorului de servicii de încredere să facă acest lucru în cazul în care organismul de supraveghere consideră că divulgarea încălcării securității sau a pierderii integrității ar fi de interes public; (b) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolele 46c și 46e; (c) să analizeze rapoartele de evaluare a conformității menționate la articolul 20 alineatul (1) și la articolul 21 alineatul (1); (d) să raporteze Comisiei cu privire la activitățile sale principale, în conformitate cu alineatul (6) de la prezentul articol; (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); (f) să coopereze cu autoritățile de supraveghere competente înființate în temeiul articolului 51 din	of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require the trust service provider to do so where the supervisory body determines that disclosure of the breach of security or loss of integrity would be in the public interest; (b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e; (c) to analyse the conformity assessment reports referred to in Article 20(1) and Article 21(1); (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article; (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service	d) asigură că prestatorii de servicii de încredere calificate cu sediul în Republica Moldova și serviciile de încredere calificate pe care aceştia le prestează îndeplinesc cerințele stabilite de prezenta lege; e) solicită prestatorilor de servicii de încredere să remedieze încălcările cerințelor prevăzute de prezenta lege; f) verifică existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului atunci când prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate cu art. 24 alin. (4) pct. 10); g) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal; h) investighează cererile formulate de furnizorii de browsere web în temeiul art. 51 și să ia măsuri, dacă este necesar.				

Regulamentul (UE) 2016/679, în special prin informarea acestora, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal; (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; (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 desemnat în temeiul alineatului (1) de la prezentul articol; (i) să verifice existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului atunci când prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate	providers in accordance with Article 20(2); (f) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them, without undue delay, where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches; (g) to grant qualified status to trust service providers and to the services they provide, and to withdraw that status in accordance with Articles 20 and 21; (h) to inform the body responsible for the national trusted list referred to in Article 22(3) of its decisions to grant or withdraw qualified status, unless that body is also the supervisory body designated pursuant to paragraph 1 of this Article; (i) to verify the existence and correct application of provisions on termination plans where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance					

cu articolul 24 alineatul (2) litera (h); (j) să solicite prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament; (k) să investigheze cererile formulate de furnizorii de browsere web în temeiul articolului 45a și să ia măsuri, dacă este necesar.	with Article 24(2), point (h); (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation; (k) to investigate claims made by providers of web-browsers pursuant to Article 45a and to take action if necessary.					
(5) Statele membre pot să solicite organismului de supraveghere desemnat în temeiul alineatului (1) să stabilească, să mențină și să actualizeze o infrastructură de asigurare a încrederii în conformitate cu dreptul intern.	5. Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law.			Compatibil		
(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere desemnat în temeiul alineatului (1) prezintă Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior. Comisia pune la dispoziția Parlamentului European și a Consiliului rapoartele anuale respective.	6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.	(6) Organismul de supraveghere transmite Parlamentului Republicii Moldova, până la 31 martie a fiecărui an, un raport cu privire la principalele activități desfășurate în anul calendaristic anterior în domeniul portofelului european pentru identitatea digitală și al serviciilor de încredere.		Compatibil		
(7) Până la 21 mai 2025, Comisia adoptă orientări privind îndeplinirea de către organismele de supraveghere desemnate în temeiul alineatului (1) de la prezentul articol a sarcinilor	7. By 21 May 2025, the Commission shall adopt guidelines on the exercise by the supervisory bodies designated pursuant to paragraph 1 of this	Articolul 69. Dispoziții finale (2)Guvernul, până la intrarea în vigoare a prezentei legi: c)în termen de 18 luni de la data publicării prezentei legi, va aduce actele sale normative în concordanță cu prezenta		Compatibil		

menționate la alineatul (4) de la prezentul articol și, prin intermediul unor acte de punere în aplicare, stabilește formatele și procedurile privind raportul menționat la alineatul (6) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	Article of the tasks referred to in paragraph 4 of this Article, and, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.				
Articolul 46c Puncte unice de contact	**Article 46c Single points of contact**	**Articolul 64. Punct unic de contact**				
(1) Fiecare stat membru desemnează un punct unic de contact pentru serviciile de încredere, portofelele europene pentru identitatea digitală și sistemele de identificare electronică notificate.	1. Each Member State shall designate a single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes.	Organismul de supraveghere acționează ca punct unic de contact pentru serviciile de încredere, portofelele pentru identitatea digitală și sistemele de identificare electronică, în relațiile cu autoritățile competente din alte state și cu organizațiile internaționale relevante.		Compatibil		
(2) Fiecare punct unic de contact exercită o funcție de legătură pentru a facilita cooperarea transfrontalieră între organismele de supraveghere pentru prestatorii de servicii de încredere și între organismele de supraveghere pentru furnizorii de portofele europene pentru identitatea digitală și, după caz, cu Comisia și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu alte autorități competente din statul său membru.	2. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other			Compatibil		

