Aprobat în ședința Guvernului din _____ 2026

Decizia protocolară nr._____/2026

Proiect

UE

PARLAMENTUL REPUBLICII MOLDOVA

L E G E

privind identificarea electronică și serviciile de încredere

Parlamentul adoptă prezenta lege organică.

Prezenta lege transpune parțial Regulamentul (UE) 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, publicat în Jurnalul Oficial al Uniunii Europene L 257/73 din 28 august 2014, CELEX: 32014R0910, așa cum a fost modificat ultima dată prin Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024.

Capitolul I
DISPOZIȚII GENERALE

Articolul 1. Obiectul legii

Prezenta lege urmărește să asigure buna funcționare a pieței digitale naționale și facilitarea interoperabilității cu piața digitală europeană, precum 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 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 web, 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 legislația națională sau din acordurile încheiate între un set definit de participanți.

(3) Prezenta lege nu aduce atingere cadrului normativ referitor la 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. Noțiuni

În sensul prezentei legi, următoarele noțiuni semnifică:

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;

atestat electronic al atributelor – atestat în format electronic care permite atributelor să fie autentificate;

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

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 responsabil de o sursă autentică ori de un organism din sectorul public care este desemnat de Guvern să emită atestate ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice, în conformitate cu art. 56;

atribut – caracteristică, calitate, drept sau permisiune a unei persoane fizice sau juridice ori a unui obiect;

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

autentificare 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;

beneficiar – persoană fizică sau juridică care beneficiază de identificarea electronică, de portofelele pentru identitatea digitală sau de alte mijloace de identificare electronică sau de un serviciu de încredere;

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;

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;

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;

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;

certificat pentru autentificarea unui site web – atestat electronic care face posibilă autentificarea unui site web și face legătura între site-ul web și persoana fizică sau juridică căreia i s-a emis certificatul;

certificat calificat pentru autentificarea unui site web – certificat pentru autentificarea unui site web care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 50;

corelare a 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;

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

date cu caracter personal – astfel cum este definit la art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal;

date de creare a semnăturilor electronice – date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;

date de creare a sigiliilor electronice – date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;

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

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

dispozitiv de creare a semnăturilor electronice – software sau hardware configurat, utilizat pentru a crea o semnătură electronică;

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

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;

dispozitiv de creare a sigiliului electronic – software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;

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

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;

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

identificare electronică – proces 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;

înregistrare de date – date electronice înregistrate împreună cu metadatele aferente care susțin prelucrarea datelor;

marcă temporală electronică – date în format electronic care leagă alte date în format electronic de un anumit moment, constituind o dovadă că acestea din urmă au existat la momentul respectiv;

marcă temporală electronică calificată – marcă temporală electronică care îndeplinește cerințele prevăzute la art. 47;

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;

mod offline – interacțiune între un utilizator și o terță parte, desfășurată într-un loc fizic care utilizează tehnologii de proximitate imediată, fără a fi necesară accesarea de către portofelul pentru identitatea digitală a unor sisteme la distanță prin rețele de comunicații electronice în scopul interacțiunii respective;

organism de drept public – organism care îndeplinește cumulativ următoarele condiții:

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

b) are personalitate juridică; și

c) este finanțat în proporție majoritară de autorități publice centrale sau locale sau de alte organisme de drept public; ori gestionarea acestuia este

supravegheată de autoritățile sau organismele respective; ori are un consiliu administrativ, de conducere sau de supraveghere, în care peste 50 % dintre membrii săi sunt numiți de autorități ale administrației publice centrale sau locale ori de alte organisme de drept public;

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;

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 prestate de acesta ori de a efectua certificarea portofelelor pentru identitatea digitală sau a mijloacelor de identificare electronică;

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 și să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate;

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;

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;

produs – hardware sau software ori componente relevante ale acestora, destinate să fie utilizate pentru prestarea serviciilor de identificare electronică și a serviciilor de încredere;

registru electronic – secvență de înregistrări electronice de date care asigură integritatea acestora, precum și acuratețea ordinii cronologice a înregistrărilor respective;

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

semnatar – persoană fizică care creează o semnătură electronică;

semnătură electronică – date în format electronic atașate sau asociate logic cu alte date în format electronic, utilizate de către semnatar pentru a semna;

semnătură electronică avansată – semnătură electronică care îndeplinește cerințele prevăzute la art. 27;

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;

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

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;

serviciu de distribuție electronică înregistrată calificat – serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art. 49;

serviciu de încredere – serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare dintre următoarele:

a) emiterea certificatelor pentru semnături electronice, a certificatelor pentru sigilii electronice, a certificatelor pentru autentificarea unui site web 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 web 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 ale 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;

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

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

sigiliu electronic avansat – sigiliu electronic care îndeplinește cerințele prevăzute la art. 38;

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;

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;

sursă autentică – registru sau 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;

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;

validare – proces 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 de identificare a utilizatorilor prevăzute de legislația aplicabilă serviciului sau activității desfășurate și nici efectelor juridice recunoscute pseudonimelor.

(3) Beneficiarii nu pot refuza utilizarea pseudonimelor decât dacă identificarea expresă este impusă prin lege sau justificată de scopul legitim al serviciului.

Capitolul II
IDENTIFICARE ELECTRONICĂ

Secțiunea 1
Portofelul pentru identitatea digitală

Articolul 5. Portofelele pentru identitatea digitală

(1) În scopul garantării faptului că toate persoanele fizice și juridice din Republica Moldova au acces securizat, fiabil și neîntrerupt la servicii, păstrând totodată controlul deplin asupra datelor lor, Guvernul asigură, prin actele sale normative, funcționarea cel puțin a unui portofel pentru identitatea digitală.

(2) Portofelele pentru identitatea digitală pot fi furnizate atât de un organism din sectorul public desemnat de către Guvern, cât și de persoane juridice de drept privat, cu respectarea cerințelor prevăzute de lege. În vederea garantării principiului liberei alegeri, utilizatorii au dreptul de a selecta în mod liber portofelul pentru identitatea digitală care corespunde necesităților lor, fără a fi constrânși să utilizeze un anumit furnizor.

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

(4) 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, 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 a unei alte persoane, să primească și să 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 lista 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 din Legea nr. 195/2024 privind protecția datelor cu caracter personal;

c) să semnaleze cu ușurință autorității naționale pentru protecția datelor cu caracter personal cu privire la un beneficiar, 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 intermediul 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 în 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 din Legea 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 criteriile prevăzute la art. 12 în ceea ce privește nivelul de asigurare ridicat, în special 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, pun 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 care 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, dar nu mai târziu de 24 de ore, cu privire la orice încălcare a securității care le-ar fi putut compromite total sau parțial portofelul pentru identitatea digitală sau conținutul acestuia, 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 parcursul întregului 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 a portofelelor 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 servicii, 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 servicii 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 ori a comportamentului utilizatorului sau obținerea în alt mod a informațiilor privind tranzacțiile ori 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 de 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) Furnizorii portofelelor pentru identitatea digitală și beneficiarii nu pot agrega, corela sau utiliza datele tranzacționale pentru profilarea comportamentală a utilizatorilor, cu excepția cazurilor prevăzute de lege în mod expres.

(20) Organismul de supraveghere publică pe site-ul său web oficial, printr-un canal securizat și într-un format care permite prelucrarea automată, semnat electronic sau sigilat electronic, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 3 zile lucrătoare, informațiile privind:

a) lista furnizorilor portofelelor pentru identitatea digitală;

b) 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);

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

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

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

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

(23) Atunci când furnizorii de portofele pentru identitatea digitală și emitenții mijloacelor 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 pentru a asigura interoperabilitatea. 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.

(24) 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. 9, 15 și 16.

(25) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri privind implementarea portofelelor pentru identitatea digitală.

Articolul 6. Beneficiarii portofelului pentru identitatea digitală

(1) În cazul în care un beneficiar intenționează să utilizeze portofele pentru identitatea digitală în vederea furnizării de servicii prin intermediul interacțiunii digitale, acesta se înregistrează în lista beneficiarilor din Republica Moldova, gestionată de organismul de supraveghere.

(2) Procesul de înregistrare se desfășoară în format electronic, în modul stabilit de Guvern, și este eficient din punct de vedere al costurilor și proporțional cu riscurile, iar beneficiarul furnizează cel puțin:

a) informațiile necesare pentru autentificarea în portofelele pentru identitatea digitală, care includ cel puțin numele sau denumirea beneficiarului și numărul de înregistrare de stat al acestuia;

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, inclusiv serviciilor financiare, bancare, de plată sau altor servicii supuse unor cerințe sectoriale speciale, precum și obligațiilor prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului.

(5) Beneficiarii pot solicita exclusiv atribute strict necesare scopului declarat și proporționale cu serviciul furnizat.

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

(7) Beneficiarii înregistrați în conformitate cu prezentul articol informează fără întârziere, dar nu mai târziu de 3 zile lucrătoare, organismul de supraveghere cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alin. (2), în măsura în care actualizarea acestora nu este asigurată automat prin interoperabilitatea cu registrele de stat și cu alte sisteme informaționale relevante.

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

(9) Beneficiarii sunt responsabili personal de îndeplinirea procedurii de autentificare și validare a datelor de identificare, precum și de atestare electronică a atributelor solicitate în cadrul portofelelor pentru identitatea digitală. Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care legislația aplicabilă serviciului sau activității desfășurate de aceștia nu impune identificarea utilizatorului.

(10) 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 alin. (5), (6) și (9), cu cerința privind separarea logică prevăzută la art. 5 alin. (15), precum și cu standardele și specificațiile tehnice stabilite de Guvern, se certifică de către organisme de evaluare a conformității.

(2) Certificarea realizată în temeiul alin. (1) este valabilă pentru o perioadă de până la 5 ani, cu condiția efectuării unei evaluări a vulnerabilității la fiecare 2 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.

(4) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru certificarea portofelelor pentru identitatea digitală.

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

(3) Organismul de supraveghere asigură actualizarea listei portofelelor pentru identitatea digitală certificate în termen de o lună de la primirea informațiilor actualizate în temeiul alin. (2).

(4) Portofelele europene pentru identitatea digitală certificate în statele membre ale Uniunii Europene păstrează statutul de certificate pe teritoriul Republicii Moldova, fără a fi necesară notificarea și desfășurarea procedurilor de verificare.

(5) În scopul informării utilizatorilor și al facilitării verificării portofelelor europene pentru identitatea digitală certificate, organismul de supraveghere preia informațiile relevante din lista portofelelor europene pentru identitatea digitală certificată și le publică pe site-ul său web oficial, asigurând actualizarea acestora în funcție de modificările operate în lista respectivă.

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. (9) 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, organismul de supraveghere suspendă fără întârziere nejustificată și, în orice caz, nu mai târziu de 8 ore, furnizarea și utilizarea portofelelor pentru identitatea digitală. Furnizorii portofelelor pentru identitatea digitală informează, în modul stabilit de organismul de supraveghere, utilizatorii și beneficiarii afectați.

(2) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) nu este remediată în termen de 3 luni de la suspendare, organismul de supraveghere retrage portofelele pentru identitatea digitală și le revocă valabilitatea. Furnizorii portofelelor pentru identitatea digitală informează, în modul stabilit de organismul de supraveghere, utilizatorii și beneficiarii afectați.

(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 și, în orice caz, nu mai târziu de 24 de ore, utilizatorii și beneficiarii afectați, precum și organismul de supraveghere.

(4) Organismul de supraveghere asigură publicarea, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 3 zile lucrătoare, a modificărilor 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 online, acestea acceptă și utilizarea portofelelor pentru identitatea digitală furnizate în statele membre ale Uniunii Europene, 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) În cazul în care beneficiarii privați care furnizează servicii, cu excepția microîntreprinderilor și a întreprinderilor mici, astfel cum sunt definite în Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii, au obligația legală 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 legii și numai la cererea voluntară a utilizatorului, acceptă și utilizarea portofelelor pentru identitatea digitală care sunt furnizate în conformitate cu prezenta lege.

(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 site-ul său web oficial.

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 a respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare substanțial sau ridicat, conform clasificării prevăzute de lege;

c) organismul din sectorul public relevant utilizează nivelul de asigurare substanțial sau ridicat în legătură cu accesarea online a serviciului respectiv.

(2) Mijloacele de identificare electronică eliberate în temeiul unui sistem de identificare electronică inclus în lista publicată de Comisia Europeană și care corespund nivelului de asigurare scăzut pot fi recunoscute de către organismele din sectorul public în scopul autentificării transfrontaliere pentru serviciul furnizat online de către organismele respective.

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

(4) Orice serviciu public online care acceptă autentificarea transfrontalieră trebuie să asigure transparența criteriilor și să informeze utilizatorii cu privire la 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 limitat 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 mijlocului de identificare în cauză, inclusiv controalele tehnice, al căror scop este de a reduce riscul utilizării 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 mijlocului de identificare în cauză, 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, standardele și procedurile corespunzătoare mijlocului de identificare în cauză, inclusiv la 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 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 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 de 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 condițiile prevăzute la alin. (2) și specificațiile tehnice, standardele și procedurile pentru nivelurile de asigurare stabilite de către 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) Un sistem de identificare electronică este eligibil pentru includerea în lista sistemelor naționale de identificare electronică dacă sunt îndeplinite cumulativ următoarele condiții:

a) mijloacele de identificare electronică din cadrul sistemului sunt emise de către un organism din sectorul public;

b) mijloacele de identificare electronică din cadrul sistemului de identificare electronică pot fi utilizate pentru a accesa cel puțin un serviciu care este prestat de către un organism din sectorul public care necesită identificare electronică;

c) sistemul de identificare electronică și mijloacele de identificare electronică emise în temeiul acestuia îndeplinesc cerințele stabilite de Guvern pentru cel puțin unul dintre nivelurile de asigurare prevăzute la art. 12;

d) deținătorul sistemului asigură atribuirea datelor unice de identificare personală, în conformitate cu specificațiile tehnice și standardele aferente nivelului de asigurare relevant, persoanei fizice sau juridice căreia îi sunt emise mijloacele de identificare electronică.

(3) Organismul de supraveghere publică pe site-ul său web oficial lista sistemelor de identificare electronică notificate în temeiul alin. (1), împreună cu informațiile de bază privind aceste sisteme, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 3 zile lucrătoare de la notificarea sistemului respectiv.

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

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 prevenirea creării de profiluri ale utilizatorilor.

Articolul 15. Interoperabilitatea

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

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

a) urmărește să fie neutru din punct de vedere al tehnologiei și nu acordă prioritate niciunei soluții tehnice specifice pentru identificarea electronică;

b) respectă standardele europene și internaționale;

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

(3) Cadrul 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 ori o persoană fizică care 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 criteriile prevăzute la art. 12 alin. (2) cu privire la 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 până la 5 ani, cu condiția să se efectueze o evaluare a vulnerabilității o dată la 2 ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în termen de 3 luni de la identificarea sa, certificarea se anulează.

Capitolul III
SERVICII DE ÎNCREDERE

Secțiunea 1
Dispoziții cu privire la serviciile de încredere

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 care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentei legi de către un prestator de servicii de încredere are dreptul de a solicita despăgubiri în conformitate cu Codul civil al Republicii Moldova nr. 1107/2002.

(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 se prezumă, cu excepția cazului în care acesta 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, în modul stabilit de organismul de supraveghere, își informează clienții în prealabil 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 calificate prestate de prestatori de servicii de încredere calificați cu sediul în orice stat membru al Uniunii Europene sau în 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, utilizate pentru prestarea serviciilor respective, sunt furnizate într-un limbaj clar și inteligibil și sunt accesibile persoanelor cu deficiențe de auz și vedere, în conformitate cu Convenția Națiunilor Unite privind drepturile persoanelor cu dizabilități, inclusiv persoanelor care se confruntă cu limitări funcționale senzoriale, 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

(1) 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 integrare aferente unui serviciu de încredere;

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

c) gestionarea și implementarea serviciilor de încredere;

2) notifică organismul de supraveghere, a persoanelor afectate care pot fi identificate, a publicului (dacă chestiunea este de interes public) și, după caz, a 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 pct. 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri. În cazul în care standardele și procedurile respective sunt respectate, se prezumă că sunt respectate cerințele prevăzute la alin. (1).

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 de prezenta lege și respectă măsurile de gestionare a riscurilor în materie de securitate cibernetică stabilite la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică. Prestatorii de servicii de încredere calificați transmit organismului de supraveghere raportul de evaluare a conformității rezultat în termen de 3 zile lucrătoare de la primirea acestuia.

(2) Prestatorii de servicii de încredere calificați informează organismul de supraveghere cu cel puțin o lună înainte de efectuarea unui 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 de prezenta lege. În cazul în care există indicii privind încălcarea normelor de protecție a datelor cu caracter personal, organismul de supraveghere informează, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore, 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 de prezenta lege, organismul de supraveghere îi solicită să remedieze situația într-un termen stabilit.

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

(6) În cazul în care prestatorul de servicii de încredere calificat nu îndeplinește măsurile de gestionare a riscurilor în materie de securitate cibernetică 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 încălcării în cauză, 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 de 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.

(9) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru:

a) acreditarea organismelor de evaluare a conformității și raportul de evaluare a conformității menționat la alin. (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 alin. (1);

c) sistemele de evaluare a conformității utilizate de organismele de evaluare a conformității pentru efectuarea evaluării conformității prestatorilor de servicii de încredere calificați și pentru furnizarea raportului menționat la alin. (1).

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 de a presta serviciul respectiv, anexând un raport de evaluare a conformității emis de un organism de evaluare a conformității, care confirmă îndeplinirea cerințelor prevăzute de prezenta lege și de 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 de prezenta lege și, în special, cerințele pentru prestatorii de servicii de încredere calificați și pentru serviciile de încredere calificate prestate de aceștia.

(3) Pentru a verifica respectarea de către prestatorul de servicii de încredere a cerințelor prevăzute la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică, organismul de supraveghere efectuează acțiunile de supraveghere necesare în acest scop și documentează rezultatele acestora fără întârzieri nejustificate și, în orice caz, în termen de 2 luni de la inițierea verificării. În cazul în care verificarea nu este încheiată în termen de 2 luni de la inițierea acesteia, organismul de supraveghere consemnează motivele întârzierii și termenul în care urmează să se încheie verificarea.

(4) 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 prezenta lege, organismul de supraveghere, în termen de 3 luni de la notificarea depusă conform alin. (1), acordă statutul de

calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta și publică informațiile respective în lista sigură prevăzută la art. 23.

(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 prevăzută la art. 23.

(6) Prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene păstrează statutul de calificat pe teritoriul Republicii Moldova, fără necesitatea desfășurării notificării sau a procedurilor de verificare.

(7) În scopul informării utilizatorilor și al facilitării verificării statutului prestatorilor de servicii de încredere calificați din statele membre ale Uniunii Europene, organismul de supraveghere preia informațiile relevante din listele de încredere naționale ale acestora și le publică pe site-ul său web oficial, asigurând actualizarea acestora în funcție de modificările operate în listele respective.

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 dispoziția 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 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 în mod direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, 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 criteriile 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.

(3) Verificarea atributelor menționată la alin. (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie în mod direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, 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 criteriile 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. (2) 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 și prin utilizarea unor mijloace de probă și proceduri adecvate.

(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 3 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 prejudiciile cauzate în conformitate cu art. 17, menține suficiente resurse financiare și/sau obține o asigurare de răspundere adecvată;

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 serviciului respectiv, 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 temeiul 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, printr-o decizie motivată, să solicite informații suplimentare față de cele 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 3 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, fără ca durata totală a verificării să depășească termenul de 4 luni de la data notificării.

(6) Dacă un prestator de servicii de încredere calificat care eliberează certificate calificate decide să revoce un certificat, acesta înregistrează revocarea

respectivă 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, inclusiv după expirarea perioadei de valabilitate a certificatului, în mod automat, fiabil, gratuit și eficient.

(8) Alineatele (6) și (7) se aplică și 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, furnizate într-un stat membru al Uniunii Europene, sunt recunoscute, după caz, 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 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, furnizate într-un stat membru al Uniunii Europene, sunt recunoscute, după caz, drept serviciu de validare calificat pentru semnături electronice calificate și drept serviciu de validare calificat pentru sigilii electronice calificate în Republica Moldova.

(5) Un serviciu calificat de păstrare a semnăturilor electronice calificate, precum și un serviciu calificat de păstrare a sigiliilor electronice calificate,

furnizate într-un stat membru al Uniunii Europene, sunt recunoscute, după caz, drept serviciu calificat de păstrare a semnăturilor electronice calificate și 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 web emis într-un stat membru al Uniunii Europene este recunoscut drept certificat calificat pentru autentificarea unui site web 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 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.

(2) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru semnăturile electronice avansate. În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile respective, 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 cazul în care se solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, se recunosc 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 alin. (4).

(2) În cazul în care se 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, se recunosc semnăturile electronice 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 alin. (4).

(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.

(4) Guvernul aprobă formate de referință ale semnăturilor electronice avansate sau metode de referință, în cazul utilizării formatelor alternative.

Articolul 29. Certificate calificate pentru semnăturile electronice

(1) Certificatele calificate pentru semnăturile electronice trebuie să îndeplinească 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 indicată clar în baza de date privind certificatele, iar 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru certificatele calificate pentru semnăturile electronice. 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 drept 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, după caz, numărul de identificare de stat;

b) în cazul unei persoane fizice: numele persoanei și, după caz, 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 trebuie să îndeplinească 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;

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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru dispozitivele de creare a semnăturilor electronice calificate. 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

(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:

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.

(2) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri în scopul aplicării alin. (1).

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

(3) Perioada de valabilitate a certificării menționate la alin. (1) nu depășește termenul de 5 ani, cu condiția efectuării unei evaluări a vulnerabilităților la fiecare 2 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.

(5) Guvernul stabilește criterii specifice ce urmează a fi îndeplinite de către organismele de evaluare a conformității.

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 unui pseudonim este indicată clar beneficiarului în cazul în care, la momentul semnării, a fost folosit un pseudonim;

f) integritatea datelor semnate nu a fost compromisă;

g) cerințele prevăzute la art. 27 au fost îndeplinite în 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru validarea semnăturilor electronice calificate sau a semnăturilor electronice avansate bazate pe certificate calificate. În cazul în care validarea semnăturilor electronice calificate 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 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 (2); și

b) permite beneficiarilor să primească rezultatul procesului de validare în mod automat, fiabil și eficient și care poartă semnătura electronică avansată sau sigiliul electronic avansat al prestatorului care oferă serviciul de validare calificat.

(2) Guvernul stabilește o listă de standarde de referință, de specificații și proceduri pentru serviciul calificat de validare menționat la alin. (1). 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru serviciul calificat de păstrare a semnăturilor electronice calificate. În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele, 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 datelor respective la care se referă sigiliul electronic calificat.

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 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru sigiliile electronice avansate. 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 cazul în care se solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, sunt recunoscute 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 menționate la alin. (4).

(2) În cazul în care se 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, sunt recunoscute sigiliile electronice avansate bazate pe un certificat calificat și sigiliile electronice

calificate care întrebuințează cel puțin formatele sau metodele definite în actele menționate la alin. (4).

(3) 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.

(4) Guvernul definește formate de referință ale sigiliilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative.

Articolul 40. Certificate calificate pentru sigiliul electronic

(1) Certificatele calificate pentru sigiliile electronice trebuie să îndeplinească cerințele prevăzute la 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 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 își pierde valabilitatea din momentul în care a fost revocat și nu se revine în niciun caz la statutul său anterior.

(7) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru certificatele calificate pentru sigiliul electronic. 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 drept 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 și, după caz, numărul de identificare de stat;

b) în cazul unei persoane fizice: numele persoanei și, după caz, numărul de identificare de stat;

3) cel puțin numele creatorului sigiliului și, după caz, 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 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. 34-36 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru legătura dintre dată și oră și date și pentru stabilirea exactității surselor orei indicate. 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 calificată.

(2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată calificată 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 calificată.

Articolul 49. Cerințe pentru serviciile de distribuție electronică înregistrată calificate

(1) Serviciile de distribuție electronică înregistrată calificate trebuie să îndeplinească 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 sunt securizate 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 de a primi datele este clar indicată expeditorului și destinatarului datelor;

f) data și ora trimiterii, primirii și ale oricărei modificări a datelor sunt indicate 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) 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru procesele de trimitere și primire de date. 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 web

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

(1) Certificatele calificate pentru autentificarea unui site web trebuie să îndeplinească cerințele prevăzute la alin. (2).

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

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

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, după caz, numărul de identificare de stat;

b) în cazul unei persoane fizice: numele și, după caz, numărul de identificare de stat;

3) 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;

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) elemente ale adresei persoanei fizice sau juridice căreia i s-a eliberat certificatul, incluzând cel puțin orașul și statul, în forma în care sunt înscrise în registrele oficiale;

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 web 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 web 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 și mijlocii, în primii 5 ani de funcționare ca prestatori de servicii de navigare pe web.

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

(5) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru certificatele calificate pentru autentificarea unui site web. În cazul în care un certificat calificat pentru autentificarea unui site web 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 web 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 notifică suspiciunile în scris, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore, 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 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 cadrului normativ aplicabil 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 actele normative ale Guvernului. Într-un astfel de caz, se acceptă, de asemenea, atestatul electronic calificat al atributelor emis într-un stat membru al Uniunii Europene.

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, după caz, numărul de identificare de stat;

b) în cazul unei persoane fizice: numele persoanei și, după caz, 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru atestatul electronic calificat al atributelor. 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 în domeniul sistemelor informaționale și al registrelor de stat, disponibilitatea mecanismelor electronice care permit verificarea atributelor persoanelor fizice și juridice de către prestatorii de servicii de încredere calificați care 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) sexul;

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 constituirea, înregistrarea, organizarea și statutul juridic ale acestora.

(3) Lista organismelor din sectorul public responsabile de furnizarea atestatelor electronice ale atributelor pentru fiecare categorie prevăzută la alin. (2) se stabilește de Guvern, cu consultarea organismului de supraveghere și a deținătorilor surselor autentice.

(4) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru catalogul de atribute, precum și sisteme pentru atestarea atributelor și procedurile de verificare pentru atestatele electronice calificate.

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 către 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 sau desemnat în condițiile legii 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 către un organism din sectorul 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 de către un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism;

b) un set de date care reprezintă fără echivoc organismul din sectorul public care emite atestatul electronic al atributelor, incluzând cel puțin statul membru în care este stabilit organismul din sectorul 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 din sectorul public emitent și, în cazurile aplicabile, o indicație 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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism. 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 asigură interoperabilitatea cu portofelele pentru identitatea digitală furnizate în conformitate cu art. 5, prin intermediul unei interfețe, în conformitate cu standardele și specificațiile tehnice aprobate de Guvern, armonizate cu standardele europene aplicabile.

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 Guvern.

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

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

(1) Prestatorii de servicii 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 trebuie să îndeplinească 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 sau formatul electronic al acestora;

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) Guvernul stabilește o listă de standarde de referință și, dacă este necesar, de specificații și proceduri pentru serviciul calificat de arhivare electronică. 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 cronologice secvențiale unice și exacte a înregistrărilor și de prezumția de integritate.

Articolul 62. Cerințe privind registrele electronice calificate

(1) Registrele electronice calificate trebuie să îndeplinească 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 ulterioară a acestora 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 instituție publică ori de către o persoană în exercitarea și în limitele atribuțiilor de putere publică ale acesteia, 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 în mod expres de actele normative sau atunci când părțile au convenit în mod explicit utilizarea semnăturilor electronice.

(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 acestora, 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 semnat cu semnătură electronică calificată se consideră a fi 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 semnat cu semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat 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 pe 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) Guvernul desemnează organismul de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere și stabilește modul de organizare și funcționare a acestuia.

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

a) supravegherea furnizorilor de portofele pentru identitatea digitală cu sediul în Republica Moldova și asigurarea, prin intermediul unor activități de supraveghere *ex ante* și *ex post*, a 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 Republica Moldova și asigurarea, prin intermediul unor activități de supraveghere *ex ante* și *ex post*, a îndeplinirii de către respectivii prestatori de servicii de încredere calificați și de către serviciile de încredere calificate prestate de aceștia a cerințelor stabilite de prezenta lege;

c) luarea măsurilor, 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 este informat că furnizorii sau portofelele pentru identitatea digitală furnizate de aceștia încalcă prezenta lege;

d) luarea măsurilor, 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 este informat 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 și, în orice caz, nu mai târziu de 24 de ore, în cazul în care există indicii privind încălcarea normelor de protecție a datelor cu caracter personal, 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) solicită prestatorilor de servicii de încredere să remedieze încălcările cerințelor prevăzute de prezenta lege;

e) 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);

f) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore, în cazul în care există indicii privind încălcarea normelor de protecție a datelor cu caracter personal, precum și cu privire la

încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal;

g) investighează cererile formulate de furnizorii de browsere web în temeiul art. 51 și întreprinde măsuri, dacă este necesar.

(4) În cazul în care organismul de supraveghere, în temeiul alin. (3) 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 și, în orice caz, nu mai târziu de 24 de ore, 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 datelor statistice cu privire la 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, PROCEDURA DE CONSTATARE ȘI SANCȚIUNILE

Secțiunea 1
Dreptul de a depune o plângere. Răspunderea civilă și dreptul la despăgubiri

Articolul 67. Dreptul de a depune o plângere

(1) Fără a aduce atingere art. 68, orice persoană fizică sau juridică are dreptul de a depune o plângere la organismul de supraveghere în cazul în care consideră că un prestator de servicii de încredere, calificat sau necalificat, sau un furnizor de portofele pentru identitatea digitală a încălcat prevederile prezentei legi în legătură cu serviciile sau funcționalitățile utilizate de aceasta.

(2) Termenul de prescripție pentru depunerea plângerii este de un an de la data la care persoana putea să ia cunoștință de presupusa încălcare, însă nu mai târziu de 3 ani de la data presupusei încălcări.

(3) În cazul unei presupuse încălcări continue sau prelungite, termenul de prescripție începe să curgă de la data săvârșirii ultimei acțiuni sau inacțiuni.

(4) În cazul în care plângerea este depusă după expirarea termenului de prescripție prevăzut la alin. (2) și (3), organismul de supraveghere o respinge.

(5) Organismul de supraveghere informează autorul plângerii cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a contesta actele acestuia în conformitate cu art. 68.

(6) Prevederile Codului administrativ al Republicii Moldova nr. 116/2018 se aplică numai în măsura în care nu contravin prezentei legi.

Articolul 68. Dreptul de a contesta acțiunile sau inacțiunile organismului de supraveghere

(1) Acțiunile sau inacțiunile organismului de supraveghere pot fi contestate direct în instanța de judecată, conform Codului administrativ al Republicii Moldova nr. 116/2018, fără respectarea procedurii prealabile.

(2) În cazul în care organismul de supraveghere nu examinează o plângere sau nu informează autorul acesteia în termen de 3 luni cu privire la progresele ori la soluționarea plângerii depuse conform art. 67, persoana afectată poate contesta inacțiunile organismului de supraveghere direct în instanța de judecată, conform Codului administrativ al Republicii Moldova nr. 116/2018, fără respectarea procedurii prealabile.

Articolul 69. Dreptul de a depune o cerere de chemare în judecată împotriva prestatorului sau furnizorului

Fără a aduce atingere art. 67 și 68, precum și fără a aduce atingere modalităților alternative de soluționare a litigiilor, orice persoană fizică sau juridică are dreptul de a depune o cerere de chemare în judecată la instanța judecătorească competentă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentei legi au fost încălcate ca urmare a prestării unor servicii de încredere sau a furnizării unor portofele pentru identitatea digitală fără respectarea prezentei legi.

Articolul 70. Dreptul la despăgubiri și răspunderea

(1) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentei legi de către un prestator de servicii de încredere sau un furnizor de portofele pentru identitatea digitală are dreptul să obțină despăgubiri de la acesta pentru prejudiciul suferit.

(2) Orice prestator de servicii de încredere sau furnizor de portofele pentru identitatea digitală implicat în furnizarea serviciului sau a funcționalității care a produs prejudiciul este răspunzător pentru prejudiciul cauzat de activitățile sale care încalcă prezenta lege.

(3) Prestatorul de servicii de încredere sau furnizorul de portofele pentru identitatea digitală este exonerat de răspundere în temeiul alin. (2) dacă dovedește că nu este răspunzător în niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) În cazul în care mai mulți prestatori de servicii de încredere sau furnizori de portofele pentru identitatea digitală sunt implicați în aceeași operațiune sau lanț de servicii care a produs prejudiciul și răspund în temeiul alin. (2) și (3) pentru orice prejudiciu cauzat, fiecare dintre aceștia este răspunzător pentru întregul prejudiciu, în vederea asigurării despăgubirii efective a persoanei afectate.

(5) În cazul în care un prestator sau furnizor a plătit, în conformitate cu alin. (4), în totalitate despăgubirile pentru prejudiciul cauzat, acesta are dreptul să solicite de la ceilalți prestatori sau furnizori implicați în aceeași operațiune sau lanț de servicii recuperarea părții din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu.

(6) Acțiunile în exercitarea dreptului de recuperare a despăgubirilor se depun la instanțele judecătorești competente în conformitate cu legislația.

Articolul 71. Răspunderea juridică în cadrul tranzacțiilor transfrontaliere

(1) Răspunderea pentru prejudiciul cauzat în cadrul tranzacțiilor transfrontaliere reglementate de prezenta lege este individuală și revine, în limitele sferei proprii de obligații, fiecăruia dintre subiecții prevăzuți la alin. (2)–(4). Răspunderea devine solidară atunci când același prejudiciu este imputabil, prin fapte proprii distincte, mai multor subiecți prevăzuți la alin. (2)–(4), fiecare dintre aceștia putând fi obligat la repararea integrală a prejudiciului, cu drept de regres

împotriva celorlalți subiecți proporțional cu contribuția fiecăruia la producerea acestuia.

(2) Organismul de supraveghere răspunde față de orice persoană fizică sau juridică pentru prejudiciul cauzat în mod intenționat sau din culpă în cadrul unei tranzacții transfrontaliere, dacă sunt întrunite cumulativ următoarele condiții:

a) organismul de supraveghere a săvârșit o faptă ilicită constând în neîndeplinirea sau îndeplinirea defectuoasă a obligațiilor care îi revin potrivit prezentei legi, în legătură cu asigurarea interoperabilității și securității sistemelor de identificare electronică;

b) persoana a suferit un prejudiciu material sau moral cert și determinabil;

c) există o legătură de cauzalitate directă între fapta ilicită și prejudiciul suferit.

(3) Emitentul mijloacelor de identificare electronică răspunde față de orice persoană fizică sau juridică pentru prejudiciul cauzat în mod intenționat sau din culpă în cadrul unei tranzacții transfrontaliere, dacă sunt întrunite cumulativ următoarele condiții:

a) emitentul a încălcat obligația de a asigura că mijloacele de identificare electronică emise corespund, la momentul emiterii și pe întreaga perioadă de valabilitate, datelor de identificare electronică ale persoanei căreia i-au fost atribuite;

b) persoana a suferit un prejudiciu material sau moral cert și determinabil;

c) există o legătură de cauzalitate directă între neconformitatea mijloacelor de identificare electronică emise și prejudiciul suferit.

(4) Partea care execută procedura de autentificare răspunde față de orice persoană fizică sau juridică pentru prejudiciul cauzat în mod intenționat sau din culpă în cadrul unei tranzacții transfrontaliere, dacă sunt întrunite cumulativ următoarele condiții:

a) procedura de autentificare a fost executată în mod incorect sau incomplet, cu nerespectarea cerințelor tehnice și de securitate prevăzute de prezenta lege;

b) persoana a suferit un prejudiciu material sau moral cert și determinabil;

c) există o legătură de cauzalitate directă între executarea incorectă a autentificării și prejudiciul suferit.

(5) Subiectul răspunzător este exonerat de răspundere dacă dovedește că prejudiciul s-a produs ca urmare a unei cauze exterioare care nu îi este imputabilă.

(6) Sarcina probei privind îndeplinirea condițiilor angajării răspunderii revine persoanei prejudiciate. Sarcina probei privind exonerarea de răspundere revine subiectului împotriva căruia se formulează pretențiile.

(7) Dispozițiile prezentului articol se completează cu prevederile legislației civile în materia răspunderii civile delictuale, în măsura în care nu contravin prezentei legi.

Secțiunea a 2-a

Procedura de constatare a încălcărilor și de aplicare a sancțiunilor

Articolul 72. Inițierea procedurii de constatare

(1) Organismul de supraveghere inițiază procedura de constatare a presupuselor cazuri de încălcare a prezentei legi:

a) la plângerea unui prestator de servicii de încredere, a unui furnizor de portofele pentru identitatea digitală, a unui utilizator sau a oricărei alte persoane afectate; sau

b) din oficiu, în baza informațiilor de care dispune cu privire la presupusa încălcare a prezentei legi.

(2) Procedura de constatare cuprinde:

a) examinarea preliminară; și/sau

b) investigarea.

(3) În orice stadiu al procedurii, părțile pot conveni asupra unei soluții amiabile, confirmată prin încheierea organismului de supraveghere, care pune capăt procedurii fără a stabili o încălcare, dar cu obligația de a corecta comportamentul.

(4) Investigarea se dispune atunci când, în urma examinării preliminare, există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi. În celelalte cazuri, etapa investigării este omisă.

Articolul 73. Examinarea preliminară a plângerii

(1) Plângerea depusă la organismul de supraveghere privind presupuse încălcări ale prezentei legi conține:

a) datele de identificare ale autorului plângerii (numele, prenumele sau denumirea, adresa sau sediul, adresa de poștă electronică);

b) specificarea circumstanțelor de fapt și de drept referitoare la pretinsa încălcare a prezentei legi;

c) informații care permit identificarea prestatorului de servicii de încredere sau a furnizorului de portofele pentru identitatea digitală vizat, în măsura în care este posibil;

d) măsurile solicitate a fi întreprinse de organismul de supraveghere;

e) după caz, informații privind adresările înaintate prestatorului sau furnizorului, precum și rezultatul acestora;

f) semnătura autorului plângerii sau a reprezentantului acestuia, iar în cazul plângerilor transmise în formă electronică – semnătura electronică.