	competent authorities within its Member State.					
(3) Fiecare stat membru publică și, fără întârzieri nejustificate, notifică Comisiei denumirea și adresa punctului unic de contact desemnat în temeiul alineatului (1), precum și orice modificare ulterioară a acestora.	3. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the single point of contact designated pursuant to paragraph 1 and any subsequent change thereto.			Prevederi UE neaplicabile		
(4) Comisia publică o listă a punctelor unice de contact notificate în temeiul alineatului (3).	4. The Commission shall publish a list of the single points of contact notified pursuant to paragraph 3.			Prevederi UE neaplicabile		
Articolul 46d **Asistență reciprocă**	**Article 46d** **Mutual assistance**					
(1) Pentru a facilita supravegherea și executarea obligațiilor prevăzute de prezentul regulament, organismele de supraveghere desemnate în temeiul articolului 46a alineatul (1) sau al articolului 46b alineatul (1) pot solicita, inclusiv prin intermediul grupului de cooperare înființat în temeiul articolului 46e alineatul (1), asistență reciprocă din partea organismelor de supraveghere dintr-un alt stat membru în care este stabilit furnizorul portofelului european pentru identitatea digitală sau prestatorul de servicii de încredere sau în care se află rețeaua și sistemele sale	1. In order to facilitate the supervision and enforcement of obligations under this Regulation, the supervisory bodies designated pursuant to Article 46a(1) and Article 46b(1) may seek, including through the Cooperation Group established pursuant to Article 46e(1), mutual assistance from the supervisory bodies of another Member State where the provider of the European Digital Identity Wallet or the trust service provider is established, or where its network and information systems are located or its services are provided.			Prevederi UE neaplicabile		

informatice ori sunt prestate serviciile acestuia.						
(2) Asistența reciprocă implică cel puțin faptul că: (a) organismul de supraveghere care aplică măsuri de supraveghere și de executare într-un stat membru informează și consultă organismul de supraveghere din celălalt stat membru în cauză; (b) un organism de supraveghere poate solicita organismului de supraveghere dintr-un alt stat membru în cauză să ia măsuri de supraveghere sau de executare, inclusiv, de exemplu, cereri de a efectua inspecții legate de rapoartele de evaluare a conformității menționate la articolele 20 și 21 în ceea ce privește prestarea de servicii de încredere; (c) după caz, organismele de supraveghere pot efectua anchete comune cu organismele de supraveghere din alte state membre. Mecanismele și procedurile pentru acțiunile comune menționate la primul paragraf sunt convenite și stabilite de către statele membre în cauză, în conformitate cu dreptul lor intern.	2. The mutual assistance shall at least entail that: (a) the supervisory body applying supervisory and enforcement measures in one Member State shall inform and consult the supervisory body from the other Member State concerned; (b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance, requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services; (c) where appropriate, supervisory bodies may carry out joint investigations with the supervisory bodies of other Member States. The arrangements and procedures for joint actions under the first subparagraph shall be agreed upon and established by the Member States concerned in accordance with their national law.			Prevederi UE neaplicabile		

(3) Un organism de supraveghere căruia i se adresează o solicitare de asistență poate respinge respectiva solicitare pentru oricare dintre următoarele motive: (a) asistența solicitată nu este proporțională cu activitățile de supraveghere ale organismului de supraveghere desfășurate în conformitate cu articolele 46a și 46b; (b) organismul de supraveghere nu are competența de a acorda asistența solicitată; (c) acordarea asistenței solicitate ar contraveni prezentului regulament.	3. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds: (a) the assistance requested is not proportionate to the supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b; (b) the supervisory body is not competent to provide the requested assistance; (c) providing the requested assistance would be incompatible with this Regulation.			Prevederi UE neaplicabile		
(4) Până la 21 mai 2025 și, ulterior, la fiecare doi ani, grupul de cooperare înființat în temeiul articolului 46e alineatul (1) emite orientări privind aspectele organizatorice și procedurile pentru asistența reciprocă menționată la alineatele (1) și (2) de la prezentul articol.	4. By 21 May 2025 and every two years thereafter, the Cooperation Group established pursuant to Article 46e(1) shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2 of this Article.			Prevederi UE neaplicabile		
Articolul 46e Grupul european de cooperare privind identitatea digitală	**Article 46e The European Digital Identity Cooperation Group**					
(1) Pentru a sprijini și a facilita cooperarea transfrontalieră și schimbul de informații dintre statele membre privind serviciile de încredere, portofelele	1. In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services,			Prevederi UE neaplicabile		