(2) Examinarea preliminară a plângerii se efectuează în termen de 30 de zile de la data înregistrării. În cadrul acesteia, organismul de supraveghere determină dacă există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi.

(3) Plângerile anonime sau cele depuse fără indicarea datelor de contact ale autorului nu se examinează.

(4) În cazul în care consideră că, în baza informațiilor prezentate, nu există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi, organismul de

supraveghere respinge motivat plângerea și informează autorul cu privire la acest fapt.

Articolul 74. Investigarea

(1) Investigarea reprezintă activitatea de colectare și administrare a informațiilor privind legalitatea activității prestatorilor de servicii de încredere și a furnizorilor de portofele pentru identitatea digitală, acumulate în condițiile prezentei legi.

(2) Dacă după examinarea preliminară se constată că există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi, organismul de supraveghere emite o dispoziție de inițiere a investigării.

(3) Investigările din oficiu se pot efectua:

a) ca urmare a transmiterii notificărilor privind încălcarea securității sistemelor sau serviciilor de încredere;

b) în baza informațiilor privind presupuse încălcări ale prezentei legi obținute din alte surse, cum ar fi sesizările altor autorități publice, mass-media, rapoarte de audit ale conformității sau orice alte informații care indică în mod rezonabil o posibilă încălcare;

c) în vederea cooperării internaționale în domeniul serviciilor de încredere și al identificării electronice.

(4) La efectuarea investigării, organismul de supraveghere are dreptul:

a) să solicite și să obțină accesul la toate documentele, informațiile, sistemele informatice și datele necesare pentru efectuarea investigării;

b) să solicite și să primească explicații și documente de la prestatorul de servicii de încredere sau furnizorul de portofele pentru identitatea digitală supus investigării, într-un termen stabilit în funcție de complexitatea solicitării;

c) să efectueze inspecții la sediul prestatorului sau furnizorului supus investigării, în prezența acestuia sau a reprezentantului său, în orele de program, în baza unei delegații de efectuare a investigării;

d) să audieze persoana supusă investigării sau reprezentantul legal al acesteia asupra faptelor relevante pentru obiectul investigării și, după caz, să înregistreze răspunsurile acestora, cu informarea prealabilă a persoanei audiate;

e) să solicite sprijinul altor autorități competente pentru efectuarea investigării.

(5) Pe parcursul efectuării investigării, persoana supusă investigării are dreptul:

a) să obțină o copie a delegației de efectuare a investigării;

b) să prezinte probe și explicații referitoare la obiectul investigării;

c) să fie asistată de avocați sau de alți reprezentanți împuterniciți conform legislației;

d) să conteste deciziile organismului de supraveghere în instanța de judecată competentă.

(6) Toate persoanele juridice de drept public sau de drept privat și persoanele fizice sunt obligate să se supună investigării efectuate de către organismul de supraveghere, inclusiv prin asigurarea condițiilor pentru buna desfășurare a acesteia.

(7) Termenul de efectuare a investigării este de până la 6 luni de la data inițierii, cu posibilitatea prelungirii justificate cu câte o lună, dar nu mai mult de 12 luni de la data inițierii, în funcție de complexitatea cauzei, de volumul de informații ce urmează a fi obținute și examinate și de comportamentul participanților la procedura de investigare.

(8) Rezultatul investigării este consemnat într-un proiect de decizie, care prevede constatarea sau lipsa încălcării, măsurile corective și sancțiunile aplicabile. Proiectul de decizie se comunică persoanei supuse investigării, cu acordarea unui termen de 30 de zile pentru înaintarea unor eventuale obiecții.

(9) Confidențialitatea informațiilor obținute pe parcursul investigării este asigurată de către personalul organismului de supraveghere implicat în procedură.

Articolul 75. Emiterea și comunicarea deciziilor

(1) La finalizarea investigării, organismul de supraveghere emite decizia motivată cu privire la constatarea sau lipsa încălcării prezentei legi și cu privire la aplicarea măsurilor corective și a sancțiunilor, după caz.

(2) Decizia se comunică persoanei supuse investigării în termen de 10 zile lucrătoare de la data emiterii.

(3) Deciziile organismului de supraveghere pot fi contestate direct în instanța de judecată competentă, conform Codului administrativ al Republicii Moldova nr. 116/2018, fără respectarea procedurii prealabile.

(4) Organismul de supraveghere publică rezumatul deciziilor emise, în care reflectă natura încălcărilor depistate, motivarea deciziei, măsurile dispuse, precum și sancțiunile aplicate.

Articolul 76. Executarea deciziilor organismului de supraveghere

(1) Deciziile organismului de supraveghere se execută în termenul menționat în ele, cu obligația persoanei supuse investigării de a informa în scris organismul de supraveghere cu privire la măsurile întreprinse.

(2) Termenul de executare benevolă a amenzii este de cel mult 3 luni de la data comunicării deciziei.

(3) Deciziile organismului de supraveghere se execută silit în conformitate cu prevederile Codului de executare al Republicii Moldova nr. 443/2004.

Secțiunea a 3-a
Sancțiunile pecuniare

Articolul 77. Amenda

(1) Amenda reprezintă sancțiunea pecuniară aplicată de către organismul de supraveghere prestatorilor de servicii de încredere sau furnizorilor de portofele pentru identitatea digitală în cazul constatării unei încălcări a prezentei legi.

(2) Amenda aplicată de organismul de supraveghere se varsă la bugetul de stat.

Articolul 78. Condiții generale pentru aplicarea amenzilor

(1) Organismul de supraveghere asigură că aplicarea amenzilor este, în fiecare caz, eficace și proporțională.

(2) În funcție de circumstanțe, amenzile sunt aplicate în completarea sau în locul altor măsuri corective. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi aplicată ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi.

(3) În scopul aplicării unei amenzi, precum și al determinării cuantumului acesteia, se iau în considerare, în fiecare caz particular, următoarele circumstanțe:

a) natura, gravitatea și durata încălcării, ținându-se seama de domeniul de aplicare sau scopul serviciului în cauză, precum și de numărul persoanelor afectate și de nivelul prejudiciilor suferite de acestea;

b) dacă încălcarea a fost comisă intenționat sau din neglijență;

c) orice acțiuni întreprinse de către prestatorul de servicii de încredere sau furnizorul de portofele pentru identitatea digitală pentru a reduce prejudiciul suferit de persoanele afectate;

d) gradul de responsabilitate al prestatorului de servicii de încredere sau al furnizorului de portofele pentru identitatea digitală, ținându-se seama de măsurile tehnice și organizaționale implementate;

e) eventualele încălcări anterioare relevante comise de prestatorul de servicii de încredere sau de furnizorul de portofele pentru identitatea digitală;

f) gradul de cooperare cu organismul de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale acesteia;

g) modul în care încălcarea a fost adusă la cunoștința organismului de supraveghere, în special dacă și în ce măsură prestatorul de servicii de încredere sau furnizorul de portofele pentru identitatea digitală a notificat cu privire la încălcare;

h) în cazul în care au fost dispuse anterior măsuri corective împotriva prestatorului sau furnizorului cu privire la același obiect, respectarea măsurilor respective;

i) aderarea la standarde tehnice europene și internaționale aplicabile în domeniu; și

j) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(4) Amenzile pot fi aplicate numai dacă se stabilește că prestatorul de servicii de încredere sau furnizorul de portofele pentru identitatea digitală a săvârșit intenționat sau din neglijență o încălcare prevăzută la art. 79.

(5) În cazul în care un prestator sau furnizor încalcă în mod intenționat sau din neglijență, pentru aceeași activitate sau activități conexe, mai multe dispoziții din prezenta lege, cuantumul total al amenzii nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

Articolul 79. Încălcările pasibile de amendă

(1) În conformitate cu art. 78, se aplică amenzi de până la 1 000 000 de lei sau, în cazul unei întreprinderi, de până la 0,5 % din cifra totală de afaceri realizată în exercițiul financiar anterior, luându-se în calcul cea mai mare valoare, pentru încălcarea următoarelor obligații de natură formală și procedurală:

1) de către furnizorii de portofele pentru identitatea digitală:

a) furnizarea unui portofel pentru identitatea digitală care nu îndeplinește cerințele tehnice și de securitate prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia, inclusiv cerințele privind nivelul de asigurare;

b) nerespectarea obligațiilor privind interoperabilitatea cu alte portofele pentru identitatea digitală recunoscute, inclusiv cu cele emise de statele membre ale Uniunii Europene;

c) nerespectarea cerințelor privind controlul utilizatorului asupra datelor proprii, inclusiv a dreptului de divulgare selectivă a datelor și a dreptului de acces la istoricul tranzacțiilor;

d) utilizarea datelor de identificare personală ale utilizatorilor în alt scop decât cel declarat sau fără consimțământul explicit al utilizatorului;

e) neasigurarea funcționalității tabloului de bord prevăzut de prezenta lege, care permite utilizatorilor să monitorizeze și să gestioneze accesul beneficiarilor la datele lor;

f) nefurnizarea sau furnizarea inexactă a informațiilor solicitate de organismul de supraveghere în exercitarea atribuțiilor de supraveghere;

g) nerespectarea obligației de a facilita exercitarea atribuțiilor de control de către personalul organismului de supraveghere, împuternicit în acest sens;

h) omiterea notificării obligatorii a incidentelor de securitate semnificative către organismul de supraveghere și, după caz, către utilizatorii afectați, în termenele prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

i) nerespectarea obligațiilor de raportare periodică față de organismul de supraveghere, prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia;

2) de către prestatorii de servicii de încredere calificați:

a) nerespectarea obligației de păstrare a documentației aferente certificatelor emise pe perioada minimă prevăzută de prezenta lege și de actele normative adoptate în aplicarea acesteia;

b) nerespectarea cerințelor privind stocarea certificatelor în forma și condițiile prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

c) emiterea certificatelor prezentate utilizatorilor ca fiind calificate, care nu conțin mențiunile obligatorii prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia, ori care conțin informații inexacte;

d) emiterea certificatelor calificate fără verificarea identității solicitantului în condițiile prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia;

e) nerespectarea obligației de a nu stoca, reproduce sau dezvălui terților datele de creare a semnăturilor sau sigiliilor electronice fără consimțământul expres al semnatarului sau al creatorului sigiliului;

f) neluarea măsurilor necesare pentru asigurarea confidențialității în cursul procesului de generare a datelor pentru crearea semnăturilor sau sigiliilor electronice;

g) nerespectarea obligației de a revoca certificatele calificate în cazurile și în termenele prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

h) divulgarea identității reale a titularului certificatului cu pseudonim, cu încălcarea obligațiilor de confidențialitate prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

i) utilizarea dispozitivelor de creare a semnăturilor sau sigiliilor electronice care nu respectă cerințele prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia, în cazul în care certificatul specifică faptul că este emis pe un astfel de dispozitiv;

j) omiterea de a lua măsurile necesare pentru asigurarea conservării arhivei proprii și a revocării certificatelor, în cazul în care prestatorul se află în una dintre situațiile de încetare a activității prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

k) nefurnizarea sau furnizarea inexactă a informațiilor solicitate de organismul de supraveghere în exercitarea atribuțiilor de supraveghere;

l) nerespectarea obligației de a facilita exercitarea atribuțiilor de control de către personalul organismului de supraveghere, împuternicit în acest sens;

m) omiterea notificării obligatorii a incidentelor de securitate semnificative către organismul de supraveghere și, după caz, către utilizatorii afectați, în termenele prevăzute de lege și de actele normative adoptate în aplicarea acesteia;

n) nerespectarea obligațiilor de raportare periodică față de organismul de supraveghere, prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia;

3) de către prestatorii de servicii de încredere necalificați:

a) prestarea serviciilor de încredere fără respectarea cerințelor tehnice minime prevăzute de prezenta lege și de actele normative adoptate în aplicarea acesteia;

b) nerespectarea obligațiilor privind informarea utilizatorilor cu privire la natura, limitele și condițiile serviciilor prestate, inclusiv cu privire la faptul că serviciul nu are statut calificat;

c) nerespectarea obligațiilor privind gestionarea cheilor criptografice și a datelor de creare a semnăturilor sau sigiliilor electronice.

(2) În conformitate cu art. 78, se aplică amenzi de până la 2 000 000 de lei sau, în cazul unei întreprinderi, de până la 0,75 % din cifra totală de afaceri realizată în exercițiul financiar anterior, luându-se în calcul cea mai mare valoare, pentru încălcarea următoarelor obligații de natură tehnică și operațională de către furnizorii de portofele pentru identitatea digitală și prestatorii de servicii de încredere, calificați sau necalificați:

a) continuarea desfășurării activității după ce organismul de supraveghere a dispus încetarea acesteia;

b) utilizarea frauduloasă sau nelegitimă a calității de prestator de servicii de încredere calificat sau de furnizor de portofele pentru identitatea digitală certificat;

c) împiedicarea exercitării atribuțiilor de control ale organismului de supraveghere;

d) nerespectarea măsurilor corective dispuse de către organismul de supraveghere în termenul stabilit prin decizie;

e) nerespectarea obligațiilor privind securitatea sistemelor și serviciilor, care a condus la un incident de securitate major cu impact asupra unui număr semnificativ de utilizatori;

f) nerespectarea obligațiilor privind protecția datelor cu caracter personal ale utilizatorilor în cadrul furnizării serviciilor reglementate de prezenta lege, în special în cazul în care încălcarea a condus la accesul neautorizat la date de identificare personală sau la atestate electronice ale atributelor.

(3) Fără a aduce atingere competențelor corective ale organismului de supraveghere, sancțiunile prevăzute de prezentul articol se aplică și autorităților și instituțiilor publice care acționează în calitate de furnizori de portofele pentru identitatea digitală sau de prestatori de servicii de încredere.

(4) În cazul în care cifra totală de afaceri realizată în exercițiul financiar anterior nu este înregistrată, se ia în considerare ultimul exercițiu financiar anterior în care entitatea a realizat o cifră de afaceri.

Capitolul VII
DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 80. Dispoziții finale

(1) Prezenta lege intră în vigoare la expirarea a 12 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Guvernul:

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, a organismului de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere, precum și a organismului din sectorul public responsabil de furnizarea portofelului pentru identitatea digitală;

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 12 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 pentru punerea 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 (Monitorul Oficial al Republicii Moldova, 2022, nr. 170-176, art. 317), cu modificările ulterioare.

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

(5) Organismele din sectorul public deținătoare de surse autentice asigură conformitatea cu obligațiile prevăzute la art. 55 și 56 în termen de 24 de luni de la data intrării în vigoare a prezentei legi, în limitele resurselor financiare alocate sau atrase în acest scop.

(6) Costurile dezvoltării și mentenanței mecanismelor electronice prevăzute la alin. (4) și (5) se acoperă din contul și limitele mijloacelor financiare aprobate anual în bugetul autorităților/instituțiilor responsabile sau din alte surse, neinterzise de lege.

Articolul 81. 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 prezentei legi.

(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.

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

(4) Sistemele de identificare electronică existente la data intrării în vigoare a prezentei legi, inclusiv sistemul național de identificare electronică bazat pe

cartea de identitate emisă în temeiul Legii nr. 273/1994 privind actele de identitate din sistemul național de pașapoarte, urmează a fi notificate organismului de supraveghere, în conformitate cu art. 13, în termen de 12 luni de la data intrării în vigoare a prezentei legi.

(5) Actele normative emise în temeiul Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere rămân aplicabile, în măsura în care nu contravin prezentei legi, până la adoptarea actelor normative noi corespunzătoare.

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 - CELEX: 32014R0910), 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 - CELEX: 02014R0910-20241018). 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 și al angajamentelor specifice asumate în procesul de aderare.

Transpunerea prevederilor Regulamentului (UE) nr. 910/2014 este prevăzută în Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru anii 2025-2027, aprobată prin Hotărârea Guvernului nr.260/2025, la Pilonul 2: Conectivitate și infrastructură digitală, măsura 10, urmând ca legea care asigură conformitatea deplină cu cadrul de identitate al UE (eIDAS 2) să fie adoptată până în decembrie 2026.

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, cu atribuții pentru organismul de supraveghere desemnat de Guvern, și stabilește un regim sancționator proporțional 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 emitentilor 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 capacității instituționale în acest domeniu. Potrivit art. 64 alin. (1) din proiectul de lege, organismul de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere este desemnat de Guvern, care stabilește și modul de organizare și funcționare a acestuia. Organismul de supraveghere exercită 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, potrivit art. 65, 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.

Până la intrarea în vigoare a legii, atribuțiile de supraveghere în domeniul serviciilor de încredere continuă să fie exercitate de Serviciul de Informații și Securitate, în temeiul Legii nr. 124/2022. Întrucât desemnarea se face în termen de 3 luni de la publicarea legii, iar legea intră în vigoare la 12 luni de la publicare, organismul desemnat dispune de timpul necesar pentru pregătirea preluării atribuțiilor, inclusiv a listei de încredere naționale și a evidențelor privind prestatorii calificați, fără întreruperea supravegherii.

Totodată, proiectul de lege la art. 80 alin. (2) lit. a) prevede obligația Guvernului ca, într-un termen de 3 luni de la publicarea legii, să întreprindă măsurile necesare pentru desemnarea:

- autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul identificării electronice și serviciilor de încredere;
- organismului de supraveghere a cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere;

• organismului din sectorul public responsabil de furnizarea unui portofel pentru identitatea digitală.

Prevederea respectivă are rolul de a asigura existența cadrului instituțional necesar pentru implementarea efectivă a noii legi și pentru realizarea obligațiilor asumate de Republica Moldova în contextul armonizării cu Regulamentul (UE) nr. 910/2014 (eIDAS) și cadrul european privind portofelele pentru identitatea digitală.

Stabilirea expresă a acestor entități la nivelul actelor Guvernului este necesară pentru delimitarea responsabilităților instituționale, coordonarea implementării cadrului normativ și asigurarea unui mecanism de guvernanță în domeniul identității digitale.

Preliminar, având în vedere domeniile sale de activitate, competențele funcționale, expertiza acumulată și experiența existentă în domeniul transformării digitale și al guvernării electronice, autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat urmează a fi propus Ministerul Dezvoltării Economice și Digitalizării.

Ministerul exercită deja, într-o formă funcțională, atribuții aferente politicilor de digitalizare și coordonării proceselor de transformare digitală la nivel național, inclusiv în domeniul serviciilor publice electronice, interoperabilității, identității electronice și infrastructurilor digitale guvernamentale. În acest context, atribuirea formală a acestui mandat reprezintă o continuare firească a competențelor și responsabilităților deja exercitate la nivel instituțional.

Totodată, organismul din sectorul public responsabil de furnizarea unui portofel pentru identitatea digitală urmează a fi propusă Agenția de Guvernare Electronică. Alegerea acestei instituții are la bază experiența tehnică și operațională deja existentă în dezvoltarea și administrarea infrastructurilor digitale guvernamentale și a platformelor naționale de servicii electronice.

În mod particular, Agenția de Guvernare Electronică a dezvoltat aplicația EVO, care reprezintă un instrument precursor al conceptului de portofel pentru identitatea digitală și care dispune deja de funcționalități relevante pentru ecosistemul viitor al portofelelor digitale, inclusiv module pentru generarea, stocarea, prezentarea și gestionarea documentelor electronice.

De asemenea, AGE a dezvoltat și aplicația EVOSign, utilizată în prezent pentru autentificarea utilizatorilor în cadrul sistemelor informaționale și serviciilor electronice, soluție care demonstrează experiența instituțională și capacitatea tehnică existentă în domeniul mecanismelor de identificare și autentificare electronică.

În prezent, aplicația EVO se află într-un proces continuu de modernizare și ajustare tehnică, în vederea alinierii acesteia la cerințele stabilite de Uniunea Europeană pentru portofelele pentru identitatea digitală.

Totodată, modernizarea aplicației EVO în vederea furnizării acesteia în calitate de portofel pentru identitatea digitală reprezintă parte a angajamentelor asumate de Republica Moldova în procesul de integrare europeană și de armonizare graduală cu cadrul normativ și tehnologic al Uniunii Europene în domeniul identității digitale și al serviciilor de încredere. Aceste acțiuni se înscriu în efortul Guvernului de a asigura cetățenilor și mediului de afaceri acces la o soluție modernă, securizată, interoperabilă și compatibilă cu politica Uniunii Europene în materie de portofele europene pentru identitatea digitală.

În conformitate cu Măsura nr.10 Reforma nr.3 Pilonul 2 din Anexa 1 a Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025-2027, aprobată prin Hotărârea Guvernului nr.60/2025, Măsura 15.2 din Foaia de parcurs privind „Reforma administrației publice" (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană), aprobată prin Hotărârea Guvernului nr.274/2025, dar și Acțiunea 7 Anexa B Capitolul 10 din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr.306/2025, până la sfârșitul anului 2027, AGE urmează să asigure implementarea unei soluții de portofel pentru identitatea digitală în conformitate cu eIDAS 2.0 (Regulamentul UE 2024/1183).

Opțiunea de valorificare și dezvoltare a infrastructurii și soluțiilor deja existente la nivel național urmărește asigurarea unei implementări eficiente și sustenabile, inclusiv prin reutilizarea expertizei instituționale, a componentelor tehnologice existente și a investițiilor deja realizate de stat în domeniul serviciilor digitale guvernamentale. În acest context, aplicația EVO și infrastructura tehnologică aferentă constituie o bază funcțională relevantă pentru dezvoltarea portofelului pentru identitatea digitală, reducând semnificativ costurile, termenii și complexitatea implementării unei soluții complet noi.

De asemenea, reutilizarea soluțiilor existente permite asigurarea continuității serviciilor digitale deja utilizate de cetățeni, facilitarea integrării cu infrastructura guvernamentală existentă, precum și accelerarea procesului de conformare la standardele și specificațiile tehnice europene aplicabile portofelelor pentru identitatea digitală. În același timp, această abordare contribuie la consolidarea capacităților instituționale și tehnice deja dezvoltate la nivel național și la utilizarea eficientă a resurselor publice disponibile.

După finalizarea procesului de modernizare și ajustare la cerințele prevăzute de lege și de standardele europene aplicabile, aplicația EVO urmează să fie supusă procedurilor de evaluare a conformității și certificare în calitate de portofel pentru identitatea digitală, în conformitate cu cerințele stabilite de cadrul normativ național și actele de implementare adoptate de Comisia Europeană. Acest proces va include inclusiv verificarea conformității cu standardele tehnice și de securitate aplicabile, cerințele privind protecția datelor cu caracter personal, interoperabilitatea și mecanismele de autentificare și validare prevăzute de cadrul european eIDAS.

Astfel, soluția instituțională avută în vedere urmărește valorificarea infrastructurii, competențelor și investițiilor deja existente la nivel național, evitarea dublicării capacităților administrative și tehnice și asigurarea unei implementări graduale a ecosistemului portofelelor pentru identitatea digitală în Republica Moldova.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea proiectului de lege nu generează, în mod direct, cheltuieli imediate și obligatorii din bugetul de stat la etapa adoptării cadrului normativ, întrucât legea are caracter de stabilire a cadrului juridic și instituțional necesar transpunerii cerințelor Regulamentului (UE) nr. 910/2014 și a modificărilor ulterioare privind identitatea digitală și serviciile de încredere.

Adoptarea prezentei legi nu implică, în sine, angajamente financiare directe și imediate la momentul intrării sale în vigoare. Impactul bugetar urmează a fi materializat

în fazele ulterioare de implementare operațională a infrastructurii digitale asociate, pe măsură ce sunt elaborate și aprobate documentațiile tehnice și normative subsecvente.

Eventualele costuri financiare apar în faza de implementare graduală și operaționalizare a infrastructurii digitale aferente, fiind corelate cu complexitatea tehnică a soluțiilor ce urmează a fi dezvoltate și integrate la nivel național. Acestea vor fi determinate de necesitatea asigurării interoperabilității, securității și conformității cu standardele europene aplicabile portofelelor pentru identitatea digitală.

Cheltuielile estimate acoperă următoarele domenii prioritare de intervenție:

1. Dezvoltarea și modernizarea infrastructurii tehnice naționale, inclusiv implementarea portofelului pentru identitatea digitala, a componentelor de autentificare, semnare electronică și gestionare a atributelor digitale;
2. Integrarea sistemelor informaționale ale autorităților publice cu infrastructura de identitate digitală și cu mecanismele de verificare a atributelor din surse autentice;
3. Dezvoltarea interfețelor electronice de tip „attribute attestation API", necesare pentru implementarea art. 55 alin. (1) din proiectul de lege, inclusiv infrastructura de expunere și verificare a atributelor din surse autentice, conform standardelor europene aplicabile (OpenID for Verifiable Credentials, standarde ISO/IEC);
4. Certificarea, auditarea și testarea periodică a conformității, inclusiv evaluări de securitate și recertificări ale componentelor critice;
5. Participarea la ecosistemul european de interoperabilitate, inclusiv activități de pilotare și integrare transfrontalieră în cadrul proiectelor-pilot EUDI Wallet.

Pentru perioada 2026–2030, costurile estimate aferente dezvoltării, implementării, operaționalizării și mentenanței Portofelului pentru identitatea digitală care urmează a fi furnizat de Guvern, prin intermediul Agenției de Guvernare Electronică sunt evaluate la aproximativ 63,5 mil. lei, în conformitate cu necesarul financiar estimat în cadrul Planului de creștere pentru Republica Moldova.

Cheltuielile estimate reflectă atât investițiile inițiale necesare pentru dezvoltarea și punerea în funcțiune a infrastructurii tehnice, cât și costurile recurente asociate operării continue, securității și conformității sistemului cu standardele europene aplicabile în domeniul identificării electronice și serviciilor de încredere. Totodată, costurile estimate includ cheltuieli aferente modernizărilor periodice ale soluției, necesare pentru adaptarea continuă la evoluțiile tehnologice, schimbările cadrului normativ european și cerințele de interoperabilitate digitală.

Pentru perioada 2027–2030, necesarul financiar estimat este în cuantum total de cca 63.483.560 lei, distribuit anual după cum urmează:

- 2027 – 16.698.951 lei;
- 2028 – 14.079.667 lei;
- 2029 – 17.182.116 lei;
- 2030 – 15.522.826 lei.

Pentru anul 2026, sunt deja aprobate resurse financiare în valoare de 2,2 mil. lei, planificate spre finanțare din resursele Planului de creștere pentru Republica Moldova, destinate achiziționării licențelor SAM (Secure Application Module) necesare dezvoltării funcționalităților de semnătură electronică la distanță, componentă esențială a ecosistemului Portofelului pentru identitatea digitală.

Se estimează că implementarea investițiilor respective va permite dezvoltarea unei infrastructuri digitale sigure, interoperabile și conforme cu cerințele europene în materie de identificare electronică și servicii de încredere, contribuind la creșterea gradului de digitalizare a serviciilor publice și private, reducerea costurilor administrative și facilitarea accesului utilizatorilor la servicii digitale securizate.

Tot în context, art. 55 alin. (1) din proiectul legii instituie obligația organismelor din sectorul public care gestionează registre de stat sau alte sisteme informaționale ce constituie surse autentice de date de a asigura disponibilitatea mecanismelor electronice care permit verificarea atributelor la cererea expresă a utilizatorului.

Implementarea acestei obligații presupune dezvoltarea unor interfețe electronice noi de tip „attribute attestation API", conforme cu standardele și arhitecturile europene relevante (inclusiv OpenID for Verifiable Credentials și standarde ISO/IEC aplicabile), ceea ce implică un efort tehnic diferențiat în funcție de gradul de digitalizare și maturitate tehnologică al fiecărui registru sau sistem informațional.

În procesul de elaborare a cadrului normativ subsecvent necesar implementării legii va fi evaluată situația actuală și nivelul de pregătire al fiecărui organism public deținător de surse autentice, în vederea stabilirii modului optim de conformare la prevederile art. 55.

Totodată, în funcție de capacitățile tehnice existente și necesitățile de modernizare, vor fi evaluate și resursele financiare și operaționale necesare pentru dezvoltarea interfețelor electronice aferente, astfel încât implementarea să fie realizată gradual, proporțional și sustenabil.

Costurile aferente organizării și funcționării organismului de supraveghere, inclusiv pentru exercitarea noilor atribuții în domeniul portofelelor pentru identitatea digitală, vor fi estimate la elaborarea hotărârii Guvernului privind desemnarea acestuia și stabilirea modului său de organizare și funcționare, în funcție de soluția instituțională aleasă și de capacitățile existente ale instituției desemnate.

4.3 Impactul asupra sectorului privat

Proiectul de lege va genera un impact multidimensional asupra sectorului privat, prin instituirea unui cadru juridic modern și previzibil pentru utilizarea identității digitale și a serviciilor de încredere în relațiile comerciale și juridice. Principalii subiecți vizați de efectele legii fiind:

1. Prestatorii de servicii de încredere calificați

La momentul elaborării prezentului proiect de lege, pe piața Republicii Moldova activează un singur prestator de servicii de încredere calificat, Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică (STISC). STISC este o instituție publică fondată de Guvernul Republicii Moldova și nu un operator privat de piață, ceea ce determină o analiză de impact orientată preponderent pe componenta instituțională și de consolidare a capacităților publice, mai degrabă decât pe efecte concurențiale.

În acest context, impactul proiectului asupra STISC este, în ansamblu, preponderent pozitiv pe termen mediu și lung. Noua lege creează un cadru normativ mai coerent, aliniat standardelor europene în materie de servicii de încredere, ceea ce contribuie la consolidarea rolului instituțional al prestatorului existent, la creșterea nivelului de încredere în serviciile furnizate și la extinderea portofoliului de servicii digitale calificate. Totodată, cadrul legal actualizat permite o mai bună integrare a STISC în ecosistemul

național și european al serviciilor de încredere, inclusiv prin facilitarea interoperabilității și recunoașterii transfrontaliere.

Totodată, legea creează premise pentru eficientizarea pe termen mediu a costurilor operaționale prin standardizare, automatizare și reducerea fragmentării serviciilor de încredere. Prin alinierea la cadrul european eIDAS, se facilitează accesul la piața unică digitală și creșterea potențialului de furnizare a serviciilor transfrontaliere, ceea ce poate genera, pe termen lung, noi oportunități de dezvoltare instituțională și venituri conexe pentru prestatorul calificat. De asemenea, este relevant de menționat că noul cadru normativ stimulează dezvoltarea ecosistemului național de servicii de încredere prin deschiderea pieței către noi actori calificați, ceea ce va contribui la creșterea competitivității, diversificarea serviciilor și reducerea riscurilor asociate concentrării unui singur furnizor. În acest sens, STISC va avea oportunitatea de a-și consolida rolul de actor strategic în domeniu, inclusiv prin participarea la proiecte naționale și europene de interoperabilitate și inovare digitală.

2. Potențialii prestatori de servicii de încredere calificați, inclusiv din Uniunea Europeană

Pentru potențialii prestatori de servicii de încredere calificați, proiectul de lege are un efect structural de liberalizare a pieței, prin crearea unui cadru normativ armonizat cu Regulamentul (UE) nr. 910/2014 (eIDAS). Această deschidere generează premisele apariției unei piețe funcționale, competitive și interoperabile, în care prestatorii pot intra pe baza unor reguli unitare și transparente.

Un element esențial al arhitecturii juridice propuse îl constituie mecanismul de recunoaștere automată a prestatorilor calificați din statele membre ale Uniunii Europene, prevăzut la art. 22 alin. (6) și (7) din proiectul de lege. Acesta instituie o abordare de tip *„mutual recognition by default”*, în temeiul căreia prestatorii deja calificați în cadrul eIDAS își păstrează statutul și pe teritoriul Republicii Moldova fără parcurgerea unor proceduri suplimentare de autorizare sau verificare. Din perspectivă operațională, acest mecanism reduce semnificativ barierele de intrare pentru actorii europeni, asigurând integrarea rapidă în piața națională și interoperabilitatea imediată cu infrastructura existentă.

În același timp, această deschidere generează un efect de accelerare a maturizării pieței locale, prin introducerea unor standarde ridicate de calitate, securitate și conformitate, deja consolidate la nivelul Uniunii Europene. Prestatorii europeni calificați beneficiază astfel de un avantaj competitiv structural, determinat de recunoașterea automată și eliminarea costurilor de conformare inițială, ceea ce poate stimula concurența și transferul de know-how către ecosistemul național.

Pe de altă parte, noii prestatori autohtoni vor avea oportunitatea de a accesa o piață aflată în formare, cu un potențial semnificativ de creștere, inclusiv determinat de digitalizarea accelerată a serviciilor publice și private. În acest sens, legea instituie o serie de domenii emergente, anterior nereglementate sau insuficient dezvoltate, precum serviciile de atestare electronică a atributelor, arhivarea electronică calificată, registrele electronice calificate și serviciile de distribuție electronică înregistrată calificată. Aceste segmente reprezintă nișe de piață cu potențial ridicat de dezvoltare, în care pot fi atrase investiții și competențe tehnice specializate.

Totodată, extinderea utilizării portofelului pentru identitatea digitală și obligația progresivă de integrare a actorilor economici în ecosistemul digital vor genera o cerere

constantă pentru servicii de încredere calificate, inclusiv servicii de semnare, autentificare, verificare a atributelor și gestionare a identității digitale. Această cerere va constitui un factor stabilizator și de creștere pentru piață.

Pentru potențialii prestatori autohtoni, intrarea pe piață este condiționată de parcurgerea procedurii complete de calificare, care implică evaluarea conformității de către organisme de evaluare a conformității acreditate, implementarea standardelor de securitate și interoperabilitate și respectarea cerințelor privind continuitatea serviciului. Aceste cerințe, deși implică investiții inițiale semnificative, sunt necesare pentru asigurarea unui nivel uniform de încredere și securitate la nivel național și pentru compatibilitatea cu spațiul digital european.

În același timp, cadrul normativ nu are un efect prohibitiv, ci unul de standardizare progresivă, în sensul în care oferă claritate asupra condițiilor de acces pe piață, reducând incertitudinea juridică și riscurile investiționale. Prestatorii care intră pe piață beneficiază de un cadru stabil, previzibil și armonizat cu standardele europene (ETSI, ISO/IEC), ceea ce facilitează planificarea investițiilor și dezvoltarea de servicii scalabile.

Impactul net asupra potențialilor prestatori de servicii de încredere calificate este, în ansamblu, pozitiv. Legea contribuie la crearea unei piețe competitive, deschise și interoperabile, în care prestatorii din Uniunea Europeană pot intra rapid prin mecanismul de recunoaștere automată, iar prestatorii autohtoni au posibilitatea de a se dezvolta într-un cadru predictibil și aliniat standardelor europene. Pe termen mediu și lung, se anticipează consolidarea unei piețe diversificate, cu efecte benefice asupra calității serviciilor, reducerii costurilor pentru utilizatori și accelerării transformării digitale a economiei și administrației publice.

3. Potențialii furnizori de portofele pentru identitatea digitală

Reglementarea portofelelor pentru identitatea digitală este introdusă pentru prima dată în cadrul normativ național prin prezentul proiect de lege, în contextul procesului de aliniere a Republicii Moldova la cadrul european privind identitatea digitală și serviciile de încredere. La momentul adoptării, nu există pe piața națională soluții comerciale mature care să corespundă integral cerințelor funcționale, de securitate și interoperabilitate specifice portofelelor pentru identitate digitală, astfel cum sunt acestea configurate la nivelul Uniunii Europene prin Regulamentul (UE) 2024/1183 (eIDAS 2.0). În consecință, legea nu intervine asupra unei piețe existente, ci creează un ecosistem nou, aflat în fază incipientă de formare.

Articolul 5 alin. (2) stabilește în mod expres că portofelele pentru identitatea digitală pot fi furnizate atât de un organism din sectorul public desemnat de Guvern, cât și de persoane juridice de drept privat, cu respectarea cerințelor prevăzute de lege. Această abordare consacră un model de piață deschisă, bazat pe concurență reglementată, în care rolul statului este de a asigura cadrul de interoperabilitate, securitate și certificare, fără a restricționa accesul operatorilor privați.

În același timp, principiul liberei alegeri a utilizatorului, prevăzut expres la art. 5 alin. (2), are un rol structural în configurarea pieței: utilizatorii nu sunt condiționați de utilizarea unui anumit furnizor, iar selecția portofelului se realizează în funcție de nevoile, nivelul de încredere și funcționalitățile oferite. Acest principiu este esențial pentru evitarea concentrării artificiale a pieței și pentru stimularea inovării tehnologice.

Din perspectiva potențialilor furnizori privați, cadrul juridic instituit creează o piață nouă, cu unele bariere de intrare inițiale determinate de cerințele de securitate, certificare, interoperabilitate și conformitate cu standardele europene. Totuși, aceste cerințe sunt justificate de natura critică a serviciului, portofelul reprezentând un instrument central în ecosistemul de identitate digitală, cu impact direct asupra accesului la servicii publice și private.

În același timp, proiectul de lege oferă un avantaj competitiv furnizorilor care se aliniază rapid standardelor tehnice și cerințelor de certificare, aceștia având posibilitatea de a ocupa o poziție consolidată într-o piață emergentă. Deschiderea pieței către sectorul privat, inclusiv în contextul compatibilității cu soluțiile europene de tip eIDAS 2.0, permite atragerea investițiilor, transfer de know-how și dezvoltarea unor produse digitale competitive la nivel regional.

Un element esențial al acestui ecosistem cu potențial impact asupra pieții îl constituie soluția de portofel pentru identitatea digitală care urmează a fi furnizată de Guvern prin intermediul Agenției de Guvernare Electronică. Această soluție reprezintă o componentă importantă a infrastructurii naționale de identitate digitală și are rolul de a asigura continuitatea serviciului public, în condiții de acces universal, securitate și încredere.