europene pentru identitatea digitală și sistemele de identificare electronică notificate, Comisia înființează un Grup european de cooperare privind identitatea digitală (denumit în continuare „grupul de cooperare”).	European Digital Identity Wallets and notified electronic identification schemes, the Commission shall establish a European Digital Identity Cooperation Group (the ‘Cooperation Group’).					
(2) Grupul de cooperare este alcătuit din reprezentanți numiți de statele membre și de Comisie. Grupul de cooperare este prezidat de Comisie. Comisia asigură secretariatul grupului de cooperare.	2. The Cooperation Group shall be composed of representatives appointed by the Member States and of the Commission. The Cooperation Group shall be chaired by the Commission. The Commission shall provide the Cooperation Group’s Secretariat.			Prevederi UE neaplicabile		
(3) Reprezentanții părților interesate relevante pot fi invitați ad-hoc să participe la reuniunile grupului de cooperare și la lucrările acestuia în calitate de observatori.	3. Representatives of relevant stakeholders may, on an ad hoc basis, be invited to attend meetings of the Cooperation Group and to participate in its work as observers.			Prevederi UE neaplicabile		
(4) ENISA este invitată să participe în calitate de observator la lucrările grupului de cooperare atunci când are loc un schimb de opinii, de bune practici și de informații cu privire la aspecte relevante în materie de securitate cibernetică, cum ar fi notificarea încălcărilor securității, și atunci când se abordează utilizarea certificatelor sau a	4. ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity			Prevederi UE neaplicabile		

standardelor de securitate cibernetică.	certificates or standards are addressed.					
(5) Grupului de cooperare îi revin următoarele sarcini: (a) să facă schimb de opinii și să coopereze cu Comisia cu privire la inițiativele de politică emergente în domeniul portofelelor pentru identitatea digitală, al mijloacelor de identificare electronică și al serviciilor de încredere; (b) să consilieze Comisia, după caz, în fazele inițiale de pregătire a proiectelor de acte de punere în aplicare și de acte delegate care urmează să fie adoptate în temeiul prezentului regulament; (c) pentru a sprijini organismele de supraveghere la punerea în aplicare a dispozițiilor prezentului regulament: (i) să facă schimb de bune practici și de informații privind punerea în aplicare a dispozițiilor prezentului regulament; (ii) să evalueze evoluțiile pertinente din sectorul portofelului pentru identitatea digitală, al identificării electronice și al serviciilor de încredere; (iii) să organizeze reuniuni comune cu părțile interesate relevante din întreaga Uniune pentru a discuta activitățile desfășurate de grupul de cooperare și pentru a colecta informații cu privire la dificultățile	5. The Cooperation Group shall have the following tasks: (a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services; (b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation; (c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation: (i) exchange best practices and information regarding the implementation of the provisions of this Regulation; (ii) assess the relevant developments in the digital identity wallet, electronic identification and trust services sectors; (iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation			Prevederi UE neaplicabile		

emergente în materie de politici; (iv) cu sprijinul ENISA, să facă schimb de opinii, de bune practici și de informații cu privire la aspectele relevante în materie de securitate cibernetică în ceea ce privește portofelele europene pentru identitatea digitală, sistemele de identificare electronică și serviciile de încredere; (v) să facă schimb de bune practici cu privire la elaborarea și punerea în aplicare a politicilor privind notificarea încălcărilor securității și măsurile comune menționate la articolele 5e și 10; (vi) să organizeze reuniuni comune cu Grupul de cooperare NIS înființat în temeiul articolului 14 alineatul (1) din Directiva (UE) 2022/2555 pentru a face schimb de informații relevante în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, capacitățile în materie de standarde și specificații tehnice, precum și standardele și specificațiile tehnice în legătură cu serviciile de încredere și identificarea electronică; (vii) să discute, la cererea unui organism de supraveghere, cererile	group and gather input on emerging policy challenges; (iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services; (v) exchange best practices in relation to the development and implementation of policies on the notification of security breaches, and common measures as referred to in Articles 5e and 10; (vi) organise joint meetings with the NIS Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications; (vii) discuss, upon a request of a supervisory					

specifice de asistență reciprocă menționate la articolul 46d; (viii) să faciliteze schimbul de informații între organismele de supraveghere prin furnizarea de orientări cu privire la aspectele organizatorice și procedurile de asistență reciprocă menționate la articolul 46d; (d) să organizeze evaluări inter pares ale sistemelor de identificare electronică ce trebuie notificate în temeiul prezentului regulament.	body, specific requests for mutual assistance as referred to in Article 46d; (viii) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d; (d) organise peer reviews of electronic identification schemes to be notified under this Regulation.					
(6) Statele membre asigură cooperarea eficace și eficientă a reprezentanților lor desemnați în grupul de cooperare.	6. Member States shall ensure effective and efficient cooperation of their designated representatives in the Cooperation Group.			Prevederi UE neaplicabile		
(7) Până la 21 mai 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, modalitățile procedurale necesare pentru facilitarea cooperării dintre statele membre menționate la alineatul (5) litera (d) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraph 5, point (d), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			Prevederi UE neaplicabile		
CAPITOLUL V	**CHAPTER V**					