În acest sens, implementarea portofelului respectiv nu este o opțiune discreționară, ci rezultă din angajamentele asumate de Republica Moldova în cadrul procesului de integrare europeană. Astfel, în conformitate cu Măsura nr. 10, Reforma nr. 3, Pilonul 2 din Anexa 1 a Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027, aprobată prin Hotărârea Guvernului nr. 60/2025, precum și cu Măsura 15.2 din Foaia de parcurs privind Reforma administrației publice (criteriu de referință în procesul de aderare la Uniunea Europeană), aprobată prin Hotărârea Guvernului nr. 274/2025, și Acțiunea 7 din Anexa B, Capitolul 10 al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025, Republica Moldova s-a angajat ca, până la sfârșitul anului 2027, Agenția de Guvernare Electronică să asigure implementarea unei soluții de portofel pentru identitatea digitală aliniate standardelor eIDAS 2.0.

În acest context, soluția guvernamentală EVO (inclusiv componentele sale, precum EVOSign), dezvoltată de Agenția de Guvernare Electronică, reprezintă fundamentul tehnologic existent pe care se construiește viitorul portofel pentru identitatea digitală care va fi furnizat de Guvern. Această soluție conține deja funcționalități relevante, inclusiv generarea, stocarea și prezentarea de documente digitale, precum și mecanisme de autentificare, urmând a fi modernizată, extinsă și certificată pentru a corespunde cerințelor stricte impuse de cadrul european.

Modernizarea EVO în calitate de portofel pentru identitatea digitală constituie, totodată, o opțiune strategică de eficiență instituțională, prin valorificarea investițiilor deja realizate, reutilizarea infrastructurii existente și capitalizarea expertizei tehnice acumulate la nivelul administrației publice. Această abordare reduce costurile de implementare, minimizează riscurile tehnologice și asigură o tranziție graduală către modelul european de identitate digitală.

Soluția de portofel pentru identitatea digitală furnizată de Guvern are rolul de a asigura implementarea unei obligații de interes public, respectiv garantarea disponibilității unui portofel pentru identitatea digitală accesibil tuturor utilizatorilor, în condiții de acces

egal, nediscriminatoriu și continuu. Aceasta nu are un caracter de soluție exclusivă sau de referință obligatorie pentru piață, ci reprezintă instrumentul prin care statul își îndeplinește angajamentul de a asigura existența cel puțin a unui portofel funcțional, sigur și interoperabil, în conformitate cu standardele europene aplicabile și cu obligațiile asumate în procesul de integrare europeană.

În acest sens, rolul soluției guvernamentale este preponderent unul de infrastructură publică digitală de bază, destinată să garanteze incluziunea digitală și continuitatea serviciului pentru toți cetățenii, inclusiv în scenariile în care piața privată nu acoperă integral cererea sau segmentele vulnerabile ale utilizatorilor.

În paralel, proiectul de lege deschide piața către furnizori privați de portofele digitale, în condiții de concurență și respectare a cerințelor de certificare și interoperabilitate, ceea ce permite dezvoltarea unui ecosistem competitiv și inovator.

Un aspect deosebit de important îl constituie faptul că utilizarea portofelului pentru identitatea digitală urmează să fie gratuită pentru persoanele fizice, în linie cu modelul prevăzut de Regulamentul eIDAS 2.0. Această opțiune de politică publică influențează în mod direct structura pieței și modelelor de sustenabilitate economică pentru furnizori.

În acest sens, dezvoltarea și operarea portofelelor digitale nu se bazează în principal pe venituri directe din partea utilizatorilor finali, ci pe modele de business indirecte și ecosistemice, axate pe relațiile cu mediul de afaceri și cu furnizorii de servicii publice și private. În acest context, pot fi identificate următoarele modele de afaceri pentru sectorul privat:

a) servicii avansate de integrare API pentru instituții financiare, furnizori de servicii de telecomunicații și de servicii digitale etc.;

b) servicii de verificare și validare a atributelor și atestatelor electronice în regim B2B și B2G, inclusiv verificări în timp real și fluxuri de conformitate;

c) soluții de onboarding digital și eKYC integrate, adaptate cerințelor sectoriale (bănci, asigurări, fintech, etc.);

d) servicii de identitate digitală pentru tranzacții comerciale complexe, inclusiv semnare contractuală avansată, managementul consimțământului și fluxuri de autorizare digitală;

e) soluții de portofel digital white-label (produs generic care poate fi rebranduit de oricine) pentru sectoare private (bănci, furnizori de servicii de telecomunicații și de servicii digitale, asigurări), integrate cu infrastructura națională.

Această structură economică este în linie cu modelele europene emergente, în care portofelele de identitate digitală funcționează ca infrastructuri publice digitale (digital public infrastructure), iar valoarea economică este generată în principal la nivelul serviciilor construite deasupra acestora, în special în zona de interoperabilitate, verificare, securitate și automatizare a proceselor digitale.

În concluzie, soluția guvernamentală are rolul de a asigura acces universal și egal la identitatea digitală, ca element de infrastructură publică, în timp ce sectorul privat este încurajat să dezvolte un ecosistem competitiv de servicii cu valoare adăugată, bazat pe utilizarea inclusiv a acestei infrastructuri, contribuind astfel la inovare, eficiență și diversificarea pieței digitale.

4. Beneficiarii portofelului pentru identitatea digitală — companiile utilizatoare

În sensul proiectului de lege (art. 3), „beneficiar" desemnează persoana fizică sau juridică care acceptă și procesează datele de identificare prezentate prin portofelul pentru identitatea digitală, în vederea furnizării de servicii publice sau private. Această categorie include, în mod direct, toate companiile din sectorul privat care vor integra portofelul digital în procesele lor de autentificare, verificare a identității și furnizare a serviciilor, atât în mediul online, cât și în interacțiunile fizice.

Reglementarea introduce un model de adoptare graduală și proporțională a portofelului digital în mediul de afaceri. Utilizarea acestuia de către companiile private este, în esență, voluntară, însă legea stabilește obligații progresive pentru anumite categorii de beneficiari, în special pentru operatorii economici mari din sectoarele cu impact ridicat asupra economiei și securității juridice a tranzacțiilor. Această abordare reflectă necesitatea asigurării unui nivel minim de interoperabilitate în sectoarele în care identificarea sigură a utilizatorilor este deja o cerință legală sau operațională.

În același timp, microîntreprinderile și întreprinderile mici, astfel cum sunt definite în Legea nr. 179/2016, sunt exceptate de la orice obligație de integrare, ceea ce asigură protecția acestora împotriva sarcinilor administrative și tehnice disproporționate. Pentru aceste entități, utilizarea portofelului rămâne strict opțională, fiind disponibilă ca instrument de eficientizare a relației cu clienții, fără constrângeri de conformare.

Din perspectiva impactului economic, adoptarea portofelului pentru identitatea digitală generează beneficii structurale semnificative pentru mediul de afaceri. Portofelul devine un instrument de infrastructură digitală care permite companiilor să acceseze date de identitate verificate din surse autentice, reducând dependența de procese manuale de verificare a documentelor și eliminând redundanțele din fluxurile tradiționale de onboarding.

În special, în sectoarele reglementate (bancar, asigurări, telecomunicații, energie, transport, servicii digitale și altele), portofelul are potențialul de a transforma fundamental procesele de tip Know Your Customer (KYC) și Anti-Money Laundering (AML), prin trecerea de la verificări fragmentate și documente statice la fluxuri digitale dinamice, bazate pe date certificate și actualizate în timp real. Aceasta conduce la reducerea costurilor operaționale, scurtarea timpilor de onboarding și creșterea acurateței verificărilor de identitate.

În plus, utilizarea autentificării bazate pe portofelele pentru identitatea digitală reduce semnificativ expunerea companiilor la riscuri de fraudă de identitate, phishing și compromitere a credențialelor, prin înlocuirea mecanismelor tradiționale bazate pe parole cu autentificare criptografică avansată. Acest lucru contribuie direct la îmbunătățirea nivelului de securitate cibernetică și la reducerea costurilor asociate incidentelor de securitate.

Un alt avantaj important îl constituie aplicarea principiului minimizării datelor, conform căruia companiile pot solicita și primi strict acele atribute necesare pentru furnizarea serviciului, fără a colecta și stoca informații excesive. Acest aspect reduce semnificativ riscurile de neconformare cu legislația privind protecția datelor și costurile aferente guvernanței datelor.

De asemenea, portofelul digital permite implementarea unor fluxuri de autentificare complet digitale, inclusiv onboarding „end-to-end" fără interacțiune fizică, precum și scenarii de verificare offline sau în proximitate, ceea ce extinde utilizabilitatea soluției în

medii cu conectivitate limitată sau în puncte de interacțiune fizică (de exemplu, ghișee, puncte de vânzare, servicii publice descentralizate).

În ansamblu, impactul asupra companiilor beneficiare este unul structural pozitiv, cu potențial transformator asupra modului de furnizare a serviciilor digitale. Legea nu introduce sarcini administrative generalizate, ci creează un cadru tehnico-juridic modern care permite optimizarea proceselor de identificare și autentificare, reducerea costurilor operaționale și creșterea nivelului de securitate și încredere în economia digitală.

Obligațiile de acceptare aplicabile anumitor categorii de operatori economici mari sunt justificate prin principiul proporționalității și prin rolul acestora în sectoarele esențiale ale economiei, unde asigurarea unor mecanisme sigure și interoperabile de identificare este deja o cerință funcțională și de reglementare.

În ansamblu, proiectul de lege privind identificarea electronică și serviciile de încredere are un impact pozitiv net asupra sectorului privat și asupra ecosistemului digital al Republicii Moldova, prin instituirea unui cadru juridic modern, predictibil și compatibil cu standardele Uniunii Europene în materie de identitate digitală și servicii de încredere electronice. Proiectul transpune și adaptează la nivel național conceptele și mecanismele prevăzute de Regulamentul (UE) 2024/1183 (eIDAS 2.0), creând premisele interoperabilității transfrontaliere și ale integrării Republicii Moldova în spațiul european al identității digitale.

Legea nu urmărește exclusiv reglementarea unor servicii existente, ci creează premisele dezvoltării unei infrastructuri digitale naționale de nouă generație, bazate pe identitate digitală verificabilă, atestate electronice ale atributelor și mecanisme moderne de autentificare și semnare electronică. În acest sens, proiectul are un caracter structural și strategic, reprezentând una dintre componentele esențiale ale procesului de transformare digitală a administrației publice și economiei naționale.

Un element central al reformei îl constituie instituirea cadrului juridic pentru portofelul pentru identitatea digitală, concept introdus pentru prima dată în ordinea juridică a Republicii Moldova. Legea creează condițiile necesare pentru apariția unei piețe complet noi, atât pentru furnizorii de portofele digitale, cât și pentru prestatorii de servicii de încredere și furnizorii de servicii digitale conexe. Totodată, prin faptul că proiectul permite furnizarea portofelelor atât de entități publice, cât și de operatori privați, se instituie un model deschis și competitiv, bazat pe libera alegere a utilizatorului și pe concurență tehnologică.

Soluția guvernamentală care urmează a fi furnizată prin intermediul Agenției de Guvernare Electronică nu urmărește instituirea unui monopol de stat asupra identității digitale, ci are rolul de a asigura disponibilitatea cel puțin a unui portofel pentru identitatea digitală, accesibil tuturor persoanelor în condiții echitabile, nediscriminatorii și gratuite, în conformitate cu cerințele eIDAS 2.0 și cu angajamentele asumate de Republica Moldova în procesul de aderare la Uniunea Europeană. În paralel, cadrul normativ creează posibilitatea dezvoltării unui ecosistem concurențial de soluții private și hibride, stimulând inovarea și investițiile în sectorul digital.

Proiectul valorifică într-o măsură semnificativă infrastructura, expertiza și soluțiile digitale deja dezvoltate la nivel național, inclusiv platformele EVO și EvoSign, reducând costurile de implementare și accelerând capacitatea statului de a livra servicii compatibile

cu standardele europene. Această abordare permite reutilizarea investițiilor publice realizate anterior și evitarea duplicării inutile a infrastructurilor tehnologice.

Impactul pozitiv asupra sectorului privat este unul multidimensional. Legea creează oportunități economice noi pentru:

- prestatorii de servicii de încredere calificați;
- furnizorii de portofele pentru identitatea digitală;
- furnizorii de servicii de onboarding digital și eKYC;
- companiile fintech, telecom și insurtech;
- furnizorii de servicii cloud și infrastructură digitală;
- integratorii IT și dezvoltatorii de soluții software;
- furnizorii de servicii de verificare și validare a atributelor electronice;
- furnizorii de soluții de interoperabilitate și integrare API;
- furnizorii de soluții white-label și platforme de identitate digitală pentru sectorul corporativ.

Legea introduce, de asemenea, pentru prima dată reglementarea unor servicii și piețe inexistente până în prezent în Republica Moldova, inclusiv:

- atestate electronice ale atributelor;
- arhivare electronică calificată;
- registre electronice calificate;
- servicii de distribuție electronică înregistrată calificată;
- servicii asociate portofelelor pentru identitatea digitală.

Un element distinctiv și de importanță majoră îl constituie mecanismul de recunoaștere automată a prestatorilor de servicii de încredere calificați din statele membre ale Uniunii Europene. Acest mecanism elimină practic barierele administrative de intrare pe piață pentru prestatorii europeni deja calificați în ecosistemul eIDAS și contribuie la integrarea rapidă a pieței moldovenești în spațiul european al serviciilor de încredere. Totodată, acesta stimulează concurența, diversificarea serviciilor și transferul de expertiză și tehnologii către piața locală.

Din perspectiva beneficiarilor privați ai portofelului pentru identitatea digitală, legea creează un cadru care permite simplificarea semnificativă a proceselor de identificare și autentificare, reducerea costurilor operaționale și creșterea securității tranzacțiilor digitale. Utilizarea identității digitale verificabile și a atributelor electronice emise din surse autentice va permite automatizarea și digitalizarea completă a numeroase procese comerciale și administrative.

În același timp, proiectul respectă principiul proporționalității și evită impunerea unor sarcini excesive asupra mediului de afaceri. Utilizarea portofelului pentru identitatea digitală rămâne, ca regulă generală, voluntară, iar obligațiile de acceptare sunt limitate doar la anumite categorii de operatori mari din sectoarele reglementate, care dispun deja de infrastructuri digitale și mecanisme de autentificare avansate. Microîntreprinderile și întreprinderile mici sunt exceptate expres de la aceste obligații.

Implementarea graduală a prevederilor legii, corelată cu obligația Guvernului de a adopta cadrul normativ subsecvent și de a asigura disponibilitatea infrastructurii tehnice necesare, oferă sectorului public și privat un termen rezonabil pentru adaptare și conformare. În procesul elaborării actelor normative subsecvente urmează a fi evaluate

suplimentar necesitățile tehnice, organizaționale și financiare ale actorilor implicați, inclusiv ale organismelor din sectorul public care gestionează surse autentice de date.

Totodată, proiectul creează premisele dezvoltării unei infrastructuri digitale de interes public („digital public infrastructure"), în care valoarea economică nu derivă exclusiv din utilizarea portofelului în sine, ci din ecosistemul extins de servicii și soluții construite peste această infrastructură — servicii financiare digitale, onboarding la distanță, contractare electronică, servicii de conformitate, verificare de identitate, servicii de interoperabilitate și automatizare digitală.

Prin urmare, proiectul de lege reprezintă nu doar o inițiativă de armonizare legislativă cu acquis-ul Uniunii Europene, ci și un instrument strategic pentru modernizarea infrastructurii digitale naționale, creșterea competitivității economiei digitale și consolidarea încrederii în serviciile electronice furnizate în Republica Moldova.

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 transpune Regulamentul (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 de lege a fost 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. În urma avizelor parvenite, proiectul de lege a fost ajustat, după caz, conform obiecțiilor și propunerilor corespunzătoare.

7. Concluziile expertizelor

Conform art. 36 și 37 din Legea 100/2017 cu privire la actele normative proiectul a fot supus expertizei anticorupție și expertizei juridice, obiecțiile și propunerile fiind luate în considerație la definitivarea acestuia.

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 hotărârea Guvernului privind desemnarea organismului de supraveghere și stabilirea modului de organizare și funcționare a acestuia, 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
Prima etapă, în termen de 3 luni de la publicarea legii, constă în desemnarea de către Guvern a autorității responsabile de realizarea politicii de stat în domeniu, a organismului de supraveghere și a organismului din sectorul public responsabil de furnizarea portofelului pentru identitatea digitală (art. 80 alin. (2) lit. a)). Pentru implementarea 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.

Ministru **Claudiu-Iulius-Gavril NĂSUI**

SINTEZA
proiectului de lege privind identificarea electronică și serviciile de încredere (număr unic 395/MDED/SIS/2026)
(denumirea proiectului actului normativ)

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Avizare și consultare publică			
Ministerul Infrastructurii și Dezvoltării Regionale (Nr. 23-2422 din 06.05.2026)	1.	Lipsa de obiecții și propuneri.	
Agenția Servicii Publice (Nr. 01/4254 din 08.05.2026)	2.1	Proiectul de lege conține sintagma „servicii publice și private”. Dacă noțiunea „serviciu public” este reglementată de Legea nr.234/2021 cu privire la serviciile publice, noțiunea ”serviciu privat” lipsește în actele normative ale Republicii Moldova. Totodată, în art. 3 al Legii nr.234/2021 se utilizează termenii: servicii cu caracter comercial - activitate de comerţ, aferentă participării la circuitul comercial, realizată pe pieţele deschise concurenţei şi desfăşurată în mod concurenţial și servicii conexe prestate beneficiarilor de servicii publice (fotocopiere simplă, scanare documente, consultare, remitere statistici, livrare documente etc.), care nu cad sub noțiunea „serviciu public”. Pentru a evita utilizarea ambiguă a termenilor, propunem substituirea în proiectul legii a sintagmei ”servicii publice și private” cu cuvântul ”servicii”, cu utilizare, după caz, a sintagmei ”furnizori de servicii de drept public și privat”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	2.2	La art. 5 alin. (2) din proiect, norma prevede că portofelele pentru identitatea digitală pot fi puse la dispoziție și de „furnizori de drept privat”. Lipsește însă orice referință la posibilitatea ca alte autorități/instituții publice să furnizeze portofele specializate, în limitele propriilor competențe. Modelul european al eIDAS 2.0 (art. 5a alin. (2)) prevede expres trei modalități de furnizare: direct de către un stat membru, pe baza unui mandat din partea unui stat membru, sau independent, dar recunoscut de stat. Această	**Se acceptă.** Proiectul a fost revizuit ținând cont de propunerile recepționate în proces de avizare.

		flexibilitate s-a pierdut în transpunere. Propunem completarea alin. (2) cu următorul conținut: „Portofelele pentru identitatea digitală pot fi puse la dispoziția utilizatorilor și de către alte autorități/instituții publice, în limitele competențelor proprii și pe baza unui mandat din partea Guvernului, precum și de către furnizori de drept privat, în condițiile prezentei legi.”	
	2.3	Art. 6 alin.(2) stabilește că procesul de înregistrare a beneficiarilor se desfășoară „prin intermediul Portalului guvernamental integrat EVO”. Această desemnare unică creează o dependență tehnică și instituțională rigidă. Mai mult, cadrul juridic actual al Portalului EVO trebuie corelat cu prevederile prezentei legi pentru a evita lacune procedurale. Astfel, propunem reformularea alin. (2) astfel: „Procesul de înregistrare se desfășoară prin intermediul Portalului guvernamental integrat (EVO) sau al unei alte platforme guvernamentale desemnate de organismul de supraveghere și este eficient din punctul de vedere al costurilor și proporțional cu riscurile (...)”.	**Se acceptă parțial.** Proiectul a fost revizuit, fiind stabilit că procesul de înregistrare a beneficiarilor are loc în mod electronic, urmând ca instrumentele și condițiile să fie stabilite de Guvern.
	2.4	Potrivit art. 7 alin.(1), certificarea conformității portofelelor pentru identitatea digitală urmează a fi efectuată „de către organisme de evaluare a conformității acreditate”. În Republica Moldova, capacitatea instituțională în materie de organisme de evaluare a conformității acreditate pentru certificarea portofelelor digitale este, în prezent, limitată. Centrul Național de Acreditare (MOLDAC) nu deține încă scheme specifice de acreditare pentru portofelele EUDI. Propunem completarea după alin. (1) cu un nou alineat cu următorul conținut: „Până la dezvoltarea capacităților naționale de acreditare pentru certificarea portofelelor pentru identitatea digitală, certificarea poate fi efectuată de organisme acreditate într-un stat membru al Uniunii Europene, în condițiile stabilite de Guvern.”	**Nu se acceptă.** Aspectul invocat referitor la capacitatea instituțională limitată existentă în prezent în Republica Moldova privind organismele de evaluare a conformității acreditate pentru certificarea portofelelor pentru identitatea digitală a fost analizat la etapa elaborării proiectului de lege și reflectat deja în conținutul acestuia. Astfel, art. 3 pct. 37 definește noțiunea de „organism de evaluare a conformității” ca fiind o persoană juridică independentă, acreditată fie în Republica Moldova, fie într-un stat membru al Uniunii Europene, competentă să efectueze certificarea portofelelor pentru identitatea digitală sau a mijloacelor de identificare electronică. Prin urmare, proiectul permite deja recunoașterea și utilizarea organismelor acreditate în statele membre ale Uniunii Europene, fără

			a condiționa aplicarea mecanismului exclusiv de existența unor scheme naționale de acreditare dezvoltate de către Centrul Național de Acreditare (MOLDAC). În acest context, completarea propusă după art. 7 alin. (1) este considerată redundantă, întrucât soluția normativă urmărită de autorul obiecției este deja acoperită de dispozițiile proiectului de lege.
	2.5	Art. 9 alin.(4) prevede că „Organismul de supraveghere, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la art. 8.” Textul este lipsit de predicat — formularea este ambiguă și nu are sens normativ complet. Prin comparație, art. 5e alin. (4) din Regulamentul (UE) 910/2014 prevede: „Comisia publică în Jurnalul Oficial al Uniunii Europene, fără întârzieri nejustificate, modificările corespunzătoare aduse listei (...).” Propunem reformulare: „Organismul de supraveghere asigură, fără întârzieri nejustificate, publicarea modificărilor corespunzătoare aduse listei menționate la art. 8.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	2.6	Definiția „nivelului de asigurare scăzut” de la art. 12 alin.(2) lit. a), conține formularea „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 (...)”. Aceasta este o transcriere literală incorectă — definiția nivelului „scăzut” utilizează aceeași formulare ca și nivelul „substanțial”, ceea ce face imposibilă diferențierea celor trei niveluri (scăzut, substanțial, ridicat). În textul Regulamentului (UE) 910/2014, nivelul scăzut este definit ca asigurând „un grad limitat de încredere” („limited degree of confidence”), iar scopul controalelor este „de a reduce riscul” (fără adverbul „substanțial”). Propunem reformularea lit. a) astfel: „nivelul de asigurare scăzut se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad limitat 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	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		de identificare, inclusiv controalele tehnice, al căror scop este de a reduce riscul unei utilizări frauduloase sau al modificării frauduloase a identității.”	
	2.7	Art. 13. alin. (1) stabilește obligația „deținătorului unui sistem de identificare electronică” de a transmite organismului de supraveghere o notificare cu informațiile prevăzute. Lipsește însă o dispoziție tranzitorie care să clarifice termenul de notificare pentru sistemele existente la data intrării în vigoare a legii. ASP, în calitate de deținător al sistemului de identificare bazat pe cartea de identitate electronică, ar trebui să dispună de un termen rezonabil pentru pregătirea documentației de notificare, inclusiv evaluarea formală a nivelului de asigurare și descrierea regimului de răspundere. În acest sens, propunem adăugarea, la art. 70 (Dispoziții tranzitorii), a unui nou alineat cu următorul conținut: „Sistemele de identificare electronică existente la data intrării în vigoare a prezentei legi, inclusiv sistemul național de identificare electronică bazat pe cartea de identitate emisă în temeiul Legii nr. 273/1994, urmează a fi notificate organismului de supraveghere, în conformitate cu art. 13, în termen de 12 luni de la data intrării în vigoare a prezentei legi.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	2.8	Art. 14 alin. (1) și (2) transpune mecanismul de „corelare transfrontalieră a identităților” („cross-border identity matching”) din art. 11a al eIDAS 2.0. În context național, acest proces va necesita accesul la registrele administrate de ASP — în primul rând la RSP. Proiectul nu precizează canalul tehnic prin care se va realiza accesul, deși există o platformă guvernamentală dedicată — MConnect — administrată de AGE, care îndeplinește exact această funcție. Propunem completarea alin. (2) cu următorul conținut: „Guvernul stabilește măsuri tehnice și organizatorice (...). Schimbul de date necesar pentru corelarea identităților se realizează exclusiv prin intermediul platformei guvernamentale de interoperabilitate MConnect și al interfețelor securizate puse la dispoziție de deținătorii surselor autentice.”	**Nu se acceptă.** Proiectul de lege stabilește cadrul juridic general aplicabil mecanismului de corelare transfrontalieră a identităților, în conformitate cu prevederile Regulamentului eIDAS 2.0, în timp ce aspectele tehnice și arhitectura de interoperabilitate urmează a fi reglementate la nivel subsecvent, prin acte normative și cerințe tehnice adoptate de Guvern. În acest context, includerea expresă în lege a unei anumite platforme tehnologice sau a unei soluții tehnice concrete nu este considerată oportună, întrucât ar limita neutralitatea tehnologică a actului normativ și ar putea afecta flexibilitatea necesară pentru adaptarea

			ulterioară la evoluțiile tehnologice, arhitecturale sau instituționale. Totodată, cadrul normativ național în materie de interoperabilitate și schimb de date în sectorul public reglementează deja utilizarea platformei guvernamentale de interoperabilitate MConnect pentru schimbul securizat de date între sisteme informaționale.
	2.9	Art. 15 alin. (2) instituie cadrul de interoperabilitate, dar nu face nici o referință la infrastructura guvernamentală existentă — în special la platforma MConnect (Hotărârea Guvernului nr. 211/2019), care este coloana vertebrală a interoperabilității între sistemele informaționale de stat din Republica Moldova. Lipsa acestei trimiteri creează riscul dezvoltării unui cadru paralel de interoperabilitate, ceea ce ar contraveni principiului eficienței administrative și ar duce la dublarea investițiilor publice. Propunem completarea alin. (2): „Guvernul va stabili cadrul de interoperabilitate, care se integrează cu și este implementat prin platforma guvernamentală de interoperabilitate MConnect, și care trebuie să îndeplinească următoarele criterii: (...).”	**Nu se acceptă.** Prevederile art. 15 alin. (2) stabilesc cadrul general de interoperabilitate la nivel de principii, urmând ca aspectele tehnice de implementare să fie reglementate prin acte normative subsecvente. Proiectul este elaborat în mod tehnologic neutru, iar includerea unei referințe explicite la platforma MConnect nu este oportună, întrucât ar limita flexibilitatea cadrului normativ și ar condiționa soluțiile tehnice la o infrastructură specifică. În același timp, utilizarea infrastructurii guvernamentale de interoperabilitate este deja reglementată la nivel național.
	2.10	La art. 16 alin. (1), similar cu art. 7, certificarea sistemelor de identificare electronică se realizează „de organismele de evaluare a conformității”, fără a preciza dacă acestea trebuie să fie acreditate la nivel național sau european. Propunem adăugarea unei mențiuni: „(...) este certificată de organismele de evaluare a conformității acreditate în Republica Moldova sau într-un stat membru al Uniunii Europene.” Aliniere semantică cu definiția de la art. 3 pct. 37).	**Nu se acceptă.** Noțiunea de „organism de evaluare a conformității” definită la art. 3 pct. 37 include deja în mod expres entitățile acreditate în Republica Moldova sau într-un stat membru al Uniunii Europene. Prin urmare, utilizarea acestei noțiuni în cuprinsul art. 16 alin. (1) asigură automat aplicarea ambelor categorii de organisme, fără a fi necesară reiterarea condițiilor de acreditare în fiecare dispoziție subsecventă.
	2.11	Art. 28 alin.(3) stabilește că „organismele din sectorul public nu pot solicita, pentru utilizarea serviciilor publice electronice, un	**Nu se acceptă.**

		nivel de securitate al semnăturii electronice mai ridicat decât cel al semnăturii electronice calificate.” Pentru a se asigura aplicarea uniformă, este oportună precizarea că această interdicție vizează doar interfața către utilizatori, nu și cerințele tehnice interne ale sistemelor informaționale (de exemplu, autentificare cu doi factori, marcare temporală suplimentară). Propunem reformulare: „Organismele din sectorul public nu pot solicita utilizatorilor finali, ca și condiție de acces la serviciile publice electronice, un nivel de securitate al semnăturii electronice mai ridicat decât cel al semnăturii electronice calificate. Cerințele tehnice și organizatorice interne aplicabile sistemelor informaționale ale organismelor din sectorul public se stabilesc separat, conform cadrului normativ aplicabil în domeniul securității cibernetice.”	Cerința prevăzută la alin. (3) se aplică exclusiv condițiilor de acces la serviciile publice electronice de către utilizatorii finali (beneficiarii serviciilor publice) și nu afectează cerințele tehnice și organizatorice interne ale sistemelor informaționale ale organismelor din sectorul public, stabilite conform cadrului normativ în domeniul securității cibernetice și al guvernanței sistemelor informaționale.
	2.12	Articolul 53 transpune art. 5b din eIDAS 2.0 privind atestatele electronice ale atributelor în cadrul serviciilor publice. Formularea actuală preia aproape literal textul european, inclusiv mențiunea „cu excepția cazului în care acest lucru este permis în mod expres de statul membru” — sintagmă care, în context național, este lipsită de sens. Propunem reformulare: „Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este obligatorie în temeiul cadrului normativ aplicabil 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, cu excepția cazului în care acest lucru este permis expres de actele normative ale Guvernului.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	2.13	Art. 55 alin.(1) instituie obligația organismelor din sectorul public care gestionează registre de stat sau alte sisteme informaționale ce constituie surse autentice de date să asigure „disponibilitatea mecanismelor electronice care permit verificarea atributelor (...) la cererea expresă a utilizatorului”. ASP este deținătorul majorității surselor autentice naționale, iar implementarea acestei obligații presupune dezvoltarea unor interfețe electronice noi de tip „attribute attestation API”, conforme cu standardele europene	**Se acceptă parțial.** Obiecția formulată este reținută parțial sub aspectul complexității tehnice și operaționale aferente implementării mecanismelor necesare pentru emiterea și verificarea atestatelor electronice ale atributelor. În acest sens a fost completat art. 80 cu alin. (5). Totodată, aspectele privind dezvoltarea infrastructurii tehnice,

		(OpenID4VC, ISO/IEC 18013-5 etc.). În acest sens, se generează mai multe riscuri: - Proiectul nu precizează termenul de implementare a acestor interfețe pentru sursele autentice. Termenul general de 18 luni de la art. 69 alin. (1) este complet insuficient pentru o astfel de sarcină tehnică majoră. - Proiectul nu prevede mecanisme de finanțare. ASP este o instituție publică autofinanțată din venituri proprii (HG nr. 314/2017), iar dezvoltarea interfețelor menționate va antrena costuri de mai multe milioane MDL (inclusiv pentru externalizare către prestatori terți - subcontractori (după caz) prin aplicarea procedurilor de achiziții publice) care nu pot fi acoperite din tarifele actuale ale serviciilor ASP. - Proiectul nu precizează regimul tarifar — atestatele electronice ale atributelor sunt sau nu servicii cu plată? Cine suportă costul? Răspunsul la aceste întrebări trebuie să fie clar din lege, nu să rămână la nivelul actelor normative subsecvente. Astfel, propunem: (a) Introducerea unui termen distinct de implementare la art. 69: „Organismele din sectorul public deținătoare de surse autentice asigură conformitatea cu obligațiile prevăzute la art. 55 în termen de 36 de luni de la data intrării în vigoare a prezentei legi, în limitele resurselor financiare alocate sau atrase în acest scop.” (b) Adăugarea unui nou alineat, după alin.(1), la art. 55: „Costurile dezvoltării și mentenanței mecanismelor electronice prevăzute la alin. (1) se acoperă din bugetul de stat sau din alte surse de finanțare alocate prin acte normative ale Guvernului. În cazul instituțiilor publice autofinanțate, mecanismele de recuperare a costurilor se stabilesc prin acte ale Guvernului.” (c) Introducerea unui nou alineat la art. 55: „Verificarea atributelor în raport cu sursele autentice administrate de organismele din sectorul public se realizează prin intermediul platformei guvernamentale de interoperabilitate MConnect, în condițiile stabilite de cadrul normativ aplicabil.”	calendarul etapizat de implementare, mecanismele de interoperabilitate și identificarea surselor de finanțare urmează a fi detaliate prin actele normative subsecvente și documentele de implementare elaborate la nivel guvernamental. Cu referire la propunerea instituirii unor mecanisme de recuperare a costurilor sau a unui regim tarifar pentru verificarea atributelor și utilizarea mecanismelor aferente portofelelor pentru identitatea digitală, aceasta nu poate fi acceptată, având în vedere obligațiile care derivă din Regulamentul (UE) nr. 910/2014. În special, Regulamentul stabilește expres obligația statelor de a pune la dispoziție cu titlu gratuit mecanismele necesare pentru verificarea autenticității și valabilității portofelelor europene pentru identitatea digitală, precum și pentru verificarea autenticității și valabilității identității utilizatorilor acestora. Totodată, regulamentul prevede expres că portofelele europene pentru identitatea digitală se emit, se utilizează și se revocă gratuit pentru toate persoanele fizice. În acest context, instituirea prin lege a unor mecanisme de tarifare sau recuperare a costurilor direct de la utilizatori persoane fizice pentru verificarea atributelor sau pentru funcționalitățile esențiale asociate portofelelor pentru identitatea digitală ar contraveni principiilor și obligațiilor prevăzute de cadrul european aplicabil. Totodată, includerea în lege a unor soluții tehnologice specifice, inclusiv utilizarea unei anumite platforme de interoperabilitate, nu

			este considerată oportună la nivel legislativ, aceste aspecte urmând a fi reglementate flexibil prin acte normative subsecvente și documente tehnice de implementare, în funcție de evoluțiile tehnologice, standardele europene aplicabile și resursele disponibile.
	2.14	Art. 55 alin.(2) enumeră 11 categorii de atribute pentru care se aplică obligația prevăzută la alin. (1). Examinarea materială arată că majoritatea acestora cad în competența directă a ASP: Atribute administrate de ASP: lit. a) adresa (RSP) — lit. b) vârsta (Registrul actelor de stare civilă) — lit. c) genul (RSP, Registrul actelor de stare civilă) — lit. d) starea civilă (Registrul actelor de stare civilă) — lit. e) componența familiei (RSP) — lit. f) naționalitatea sau cetățenia (RSP) — lit. i) împuterniciri și mandate (Registrul de stat al actelor notariale, după caz) — lit. k) datele privind societățile (Registrul de stat al unităților de drept). Atribute administrate de alte instituții: lit. g) nivelul de studii — Ministerul Educației și Cercetării; lit. h) calificări profesionale — instituții abilitate; lit. j) acte permisive — diverse autorități, parțial ASP. Pentru asigurarea unei aplicări coerente, ar fi util ca legea să stabilească mecanismul de identificare a deținătorului responsabil pentru fiecare atribut, în baza registrelor existente (cf. Legea nr. 71/2007 privind registrele). Propunem adăugarea unui nou alineat (3) cu următorul conținut: „Lista organismelor din sectorul public responsabile de furnizarea atestatelor electronice ale atributelor pentru fiecare categorie prevăzută la alin. (2) se stabilește de Guvern, cu consultarea organismului de supraveghere și a deținătorilor surselor autentice.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	2.15	Art. 56 alin.(5) prevede obligația organismelor din sectorul public care emit atestate electronice ale atributelor să pună la dispoziție „o interfață cu portofelele pentru identitatea digitală (...)”. Cerința tehnică implică standarde specifice (OpenID for Verifiable Credentials, OID4VP/OID4VCI, formate SD-JWT VC sau ISO mDOC), care evoluează rapid la nivel european. Pentru a asigura aplicabilitatea normei, este nevoie de o referință la cadrul	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		tehnic stabilit de Guvern. Propunem completarea alin. (5): „Organismele din sectorul public care emit atestate electronice ale atributelor pun la dispoziție o interfață cu portofelele pentru identitatea digitală (...), conform standardelor și specificațiilor tehnice stabilite de Guvern, prin armonizare cu standardele europene aplicabile.”	
	2.16	Propunem completarea art. 56 cu un nou alineat (6), având în vedere rolul instituțional al ASP: „Instituția Publică Agenția Servicii Publice este, prin prevederile prezentei legi și ale Legii nr. 71/2007 privind registrele, organism din sectorul public responsabil de sursele autentice administrate, cu atribuția de a emite atestate electronice ale atributelor în condițiile prezentului articol, în limita atributelor disponibile din registrele de stat administrate.” Recunoașterea expresă a calității ASP de organism emitent este esențială pentru securitatea juridică a serviciilor prestate și pentru evitarea oricăror litigii ulterioare. Mai mult, această recunoaștere poate contribui la finanțarea adecvată a infrastructurii necesare.	**Nu se acceptă.** Rolul instituțional al ASP în calitate de deținător și administrator al mai multor registre de stat, precum și atribuțiile sale în raport cu sursele autentice de date, sunt deja stabilite prin cadrul normativ existent. Proiectul de lege utilizează o abordare funcțională și neutră instituțional, reglementând competențele privind emiterea atestatelor electronice ale atributelor prin raportare la calitatea de „organism din sectorul public” și la deținerea surselor autentice, fără a nominaliza instituții individuale în textul de bază, acolo unde acestea sunt deja determinate de legislația specială. În acest context, includerea unei prevederi explicite privind ASP ar reprezenta o dublare normativă a competențelor deja stabilite prin acte legislative existente și ar afecta coerența și caracterul general al reglementării. Totodată, aspectele privind organizarea instituțională și eventualele implicații financiare ale exercitării atribuțiilor țin de cadrul bugetar și de actele de implementare, nefiind necesar a fi detaliate la nivelul prezentei legi.
	2.17	Articolul 60 alin.(1) stabilește cerințele pentru serviciile calificate de arhivare electronică. Lipsește însă o trimitere la cadrul național aplicabil în materie de arhivă, în special la Legea nr. 880/1992 cu privire la Fondul Arhivistic al Republicii Moldova, precum și la cadrul ASP în materie de arhivare a documentelor	**Nu se acceptă.** Art. 60 alin. (1) stabilește regimul juridic al serviciilor calificate de arhivare electronică în cadrul prezentei legi, care are caracter special în raport cu legislația generală privind Fondul