DELEGAREA DE COMPETENȚE ȘI MĂSURI DE PUNERE ÎN APLICARE	**DELEGATION OF POWERS AND IMPLEMENTING MEASURES**					
Articolul 47 **Exercitarea delegării**	**Article 47** **Exercise of the delegation**					
(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	
(2) Competența de a adopta acte delegate menționată la articolul 5c alineatul (8), la articolul 24 alineatul (4b) și la articolul 30 alineatul (4) se conferă Comisiei pe o perioadă nedeterminată de la 17 septembrie 2014.	2. The power to adopt delegated acts referred to in Article 5c(8), Article 24(4b) and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	
(3) Delegarea de competențe menționată la articolul 5c alineatul (8), la articolul 24 alineatul (4b) și la articolul 30 alineatul (4) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.	3. The delegation of power referred to in Article 5c(8), Article 24(4b) and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	

	any delegated acts already in force.					
(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.	4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	
(5) Un act delegat adoptat în temeiul articolului 5c alineatul (8), al articolului 24 alineatul (4b) sau al articolului 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 acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.	5. A delegated act adopted pursuant to Article 5c(8), Article 24(4b) or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	
Articolul 48 **Procedura comitetului**	**Article 48** **Committee procedure**					
(1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii Europene	
(2) În cazul în care se face trimitere la prezentul alineat,	2. Where reference is made to this paragraph,			Prevederi UE neaplicabile	Normă adresată instituțiilor Uniunii	

se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.	Article 5 of Regulation (EU) No 182/2011 shall apply.				Europene	
CAPITOLUL VI DISPOZIȚII FINALE	**CHAPTER VI FINAL PROVISIONS**					
Articolul 48a Cerințe de raportare	**Article 48a Reporting requirements**	**Articolul 66. Cerințe de raportare**				
(1) Statele membre asigură colectarea de date statistice în legătură cu funcționarea portofelelor europene pentru identitatea digitală și a serviciilor de încredere calificate furnizate pe teritoriile lor.	1. Member States shall ensure the collection of statistics in relation to the functioning of European Digital Identity Wallets and the qualified trust services provided on their territory.	(1) Organismul de supraveghere asigură colectarea de date statistice în legătură cu funcționarea portofelelor pentru identitatea digitală și a serviciilor de încredere calificate furnizate pe teritoriul Republicii Moldova.		Compatibil		
(2) Datele statistice colectate în conformitate cu alineatul (1) includ următoarele: (a) numărul persoanelor fizice și juridice care dețin un portofel european pentru identitatea digitală valabil; (b) tipul și numărul serviciilor care acceptă utilizarea portofelului european pentru identitatea digitală; (c) numărul reclamațiilor din partea utilizatorilor și al incidentelor privind protecția consumatorilor sau protecția datelor în legătură cu beneficiarii și serviciile de încredere calificate; (d) un raport de sinteză care include date privind incidentele care împiedică utilizarea portofelului	2. The statistics collected in accordance with paragraph 1 shall include the following: (a) the number of natural and legal persons having a valid European Digital Identity Wallet; (b) the type and number of services accepting the use of the European Digital Identity Wallet; (c) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services; (d) a summary report including data on incidents preventing the	(2) Datele statistice colectate în conformitate cu alin. (1) includ următoarele: (a) numărul persoanelor fizice și juridice care dețin un portofel pentru identitatea digitală valabil; (b) tipul și numărul serviciilor care acceptă utilizarea portofelului pentru identitatea digitală; (c) numărul reclamațiilor din partea utilizatorilor și al incidentelor privind protecția consumatorilor sau protecția datelor în legătură cu beneficiarii și serviciile de încredere calificate; (d) un raport de sinteză care include date privind incidentele care împiedică utilizarea portofelului european pentru identitatea digitală;		Compatibil		

european pentru identitatea digitală; (e) un rezumat al incidentelor semnificative de securitate, al încălcărilor securității datelor și al utilizatorilor afectați ai portofelelor europene pentru identitatea digitală sau ai serviciilor de încredere calificate.	use of the European Digital Identity Wallet; (e) a summary of significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services.	(e) un rezumat al incidentelor semnificative de securitate, al încălcărilor securității datelor și al utilizatorilor afectați ai portofelelor europene pentru identitatea digitală sau ai serviciilor de încredere calificate.				
(3) Datele statistice menționate la alineatul (2) sunt puse la dispoziția publicului într-un format deschis, utilizat în mod obișnuit și prelucrabil automat.	3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.	(3) Datele statistice menționate la alin. (2) sunt puse la dispoziția publicului într-un format deschis, utilizat în mod obișnuit și prelucrabil automat.		Compatibil		
(4) Până la data de 31 martie a fiecărui an, statele membre transmit Comisiei un raport privind datele statistice colectate în conformitate cu alineatul (2).	4. By 31 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.			Prevederi UE neaplicabile		
Articolul 49 **Reexaminare**	**Article 49** **Review**					
(1) Comisia reexaminează modul de aplicare a prezentului regulament și, până la 21 mai 2026, prezintă un raport în acest sens Parlamentului European și Consiliului. În respectivul raport, Comisia evaluează, în special, dacă este oportun să se modifice domeniul de aplicare al prezentului regulament sau dispozițiile sale specifice, inclusiv, în special, dispozițiile articolului 5c	1. The Commission shall review the application of this Regulation and shall, by 21 May 2026, submit a report to the European Parliament and to the Council. In that report, the Commission shall, in particular, evaluate whether it is appropriate to modify the scope of this Regulation or its specific provisions including, in particular,			Prevederi UE neaplicabile		

alineatul (5), ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, ale pieței și juridice. Dacă este necesar, raportul respectiv este însoțit de o propunere de modificare a prezentului regulament.	the provisions included in Article 5c(5), taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal to amend this Regulation.					
(2) Raportul menționat la alineatul (1) include o analiză a disponibilității, a securității și a posibilității de utilizare a mijloacelor de identificare electronică notificate și a portofelelor europene pentru identitatea digitală care intră în domeniul de aplicare al prezentului regulament și analizează dacă tuturor prestatorilor privați de servicii online care recurg la servicii de identificare electronică furnizate de terți pentru autentificarea utilizatorilor trebuie să le revină obligația să accepte utilizarea mijloacelor de identificare electronică notificate și a portofelului european pentru identitatea digitală.	2. The report referred to in paragraph 1 shall include an assessment of the availability, security and usability of the notified electronic identification means and European Digital Identity Wallets that fall within the scope of this Regulation and assess whether all online private service providers relying on third-party electronic identification services for users authentication, shall be required to accept the use of notified electronic identification means and European Digital Identity Wallet.			Prevederi UE neaplicabile		
(3) Până la 21 mai 2030 și, ulterior, la fiecare patru ani, Comisia prezintă un raport Parlamentului European și Consiliului cu privire la progresele realizate în vederea atingerii	3. By 21 May 2030 and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards			Prevederi UE neaplicabile		

obiectivelor prezentului regulament.	achieving the objectives of this Regulation.					
Articolul 50 Abrogare	**Article 50 Repeal**					
(1) Directiva 1999/93/CE se abrogă cu efect de la 1 iulie 2016.	1. Directive 1999/93/EC is repealed with effect from 1 July 2016.			Prevederi UE neaplicabile		
(2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament.	2. References to the repealed Directive shall be construed as references to this Regulation.			Prevederi UE neaplicabile		
Articolul 51 Măsuri tranzitorii	**Article 51 Transitional measures**					
(1) Dispozitivele sigure de creare a semnăturilor a căror conformitate a fost stabilită în conformitate cu articolul 3 alineatul (4) din Directiva 1999/93/CE sunt considerate în continuare dispozitive de creare a semnăturilor electronice calificate în temeiul prezentului regulament până la 21 mai 2027.	1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered to be qualified electronic signature creation devices under this Regulation until 21 May 2027.			Prevederi UE neaplicabile		
(2) Certificatele calificate emise persoanelor fizice în temeiul Directivei 1999/93/CE sunt considerate în continuare certificate calificate pentru semnături electronice în temeiul prezentului regulament până la 21 mai 2026.	2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until 21 May 2026.			Prevederi UE neaplicabile		
(3) Până la 21 mai 2026, gestionarea dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice la distanță de	3. The management of remote qualified electronic signature and seal creation devices by qualified trust service			Prevederi UE neaplicabile		