		de stare civilă. Propunem introducerea unei trimiteri normative: „Serviciile calificate de arhivare electronică se prestează în conformitate cu prevederile prezentei legi și cu cadrul național privind Fondul Arhivistic al Republicii Moldova.” Mențiunea evită orice conflict normativ între cele două regimuri.	Arhivistic și arhivarea documentelor pe suport fizic sau tradițional. Cadrul național privind arhivarea, inclusiv Legea nr. 880/1992 și reglementările privind arhivarea documentelor de stare civilă, rămâne aplicabil în măsura în care nu contravine regimului special instituit pentru arhivarea electronică și nu necesită reiterare expresă în fiecare act normativ sectorial. În acest context, includerea unei trimiteri generale la legislația arhivistică nu aduce valoare normativă suplimentară, întrucât principiul aplicării coroborate a actelor normative este deja consacrat în sistemul juridic național.
	2.18	Termenul general de intrare în vigoare — 18 luni de la publicare — este insuficient pentru pregătirea infrastructurii de către sursele autentice (în special ASP), care trebuie să dezvolte interfețe API conforme cu standardele europene, și în special să certifice infrastructura, precum și să ajusteze procesele interne, dar și să formeze personal calificat și abilitat pentru rigorile tehnologice impuse. Propunem diferențierea termenelor de intrare în vigoare în funcție de natura obligațiilor: • Dispozițiile generale și cele privind serviciile de încredere (art. 17-62, exceptând art. 55-57) — 18 luni; • Dispozițiile privind portofelul pentru identitatea digitală (art. 5-10) — 24 luni (compatibil cu art. 69 alin. (4)); • Dispozițiile privind atributele din surse autentice (art. 55-57) — 36 luni (luând în considerare amploarea sarcinilor de implementare); • Art. 67 și 68 — la momentul aderării la UE (cum este deja prevăzut).	**Se acceptă parțial.** Proiectul stabilește un mecanism etapizat și proporțional de implementare a noilor obligații, care oferă autorităților și instituțiilor publice termene suficiente pentru pregătirea cadrului normativ, dezvoltarea infrastructurii tehnice necesare și ajustarea proceselor operaționale. Astfel, legea intră în vigoare la expirarea a 12 luni de la publicare, perioadă în care Guvernul urmează să adopte actele normative subsecvente necesare implementării legii. În același timp, proiectul prevede termene suplimentare distincte pentru implementarea obligațiilor operaționale complexe: - disponibilitatea unui portofel pentru identitatea digitală certificat — în termen de 24 de luni de la intrarea în vigoare a legii; - conformarea organismelor din sectorul public deținătoare de surse autentice cu obligațiile prevăzute la art. 55 și 56 — în termen de 24 de luni de la intrarea în vigoare a legii.

			Prin urmare, cadrul propus acordă, în practică, o perioadă extinsă (de până la 36 luni din momentul adoptării legii) pentru implementarea obligațiilor tehnice și organizaționale, inclusiv pentru dezvoltarea infrastructurii necesare, ajustarea proceselor interne și consolidarea capacităților instituționale. Totodată, nu este considerată oportună instituirea unor termene diferențiate de intrare în vigoare pentru anumite categorii de dispoziții exclusiv în considerarea nivelului de pregătire al unor entități individuale, întrucât aceasta ar afecta coerența și aplicarea uniformă a cadrului normativ. În practică, gradul de pregătire instituțională poate varia între diferite organisme din sectorul public, unele autorități putând implementa obligațiile prevăzute de lege într-un termen mai redus decât altele. În acest context, soluția legislativă propusă asigură un echilibru rezonabil între necesitatea implementării într-un termen previzibil a cadrului eIDAS și acordarea unor perioade suficiente pentru conformare și dezvoltare instituțională.
	2.19	Art. 70 alin. (1) asigură continuitatea statutului prestatorilor de servicii de încredere calificați obținut în baza Legii nr. 124/2022. Continuitatea este oportună, dar este insuficientă. Proiectul nu prevede: (i) Continuitatea sistemelor și mijloacelor de identificare electronică emise în baza cadrului anterior — în special a cărților de identitate electronice emis de ASP. (ii) Statutul tranzitoriu al certificatelor calificate emise pentru sigilii electronice (alin. (2) face referință doar la certificatele pentru semnături electronice ale persoanelor fizice).	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		(iii) Statutul actelor normative aprobate în baza Legii nr. 124/2022 — sunt menținute în vigoare? Sunt abrogate ca urmare a abrogării legii de bază? Propunem adăugarea următoarelor noi alineate la art. 70: „(3) Sistemele de identificare electronică emise în baza Legii nr. 124/2022, inclusiv sistemul național de identificare electronică bazat pe cărțile de identitate, își păstrează valabilitatea și produc efecte juridice, urmând a fi notificate organismului de supraveghere conform art. 13 în termen de 12 luni de la data intrării în vigoare a prezentei legi. (4) Certificatele calificate emise persoanelor juridice pentru sigilii electronice în temeiul Legii nr. 124/2022 sunt considerate în continuare certificate calificate pentru sigilii electronice în temeiul prezentei legi până la expirarea acestora. (5) Actele normative emise în temeiul Legii nr. 124/2022 rămân aplicabile, în măsura în care nu contravin prezentei legi, până la adoptarea actelor normative noi corespunzătoare.”	
	2.20	La Nota de fundamentare, la compartimentul „Impactul asupra sectorului public” se menționează doar Serviciul de Informații și Securitate (în calitate de organism de supraveghere) și Agenția de Guvernare Electronică (în calitate de dezvoltator al portofelului). Lipsește orice referință la celelalte instituții cu rol structural în implementare. ASP (deținător al RSP, Registrului de stat a unităților de drept etc.); MAI (deținător al Registrului de stat al armelor, Registrul evidenței conducătorilor auto sancționați etc.); Ministerul Educației și Cercetării (deținător al Registrului de stat al diplomelor); Centrul Național Anticorupție; Comisia Națională a Pieței Financiare; STISC; CNSC etc. Propunem completarea pct. 4.1 cu un subcapitol distinct privind impactul asupra fiecărei categorii de actori publici afectați, inclusiv cu o estimare a sarcinilor administrative și financiare aferente.	**Nu se acceptă.** Compartimentul „Impactul asupra sectorului public” din Nota de fundamentare are caracter sintetic și urmărește evidențierea principalilor actori instituționali cu rol direct și imediat în implementarea cadrului de identificare electronică și servicii de încredere. Detalierea exhaustivă a tuturor instituțiilor care dețin registre de stat sau sisteme informaționale cu relevanță potențială pentru implementare ar presupune o analiză interinstituțională complexă și o evaluare individuală a impactului tehnic, organizațional și financiar pentru fiecare sistem în parte, exercițiu care excede conținutului Notei de fundamentare și este specific etapei de implementare. În acest context, adoptarea cadrului normativ va servi ca temei juridic pentru inițierea

			acțiunilor de evaluare, planificare și coordonare interinstituțională privind identificarea tuturor sistemelor și registrelor relevante, estimarea impactului detaliat și stabilirea măsurilor de implementare la nivelul fiecărei autorități publice implicate. Prin urmare, Nota de fundamentare reflectă în mod proporțional impactul asupra principalilor actori instituționali cu rol structural, urmând ca analiza detaliată și operaționalizarea măsurilor să fie realizate ulterior, în baza actului normativ adoptat.
Ministerul Educației și Cercetării (Nr. 15/60/26 din 07.05.2026)	3.	Lipsa de obiecții și propuneri.	
Ministerul Apărării (Nr. 11/724 din 06.05.2026)	4.	Lipsa de obiecții și propuneri.	
Ministerul Culturii (Nr. 05/1-09/1340 din 06.05.2026)	5.	Lipsa de obiecții și propuneri.	
Ministerul Muncii și Protecției Sociale (Nr. 22/2454 din 06.05.2026)	6.	Urmare a ratificării Convenției ONU privind drepturile persoanelor cu dizabilități, a fost adoptată Legea nr. 60/2012, privind incluziunea socială a persoanelor cu dizabilități, care prevede asigurarea drepturilor persoanelor cu dizabilități, în egală măsură cu alți cetățeni la educație, protecție socială, asistență medicală, reabilitare, muncă, viață publică, mediu fizic, transport, paginile web, tehnologii și sisteme informaționale, de comunicare și la alte utilități și servicii la care are acces publicul larg, în scopul promovării incluziunii sociale a persoanelor cu dizabilități și asigurării respectării drepturilor fundamentale ale acestora, în condiții de egalitate cu ceilalți cetățeni, inclusiv prin promovarea limbajului mimico-gestual şi alte moduri alternative de comunicare în calitate de mijloace de comunicare între persoane. În context, pe parcursul textului proiectului de lege notat:	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	6.1	- sintagma „persoane cu handicap” urmează a fi corelat cu noțiunea din Legea nr. 60/2012, în speță: „persoană cu dizabilități” (persoană cu deficienţe fizice, mintale, intelectuale sau senzoriale, deficienţe care, în interacţiune cu diverse bariere/obstacole, pot îngrădi participarea ei deplină şi eficientă la viaţa societăţii în condiţii de egalitate cu celelalte persoane). Astfel, menționăm, că la componenta de incluziune a persoanelor cu dizabilități, se va ține cont de reglementarea normelor propuse de principiul facilitării accesibilității măsurilor stabilite și a impactului acestor măsuri pentru toate persoanele cu dizabilități, în condiții de egalitate cu ceilalți, la informație și la mijloacele de comunicare, nu doar pentru persoanele cu dizabilități vizuale, dar și auditive;	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	6.2	- textul „persoanele care se confruntă cu limitări funcționale” urmează a fi completat cu cuvântul „senzoriale”;	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	6.3	- textul „limbaj clar și inteligibil” urmează a fi completat cu „ , inclusiv accesibil persoanelor cu deficiențe de auz și vedere”. Prioritate, conform agendei de aderare a Republicii Moldova la Uniunea Europeană, este inclusiv și transpunerea Directivei (UE) 2019/882, privind cerințele de accesibilitate aplicabile produselor și serviciilor, care are scopul de a contribui la buna funcționare a pieței interne, prin apropierea actelor cu putere de lege și a actelor administrative ale statelor membre în ceea ce privește cerințele de accesibilitate aplicabile anumitor produse și servicii, în special prin eliminarea și prevenirea barierelor din calea liberei circulații a anumitor produse și servicii accesibile, bariere care decurg din cerințe de accesibilitate divergente ale statelor membre (la etapa actuală Ministerul a elaborat proiectul de lege de transpunere, număr unic 45/MMPS/2026, și transmis spre coordonare către Comisia Europeană). În contextul celor menționate, considerăm oportun definitivarea proiectului prenotat în corespundere cu prevederile Legii nr. 60/2012 privind incluziunea socială a persoanelor cu dizabilități, propunerile înaintate și prevederile Directivei (UE) 2019/882, privind cerințele de accesibilitate aplicabile produselor și serviciilor, cu asigurarea implementării acestora, prin prisma drepturilor	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		fundamentale ale persoanelor cu dizabilități, în egală măsură cu ceilalți cetățeni.	
Ministerul Afacerilor Interne (Nr.38/1829 din 07.05.2026)	7.1	La art. 5 alin. (18), se constată o eroare gramaticală în sintagma „Orice prelucrare a datelor cu caracter personal efectuată furnizorii...”, motiv pentru care aceasta necesită a fi revizuită.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	7.2	La art. 8 alin. (4), se constată o formulare incorectă în sintagma „informațiile înregistrare în lista...”, motiv pentru care aceasta urmează a fi substituită cu forma corectă din punct de vedere gramatical.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	7.3	Textul propus la art. 9 alin. (4) este incomplet și necesită reformulare. Se recomandă revizuirea acestuia, întrucât structura actuală nu conține un verb și nu exprimă o idee completă.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	7.4	Articolul 18 alineatul (1), se propune de a fi expus în următoarea redacție: „(1) Serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați cu sediul într-un stat membru al Uniunii Europene sau în orice altă țară cu care Republica Moldova a încheiat un acord de recunoaștere reciprocă sunt recunoscute în Republica Moldova 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.”. În contextul reglementărilor proiectului, se recomandă precizarea că efectul juridic privilegiat vizează serviciile de încredere calificate prestate de prestatori calificați, și nu orice serviciu de încredere prestat în Uniunea Europeană.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	7.5	Articolul 22 alineatele (6)–(8), se propune de a fi expuse în următoarea redacție: „(6) Prestatorii de servicii de încredere calificați cu sediul în statele membre ale Uniunii Europene pot presta în Republica Moldova servicii de încredere calificate în baza notificării privind intenția de a presta serviciile respective pe teritoriul Republicii Moldova, transmisă organismului de supraveghere, fără 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 de calificat al prestatorului și al serviciului de încredere calificat în lista sigură a statului membru al Uniunii Europene în care	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		acesta este stabilit și, în cazul confirmării statutului, asigură includerea informațiilor relevante în lista sigură prevăzută la art. 23. (8) În cazul retragerii statutului de calificat al prestatorului de servicii de încredere sau al serviciului de încredere calificat într-un stat membru al Uniunii Europene, organismul de supraveghere radiază fără întârziere înregistrarea relevantă din lista sigură prevăzută la art. 23.”. Propunerea este necesară pentru a preciza că verificarea privește atât prestatorul, cât și serviciul calificat. În contextul celor expuse, Ministerul Afacerilor Interne susține promovarea proiectului, cu integrarea propunerilor de modificare și a obiecțiilor formulate supra.	
Centrul de Armonizare a Legislației (Nr. 31/02-126-5200 din 07.05.2026)	8.1	*Analiza comparativă a transpunerii Regulamentului (UE) nr. 910/2014* În ceea ce privește transpunerea Regulamentului (UE) nr. 910/2014, apreciem că proiectul național asigură transpunerea parțială a actului UE, cu observațiile de mai jos.	**Se acceptă.**
	8.2.1	*Observații de compatibilitate cu Regulamentul (UE) nr. 910/2014* - Cu referire la art. 10, alin. (2) din proiectul național referitor la furnizorii de servicii din sectorul privat care solicită identificarea sau autentificarea electronică a utilizatorilor acceptă utilizarea portofelelor pentru identitatea digitală, se va specifica că obligația respectivă nu se răsfrânge asupra microîntreprinderilor și întreprinderilor mici potrivit Legii nr. 179/2016 cu privire la întreprinderile mici şi mijlocii (aflată în curs de modificare pentru aliniere la Recomandarea 2003/361/CE a Comisiei) similar art. 5f (2) din Regulamentul UE;	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	8.2.2	Art. 69, alin. (1) din proiectul național stabilește că, art. 67 și 68, care se referă la sancțiunile pentru încălcarea prevederilor Legii se pun în aplicare doar din momentul aderării Republicii Moldova la Uniunea Europeană. O asemenea abordare este incorectă juridic și afectează punerea în aplicare eficientă a cadrului normativ armonizat în domeniul identificării electronice. În măsura în care, intenția autorului este de a institui un regim sancționator	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.

		similar cu cel UE doar din data aderării la UE, se impune stabilirea unor norme sancționatorii tranzitorii, adaptate la realitățile pieței RM, valabile până la data aderării la UE pentru a nu crea un vid legislativ și a distorsiona efectul util al reglementării naționale.	
	8.2.3	Proiectul național nu a asigurat transpunerea unor norme obligatorii din actul UE, care nu pot fi implementate/transpuse de RM în calitate de stat candidat la aderare și vor fi aplicate direct din data aderării la UE, după cum urmează: art. 4; art. 5b (7); art. 5c (7); art. 5d; art. 7; art. 9; art. 10; art. 11; art. 11a (5); art. 20 (1b); art. 22 (3); art. 30 (2); art. 31; art. 45f (2) și (3); art. 46a (2) și (6); art. 46b (2) și (6); art. 46c (3); art. 46d; art. 48a (4). Aceste norme vor fi calificate în Tabelul de concordanță ca ”Prevederi UE netranspuse”, cu explicația imposibilității aplicării de RM ca stat candidat și aplicarea directă a acestora prin efectul direct al Regulamentului UE.	**Se acceptă.** Tabelul a fost modificat conform propu-nerii.
	8.2.4	Reieșind din considerentul că, obiect al transpunerii este un Regulament UE, care va deveni direct aplicabil din data aderării la UE, precum și ținând cont de faptul că, prin proiectul național numeroase atribuții ale Comisiei Europene sunt atribuite la nivel național autorității de supraveghere, se impune completarea art. 69 cu un nou alineat care va prevedea abrogarea Legii din data intrării în vigoare a Tratatului de aderare a RM la UE. Pot fi menținute în vigoare și după momentul aderării la UE doar prevederile proiectului care desemnează autoritățile responsabile și punctele de contact, stabilesc anumite proceduri naționale mai detaliate, reglementează procedura de cooperare dintre autoritatea națională și Comisia Europeană, Grupul de lucru și autoritățile din alte state membre, precum și prevederile de sancționare.	**Nu se acceptă.** Instituirea, în acest moment, a unei clauze de abrogare automată la data intrării în vigoare a Tratatului de aderare la Uniunea Europeană nu este oportună și nu corespunde principiilor de previzibilitate și securitate juridică, întrucât cadrul normativ european și cel național în materie sunt în continuă evoluție. Atât Regulamentul (UE) nr. 910/2014, cât și legislația națională aferentă sunt susceptibile de modificări până la momentul aderării, inclusiv în ceea ce privește actele de implementare și standardele tehnice aplicabile. În aceste condiții, nu este posibilă stabilirea în mod cert, la etapa actuală, a normelor care vor necesita menținere, ajustare sau abrogare la momentul aderării. De asemenea, o parte semnificativă a dispozițiilor proiectului are caracter instituțional și

			operațional, fiind destinate să asigure funcționarea autorităților naționale competente și a mecanismelor de implementare, elemente care vor necesita o evaluare ulterioară în funcție de arhitectura finală a cadrului european și național la momentul aderării. În acest context, soluția juridică adecvată este realizarea unei intervenții legislative într-o etapă apropiată de momentul aderării, printr-un exercițiu distinct de revizuire și armonizare, care să permită ajustarea punctuală, inclusiv abrogarea totală sau parțială a legii, în funcție de forma finală a acquis-ului european și de opțiunile instituționale ale Republicii Moldova la acel moment.
	8.3	*Observații privind clauza de armonizare* Clauza de armonizare a proiectului național se va expune în următoarea redacție: „Prezenta Lege transpune parțial Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directive 1999/93/CE, publicat în Jurnalul Oficial al Uniunii Europene L 257/73 din 28 august 2014, CELEX: 32014R0910, așa cum a fost modificat ultima dată prin Regulamentul (UE) nr. 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	8.4.1	*Obiecții privind tabelul de concordanță* Tabelul de concordanță pentru Regulamentul (UE) nr. 910/2014 urmează a fi revizuit, după cum urmează: Gradul general de compatibilitate va fi „Parțial compatibil”;	**Se acceptă.** Tabelul a fost modificat conform propunerii.
	8.4.2	Pentru art. 4; art. 5b (7); art. 5c (7); art. 5d; art. 7; art. 9; art. 10; art. 11; art. 11a (5); art. 20 (1b); art. 22 (3); art. 30 (2); art. 31; art. 45f (2) și (3); art. 46a (2) și (6); art. 46b (2) și (6); art. 46c	**Se acceptă.** Tabelul a fost modificat conform propunerii.