către alți prestatori de servicii de încredere calificați decât cei care prestează servicii de încredere calificate pentru gestionarea dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice la distanță în conformitate cu articolele 29a și 39a, se poate desfășura fără să fie necesară obținerea statutului de calificat pentru prestarea acestor servicii de gestionare.	providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a may be carried out without the need to obtain the qualified status for the provision of these management services until 21 May 2026.					
(4) Prestatorii de servicii de încredere calificați cărora li s-a acordat statutul de calificat în temeiul prezentului regulament înainte de 20 mai 2024 prezintă organismului de supraveghere un raport de evaluare a conformității care dovedește conformitatea cu articolul 24 alineatele (1), (1a) și (1b) cât mai curând posibil și în orice caz până la 21 mai 2026.	4. Qualified trust service providers that have been granted their qualified status under this Regulation before 20 May 2024 shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1), (1a) and (1b) as soon as possible and in any event by 21 May 2026.			Prevederi UE neaplicabile		
Articolul 52 **Intrarea în vigoare**	**Article 52** **Entry into force**					
(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.	1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.			Prevederi UE neaplicabile		
(2) Prezentul regulament se aplică de la 1 iulie 2016, cu excepția următoarelor dispoziții: (a) articolul 8 alineatul (3), articolul 9 alineatul (5),	2. This Regulation shall apply from 1 July 2016, except for the following: (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4),			Prevederi UE neaplicabile		

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; (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); (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).	22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014; (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8); (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).					
(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	3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of			Prevederi UE neaplicabile		

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.	paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.					
(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 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.	4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public . This Regulation shall be binding in its entirety and directly applicable in all Member States.			Prevederi UE neaplicabile		
ANEXA I	**ANNEX I**					
CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU	**REQUIREMENTS FOR QUALIFIED CERTIFICATES**	**Articolul 30. Cerințe pentru certificatele calificate pentru semnături electronice**				

SEMNĂTURI ELECTRONICE	FOR ELECTRONIC SIGNATURES					
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	Qualified certificates for electronic signatures shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated; (d) electronic signature validation data that corresponds to the electronic signature creation data; (e) details of the beginning and end of the certificate's period of validity;	Certificatele calificate pentru semnături electronice conțin: 1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice; 2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin: a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat; b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat; 3) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; 4) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice; 5) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; 6) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; 7) semnătura electronică avansată sau sigiliul electronic avansat al		Compatibil		

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) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii; (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.	(f) the certificate identity code, which must be unique for the qualified trust service provider; (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge; (i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate; (j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.	prestatorului de servicii de încredere calificat emitent; 8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 7); 9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii; 10) 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.				
ANEXA II	**ANNEX II**					
CERINȚE PENTRU DISPOZITIVELE CALIFICATE DE CREARE A SEMNĂTURILOR ELECTRONICE	**REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES**	**Articolul 31. Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate**				
1. Dispozitivele de creare a semnăturilor electronice	1. Qualified electronic signature creation	(2) Dispozitivele de creare a semnăturilor				

calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că: (a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil; (b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată; (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; (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.	devices shall ensure, by appropriate technical and procedural means, that at least: (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured; (b) the electronic signature creation data used for electronic signature creation can practically occur only once; (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology; (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.	electronice calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că: a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil; b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată; 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; 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.		Compatibil		
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.	2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.	(3) 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.				

ANEXA III	**ANNEX III**					
CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SIGILII ELECTRONICE	**REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS**	**Articolul 41. 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;	Qualified certificates for electronic seals shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records; (d) electronic seal validation data, which corresponds to the	Certificatele calificate pentru sigiliile electronice conțin: 1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru sigilii electronice; 2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin: a) în cazul unei persoane juridice: denumirea; b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat; 3) cel puțin numele/prenumele creatorului sigiliului și numărul de identificare de stat; 4) datele de validare a sigiliilor electronice, care corespund datelor de creare a sigiliilor electronice; 5) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; 6) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat;		Compatibil		

(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) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii; (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.	electronic seal creation data; (e) details of the beginning and end of the certificate's period of validity; (f) the certificate identity code, which must be unique for the qualified trust service provider; (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge; (i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate; (j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.	7) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; 8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 7); 9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii; 10) 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.				
ANEXA IV	**ANNEX IV**					
CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU AUTENTIFICAREA	**REQUIREMENTS FOR QUALIFIED CERTIFICATES**	**Articolul 49. Cerințe pentru certificatele calificate pentru**				

SITE-URILOR INTERNET	FOR WEBSITE AUTHENTICATION	autentificarea unui site internet				
Certificatele calificate pentru autentificarea unui site internet conțin: (a) o indicație, cel puțin într-o formă 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 emis certificatul sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (ca) în cazul persoanelor juridice: un set unic de date care reprezintă fără echivoc persoana juridică căreia i se emite certificatul, incluzând cel puțin denumirea persoanei juridice căreia i se emite certificatul și, după caz, numărul de înregistrare	Qualified certificates for website authentication shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; if a pseudonym is used, it shall be clearly indicated; (ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the	(2) Certificatele calificate pentru autentificarea unui site internet conțin: 1) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unui site internet; 2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin: a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat, b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat; 3) în cazul persoanelor fizice: cel puțin numele/prenumele persoanei căreia i s-a emis certificatul sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; 4) în cazul persoanelor juridice: un set unic de date care reprezintă fără echivoc persoana juridică căreia i se emite certificatul, incluzând cel puțin denumirea persoanei juridice căreia i se emite certificatul și, numărul de identificare de stat;		Compatibil		

astfel cum este menționat 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) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.	legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records; (d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records; (e) the domain name(s) operated by the natural or legal person to whom the certificate is issued; (f) details of the beginning and end of the certificate's period of validity; (g) the certificate identity code, which must be unique for the qualified trust service provider; (h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge; (j) the information or the location of the certificate validity status services that can be used to enquire about the	5) adresa persoanei fizice sau juridice căreia i s-a eliberat certificatul; 6) numele domeniului (domeniilor) gestionat(e) de persoana fizică sau juridică căreia i s-a emis certificatul; 7) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; 8) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; 9) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; 10) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la pct. 9); 11) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.				

	validity status of the qualified certificate.					
ANEXA V	**ANNEX V**					
CERINȚE PENTRU ATESTAREA ELECTRONICĂ CALIFICATĂ A ATRIBUTELOR	**REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES**	**Articolul 54. Cerințe privind atestatul electronic calificat al atributelor**				
Atestatul electronic calificat al atributelor conține: (a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic calificat al atributelor; (b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite atestatul electronic calificat al atributelor, incluzând cel puțin statul membru în care este stabilit prestatorul respectiv și: (i) în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum figurează în registrele oficiale, (ii) în cazul unei persoane fizice: numele persoanei; (c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru	Qualified electronic attestation of attributes shall contain: (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and: (i) for a legal person: the name and, where applicable, registration number as stated in the official records; (ii) for a natural person: the person's name; (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it	(2) Atestatul electronic calificat al atributelor conține: 1) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic calificat al atributelor; 2) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite atestatul electronic calificat al atributelor, incluzând cel puțin: a) în cazul unei persoane juridice: denumirea și numărul de identificare de stat, b) în cazul unei persoane fizice: numele/prenumele persoanei și numărul de identificare de stat; 3) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; 4) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a			

a identifica domeniul de aplicare al atributelor respective; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului; (f) codul de identificare al atestatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat și, în cazurile aplicabile, indicarea sistemului de atestare din care face parte atestatul atributelor; (g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent; (h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la litera (g); (i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.	shall be clearly indicated; (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes; (e) details of the beginning and end of the attestation's period of validity; (f) the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of; (g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge; (i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.	identifica domeniul de aplicare al atributelor respective; 5) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului; 6) codul de identificare al atestatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat și, în cazurile aplicabile, indicarea sistemului de atestare din care face parte atestatul atributelor; 7) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent; 8) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la pct. 7); 9) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.		Compatibil		
ANEXA VI	**ANNEX VI**					
LISTA MINIMĂ DE ATRIBUTE	**MINIMUM LIST OF ATTRIBUTES**	**Articolul 55. Verificarea atributelor în raport cu surse autentice**				

În conformitate cu articolul 45e, statele membre se asigură că se iau măsuri pentru a permite furnizorilor calificați de servicii de atestare electronică a atributelor să verifice prin mijloace electronice, la cererea utilizatorului, autenticitatea următoarelor atribute față de sursa autentică relevantă la nivel național sau prin intermediari desemnați recunoscuți la nivel național, în conformitate cu dreptul Uniunii sau cu dreptul intern și în cazul în care aceste atribute se bazează pe surse autentice din sectorul public: 1. Adresa; 2. Vârsta; 3. Sexul; 4. Starea civilă; 5. Componența familiei; 6. Naționalitatea sau cetățenia; 7. Calificările, titlurile și licențele educaționale; 8. Calificările, titlurile și licențele profesionale; 9. Împuternicirile și mandatele de a reprezenta persoane fizice sau juridice; 10. Autorizațiile și licențele publice; 11. Pentru persoanele juridice: datele financiare și datele privind societatea.	Pursuant to Article 45e, Member States shall ensure that measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and where these attributes rely on authentic sources within the public sector: 1. Address; 2. Age; 3. Gender; 4. Civil status; 5. Family composition; 6. Nationality or citizenship; 7. Educational qualifications, titles and licences; 8. Professional qualifications, titles and licences; 9. Powers and mandates to represent natural or legal persons; 10. Public permits and licences; 11. For legal persons, financial and company data.	(2) Măsurile prevăzute la alin. (1) se aplică, cel puțin, pentru următoarele categorii de atribute, în măsura în care acestea se bazează pe surse autentice din sectorul public: a) adresa; b) vârsta; c) genul; d) starea civilă; e) componența familiei; f) naționalitatea sau cetățenia; g) nivelul de studii, titluri și diplome; h) calificări profesionale, titluri și licențe; i) împuterniciri și mandate de reprezentare a persoanelor fizice sau juridice; j) acte permisive; k) pentru persoanele juridice, datele financiare și datele privind societățile.		Compatibil		
ANEXA VII	**ANNEX VII**					
CERINȚE PENTRU ATESTAREA ELECTRONICĂ A ATRIBUTELOR EMISĂ	**REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES**	**Articolul 56. Cerințe privind atestatul electronic al atributelor emis de un organism din**				

DE SAU ÎN NUMELE UNUI ORGANISM PUBLIC RESPONSABIL PENTRU O SURSĂ AUTENTICĂ	ISSUED BY OR ON BEHALF OF A PUBLIC BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE	sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism				
Un atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism conține: (a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism; (b) un set de date care reprezintă fără echivoc organismul public care emite atestatul electronic al atributelor, incluzând cel puțin statul membru în care este stabilit organismul public respectiv și denumirea sa și, după caz, numărul său de înregistrare, astfel cum figurează în registrele oficiale; (c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile,	An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain: (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source; (b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records; (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;	(2) Un atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism conține: (a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism; (b) un set de date care reprezintă fără echivoc organismul public care emite atestatul electronic al atributelor, incluzând cel puțin statul membru în care este stabilit organismul public respectiv și denumirea sa și, după caz, numărul său de înregistrare, astfel cum figurează în registrele oficiale; (c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a		Compatibil		

informațiile necesare pentru a identifica domeniul de aplicare al atributelor respective; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului; (f) codul de identificare al atestatului, care trebuie să fie unic pentru organismul public emitent și, în cazurile aplicabile, o indicare a sistemului de atestare din care face parte atestatul atributelor; (g) semnătura electronică calificată sau sigiliul electronic calificat al organismului emitent; (h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la litera (g); (i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.	(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes; (e) details of the beginning and end of the attestation's period of validity; (f) the attestation identity code, which must be unique for the issuing public body and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of; (g) the qualified electronic signature or qualified electronic seal of the issuing body; (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge; (i) the information or location of the services that can be used to enquire about the validity status of the attestation.	identifica domeniul de aplicare al atributelor respective; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului; (f) codul de identificare al atestatului, care trebuie să fie unic pentru organismul public emitent și, în cazurile aplicabile, o indicare a sistemului de atestare din care face parte atestatul atributelor; (g) semnătura electronică calificată sau sigiliul electronic calificat al organismului emitent; (h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la litera (g); (i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.				

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 13/1-1288 din 15.04.2026

Cancelaria de Stat

În temeiul prevederilor pct. 38 și 185 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, se transmite cererea privind înregistrarea în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali proiectul de lege privind identificarea electronică și serviciile de încredere.

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul de lege privind identificarea electronică și serviciile de încredere.
2.	Autoritatea care a elaborat proiectul	Elaborat de către Serviciul de Informații și Securitate al Republicii Moldova și promovat de către Ministerul Dezvoltării Economice și Digitalizării.
3.	Justificarea depunerii cererii	Elaborarea proiectului de lege privind identificarea electronică și serviciile de încredere este determinată de necesitatea modernizării și consolidării cadrului normativ național în domeniul identității digitale și al serviciilor de încredere electronice, în scopul alinierii depline a acestuia la evoluțiile accelerate ale cadrului legislativ al Uniunii Europene și la standardele tehnice internaționale aplicabile în domeniu.
4.	Referința la documentul de planificare care prevede elaborarea proiectului (PNA, PND, PNR, alte documente de planificare sectoriale)	PNA
5.	Lista autorităților și instituțiilor a căror avizare este necesară	Cancelaria de Stat (inclusiv Centrul de Armonizare a Legislației) Ministerul Finanțelor

		I.P. „Agenția de Guvernare Electronică” I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” I.P. „Agenția Servicii Publice” Serviciul de Informații și Securitate al Republicii Moldova
6.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile lucrătoare
7.	Persoana/e responsabile de promovarea proiectului	Oxana Rusanovschi, Șef adjunct Direcție tehnologii informaționale, tel. 022 250 636, e-mail, oxana.rusanovschi@mded.gov.md Ștefan Vornic, Șef Serviciu politici și reglementări în domeniul datelor deschise și reutilizarea informației, tel. 022 23 23 27, stefan.vornic@mded.gov.md
8.	Anexe	1. Proiect de lege; 2. Nota de fundamentare; 3. Tabel de concordanță.
9.	Data și ora depunerii cererii	
10.	Semnătura	/semnat electronic/

Secretar de Stat **Michelle ILIEV**

Ștefan Vornic
022 23 23 27