		(3); art. 46d; art. 48a (4) din actul UE, calificativul de compatibilitate va fi ”Prevederi UE netranspuse”, cu motivația aplicării directe din data aderării la UE;	
	8.4.3	Pentru celelalte prevederi UE netranspuse de proiect, în speță, cele ce vizează atribuțiile CE și altor organisme UE, dispoziții finale și tranzitorii va fi păstrat calificativul ”Prevederi UE neaplicabile”.	**Se acceptă.** Tabelul a fost modificat conform propunerii.
	8.5	*Concluzii* Ca urmare a expertizei de compatibilitate realizate, proiectul național și instrumentele de armonizare (clauza de armonizare și tabelul de concordanță) se vor revizui potrivit obiecțiilor formulate în prezenta Declarație de compatibilitate. Facem mențiunea că analiza Centrului de armonizare a legislației nu are în vedere elementele de oportunitate ale soluțiilor juridice incluse în proiectul de act normativ, ci se referă strict la conformitatea acestora cu Dreptul UE aplicabil și obligațiile juridice asumate în lumina Acordului de Asociere RM-UE și Cadrului de negociere cu Uniunea Europeană.	**Se acceptă.** Tabelul a fost modificat conform propunerii.
EUROPARC S.R.L (Nr. 1 din 08.05.2026)	9.1	*I. INTRODUCERE ȘI TEMEIUL SESIZĂRII* După o analiză aprofundată a proiectului de lege, a notei de fundamentare, a tabelului de concordanță și a Regulamentului (UE) 2024/1183, constatăm că proiectul de lege, în forma sa actuală, conține vicii fundamentale de procedură, de fond și de aliniere la cadrul european, care, dacă nu sunt remediate, vor conduce la monopolizarea unui sector strategic, la prejudicierea bugetului de stat și la încălcarea angajamentelor internaționale ale Republicii Moldova. *A. Absența Analizei Impactului de Reglementare (AIR)* Legea nr. 100/2017 cu privire la actele normative stabilește, în art. 21–30, obligația imperativă a autorității care elaborează un proiect de act normativ de a efectua Analiza Impactului de Reglementare (AIR). Această obligație nu este o formalitate - este o condiție de fond a procesului legislativ, a cărei nerespectare viciază întregul parcurs de adoptare.	**Se acceptă parțial.** Capitolul 4 Analiza impactului de reglementare din Nota de fundamentare la proiectul de lege privind identificarea electronică și serviciile de încredere a fost completată în conformitate cu prevederile Metodologiei de analiză a impactului de reglementare, aprobată prin HG nr. 574/2024. Totodată, în baza propunerilor recepționate în proces de avizare Nota de fundamentare la proiectul de lege a fost ajustată și completată cu informații suplimentare.

		Nota de fundamentare a proiectului de lege, elaborată de Ministerul Dezvoltării Economice și Digitalizării, nu conține o Analiză a Impactului de Reglementare conform cerințelor art. 21–30 din Legea nr. 100/2017. În mod specific: (i) Nu este evaluat impactul asupra concurenței. Nota de fundamentare nu analizează în niciun mod impactul proiectului asupra pieței serviciilor de încredere, asupra prestatorilor privați existenți și potențiali, și asupra concurenței în general. Desemnarea nominală a Agenției de Guvernare Electronică (AGE) ca furnizor unic al portofelului digital - o decizie cu impact concurențial major - nu este supusă niciunei analize de impact. (ii) Nu este evaluat impactul financiar real. Nota de fundamentare afirmă, în mod nerealist, că proiectul "nu implică, în mod direct, cheltuieli suplimentare din bugetul de stat». Această afirmație este contrazisă de însăși structura proiectului: AGE, finanțată integral din bugetul de stat, este desemnată ca furnizor, operator, dezvoltator și administrator al portofelului digital național. (iii) Nu sunt evaluate opțiunile alternative de reglementare. Art. 22 din Legea nr. 100/2017 impune analiza a cel puțin două opțiuni alternative. Deși nota de fundamentare menționează formal trei opțiuni, niciuna nu analizează alternativa unui cadru concurențial deschis versus monopolul de stat. (iv) Nu este evaluat impactul asupra sectorului privat. Secțiunea 4.3 a notei de fundamentare descrie impactul asupra sectorului privat exclusiv în termeni de beneficii ale digitalizării, ignorând complet prejudiciul adus prestatorilor de servicii de încredere existenți. Consecința juridică: Absența AIR constituie o încălcare a art. 21–30 din Legea nr. 100/2017, care poate fi invocată ca viciu de procedură în fața instanțelor de contencios administrativ. Solicităm Ministerului efectuarea integrală a AIR, cu publicarea rezultatelor și supunerea acestora dezbaterii publice. *B. Transpunerea deformată a Regulamentului (UE) 2024/1183* Proiectul de lege pretinde că transpune Regulamentul (UE) nr. 910/2014 astfel cum a fost modificat prin Regulamentul (UE)	

		2024/1183 (eIDAS 2.0). Analiza comparativă a textelor relevă o transpunere selectivă și deformată, prin care: • se preia obligația statelor membre de a asigura disponibilitatea a cel puțin unui portofel digital, dar se transformă în desemnare nominală a unei instituții publice specifice (AGE) ca furnizor unic; • se ignoră principiul neutralității concurențiale consacrat în considerentul (19) al Regulamentului eIDAS 2.0; • se omite obligația de recunoaștere automată a prestatorilor calificați din statele membre UE, înscriși în Trusted List; • se substituie standardele tehnice europene (ETSI EN 319 411-2, ETSI TS 119 471/472) cu „standardele și specificațiile tehnice stabilite de Guvern”.	**Se acceptă parțial.** În baza propunerilor recepționate în proces de avizare art. 5 alin. (1) din proiectul de lege a fost revizuit.
	9.2	*III. MONOPOLIZAREA SECTORULUI PRIN DESEMNAREA NOMINALĂ A AGE* Art. 5 alin. (1) din proiectul de lege desemnează, în mod nominal și direct, Instituția Publică Agenția de Guvernare Electronică (AGE) ca furnizor al portofelului pentru identitatea digitală. Această desemnare, realizată la nivel de lege organică, generează un monopol de stat cu consecințe juridice și economice grave. *A. Monopolul de drept și de fapt* Desemnarea prin lege organică a unui furnizor unic creează un monopol de drept. Deși proiectul admite formal existența altor furnizori, lipsa unei proceduri transparente și nediscriminatorii de certificare, combinată cu avantajele structurale ale AGE, transformă monopolul de drept într-un monopol de fapt: 1. Finanțare bugetară directă. AGE beneficiază de finanțare integrală din bugetul de stat pentru dezvoltarea, operarea și mentenanța portofelului digital. Niciun prestator privat nu beneficiază de această subvenționare. 2. Acces preferențial la registrele de stat. AGE are acces direct și prioritar la bazele de date ale statului (registrul populației, registrul întreprinderilor etc.), un avantaj esențial pentru furnizarea serviciilor de identificare electronică.	**Se acceptă parțial.** În baza propunerilor recepționate în proces de avizare art. 5 alin. (1) din proiectul de lege a fost revizuit.

		3. Recunoaștere automată. AGE nu este supusă procedurii de evaluare și certificare pe care o parcurg ceilalți prestatori, beneficiind de recunoaștere automată prin lege. B. AGE - instituție publică care acționează ca operator comercial Agenția de Guvernare Electronică, deși are statut de instituție publică finanțată din bugetul de stat, acționează în practică ca un operator comercial (similar unui SRL), concentrând funcții de dezvoltator, furnizor, operator și administrator al soluțiilor de identificare electronică. Această dualitate generează un conflict structural: - AGE este simultan beneficiară a reglementării (în calitate de furnizor desemnat) și participantă la elaborarea cadrului normativ care o avantajează; - AGE utilizează fonduri publice pentru a concura (sau, mai exact, a elimina concurența) pe o piață care ar trebui să fie deschisă; - AGE nu este supusă aceluiași regim fiscal, de raportare financiară și de audit ca prestatorii privați. Poziția noastră este fermă: dacă AGE dorește să acționeze ca operator pe piața serviciilor de încredere, aceasta trebuie să fie supusă aceluiași regim juridic, fiscal și concurențial ca orice alt prestator privat. AGE poate și trebuie să aibă un rol de regulator, dar nu poate fi simultan regulator și operator dominant pe piața pe care o reglementează. *C. Prejudiciul adus bugetului de stat* Monopolizarea sectorului de către AGE generează un prejudiciu financiar direct bugetului de stat: - costurile de dezvoltare, mentenanță, actualizare și operare continuă a portofelului digital sunt suportate integral din fonduri publice, în condițiile în care piața privată ar putea furniza aceleași servicii fără cost bugetar; - gratuitatea semnăturii electronice calificate, impusă prin art. 5 alin. (10) pct. 8), fără un mecanism de compensare transparent, înseamnă că bugetul de stat subvenționează exclusiv AGE;	

		- lipsa de concurență elimină orice stimulent de eficiență, generând costuri disproporționate față de valoarea reală a serviciilor furnizate.	
	9.3	*IV. DESEMNAREA SIS CA ORGANISM DE SUPRAVEGHERE - ANOMALIE INSTITUȚIONALĂ* Art. 64 alin. (1) din proiectul de lege desemnează Serviciul de Informații și Securitate al Republicii Moldova (SIS) ca organism de supraveghere a cadrului pentru portofelul digital și a serviciilor de încredere. Această desemnare este lipsită de precedent în spațiul european. *A. Încălcarea standardului european* În toate statele membre ale Uniunii Europene, atribuțiile de supraveghere a pieței serviciilor de încredere sunt exercitate de autorități civile: - Franța: ANSSI (Agence nationale de la sécurité des systèmes d'information); - Germania: BSI (Bundesamt für Sicherheit in der Informationstechnik); - Italia: AgID (Agenzia per l'Italia Digitale); - România: ADR (Autoritatea pentru Digitalizarea României). Niciun stat membru al Uniunii Europene nu deleagă atribuțiile de reglementare a pieței digitale unui serviciu de informații. Atribuțiile prevăzute de proiect (acordarea/retragerea statutului de calificat, ținerea listei sigure, auditul tehnic, raportarea către Parlament) au natură pur administrativ-tehnică și de reglementare a pieței, nu operativ-informativă. *B. Efect de descurajare a investițiilor* Implicarea unui serviciu de informații în deciziile de avizare și supraveghere a prestatorilor are un efect devastator asupra atractivității pieței moldovenești: - prestatorii europeni calificați, înscriși în Trusted List UE, vor ezita să se supună supravegherii unui serviciu de informații; - investitorii străini în sectorul digital vor percepe această alegere instituțională ca un semnal de risc, incompatibil cu standardele europene de guvernanță;	**Se acceptă de principiu.** Obiecția este reținută ca fiind relevantă din perspectiva alinierii la bunele practici europene privind separarea funcțiilor de supraveghere în domeniul serviciilor de încredere și al portofelelor pentru identitatea digitală, acestea fiind exercitate, în mod obișnuit, de autorități civile specializate. Totuși, la etapa actuală, Serviciul de Informații și Securitate exercită deja atribuții de supraveghere în domeniul vizat, iar proiectul de lege urmărește asigurarea continuității instituționale, în contextul angajamentelor Republicii Moldova de transpunere într-un termen restrâns a Regulamentului (UE) nr. 910/2014 și a cadrului aferent. În lipsa unei autorități publice alternative care să dispună în prezent de capacitățile instituționale necesare pentru preluarea integrală a acestui mandat, se optează pentru menținerea soluției propuse în proiect. Totodată, se reține necesitatea analizării, în perioada imediat următoare, a opțiunilor de reconfigurare instituțională a funcției de supraveghere, inclusiv prin identificarea și consolidarea capacităților unei autorități civile specializate, în vederea unei eventuale preluări a acestui mandat într-un cadru ulterior de ajustare legislativă.

		- încrederea utilizatorilor în confidențialitatea datelor gestionate prin portofelul digital va fi subminată.	
	9.4	*V. ÎNCĂLCAREA ANGAJAMENTELOR INTERNAȚIONALE* *A. Acordul de Asociere RM-UE* Proiectul de lege contravine în mod direct angajamentelor asumate de Republica Moldova prin Acordul de Asociere cu Uniunea Europeană: Art. 47 (Servicii): Republica Moldova s-a angajat să asigure un mediu deschis și concurențial pentru prestarea serviciilor. Monopolizarea sectorului serviciilor de încredere de către o instituție publică finanțată din buget contravine direct acestui angajament. Art. 50 (Recunoaștere reciprocă): Acordul prevede recunoașterea reciprocă a standardelor. Proiectul de lege, prin absența unui mecanism de recunoaștere automată a prestatorilor din Trusted List UE, creează bariere care încalcă spiritul și litera acestui angajament. Art. 102 (Concurență): Acordul prevede alinierea la regulile UE în materie de concurență, inclusiv în ceea ce privește ajutoarele de stat. Finanțarea bugetară a AGE ca operator pe o piață concurențială constituie un ajutor de stat care denaturează concurența, în sensul art. 339–342 din Acordul de Asociere. *B. Programul național de aderare 2025–2029 și Planul de creștere 2025–2027* Paradoxal, nota de fundamentare invocă ea însăși Programul național de aderare (Clusterul 3, capitolul 10, acțiunea 11) și Planul de creștere 2025–2027 (măsura 2-3-10-MDED) ca temei. Însă, proiectul de lege contravine tocmai obiectivelor acestor documente strategice: - Programul de aderare prevede alinierea la cadrul UE, nu crearea unui monopol de stat absent din modelul european; - Planul de creștere vizează dezvoltarea ecosistemului digital, nu concentrarea acestuia în mâinile unei singure instituții publice; - ambele documente presupun o piață deschisă și concurențială, incompatibilă cu mecanismele de monopolizare instituite prin proiect.	**Se acceptă parțial.** În baza propunerilor recepționate în proces de avizare art. 5 alin. (1) din proiectul de lege a fost revizuit.

		C. Regulamentul eIDAS 2.0 - analiza prevederilor anti-monopol, de protecție a investițiilor și privind serviciile contra cost O analiză sistematică a Regulamentului (UE) 2024/1183 (eIDAS 2.0) relevă că acesta conține un sistem coerent de garanții anti-monopol și de protecție a pieței, pe care proiectul moldovenesc le ignoră deliberat: *C.1. Interzicerea monopolului și obligația de pluralitate a furnizorilor* Considerentul (16): prevede explicit că portofelele pot fi furnizate direct de către un stat membru, în temeiul unui mandat, sau independent dar recunoscute de statul membru. Regulamentul oferă trei modalități alternative - nicidecum o desemnare nominală a unui furnizor unic. Art. 5a alin. (2): transpune considerentul (16) în normă juridică obligatorie, prevăzând trei moduri de furnizare: (a) direct de stat, (b) pe bază de mandat, (c) independent dar recunoscut. Proiectul moldovenesc ignoră opțiunile (b) și (c). Considerentul (48): prevede explicit că Regulamentul "ar trebui să încurajeze alegerea și posibilitatea de a trece de la un portofel la altul în cazul în care un stat membru a aprobat mai multe soluții". Principiul pluralității furnizorilor și al portabilității - ambele absente din proiectul moldovenesc. Considerentul (49): impune "condiții echitabile, rezonabile și nediscriminatorii" pentru accesul la componentele de hardware și software. *C.2. Neutralitatea tehnologică și interzicerea discriminării* Regulamentul prevede explicit: "Prezentul regulament ar trebui să asigure neutralitatea tehnologică, și anume să nu favorizeze și nici să nu discrimineze nicio tehnologie". Impunerea unui singur furnizor desemnat prin lege este antiteza neutralității tehnologice. Art. 12b: prevede obligația de acces la componentele de hardware și software în condiții echitabile pentru toți furnizorii care acționează "cu titlu comercial sau profesional". Norma recunoaște explicit dimensiunea comercială a pieței. *C.3. Protecția investițiilor existente*	

		Regulamentul recunoaște explicit investițiile realizate: "s-au realizat investiții în soluții naționale și transfrontaliere pe baza Regulamentului (UE) nr. 910/2014". Statele membre au obligația de a proteja aceste investiții, nu de a le anula prin monopolizare. Proiectul moldovenesc, prin abrogarea Legii 124/2022 fără regim tranzitoriu adecvat, distruge investițiile deja realizate. *C.4. Serviciile de încredere - contra cost, nu gratuite pentru business* Definiția serviciului de încredere (art. 3 pct. 16): "serviciu electronic prestat în mod obișnuit în schimbul unei remunerații". Regulamentul definește serviciul de încredere ca un serviciu COMERCIAL, prestat contra remunerație. Considerentul (20) - Gratuitate STRICT pentru scopuri neprofesionale: "Utilizarea unei semnături electronice calificate ar trebui să fie gratuită pentru toate persoanele fizice în scopuri neprofesionale. Statele membre ar trebui să aibă posibilitatea să prevadă măsuri de prevenire a utilizării gratuite în scopuri profesionale". Prin urmare, pentru scopuri profesionale și comerciale, serviciile de încredere sunt și trebuie să rămână contra cost. Modelul de afaceri: Regulamentul prevede că "statele membre ar trebui să ajungă la un acord cu privire la elementele comune ale unui model de afaceri și ale structurii taxelor aferente portofelelor, pentru a facilita adoptarea acestora, în special de către IMM-uri". Existența unui model de afaceri și a unei structuri de taxe confirmă explicit natura comercială a sectorului. Implicatie directa: proiectul moldovenesc, prin impunerea gratuității generalizate fără distincție între scopuri neprofesionale și profesionale, și fără mecanism de compensare, denaturează fundamental piața. Un model sustenabil impune: (i) gratuitate pentru persoane fizice în scopuri neprofesionale - finanțată din buget pentru TOȚI prestatorii; (ii) contra cost pentru scopuri profesionale/comerciale. *C.5. Concluzie - transpunere selectivă* Proiectul moldovenesc preia din Regulamentul eIDAS 2.0 obligațiile (furnizarea portofelului, gratuitatea, certificarea), dar ignoră sistematic garanțiile (pluralitatea furnizorilor, neutralitatea	

		tehnologică, accesul echitabil, protecția investițiilor, caracterul comercial al serviciilor). Această transpunere selectivă transformă un instrument european de deschidere a pieței într-un instrument de monopolizare - exact contrar scopului Regulamentului. *VI.PREJUDICIUL CONCRET ADUS PIEȚEI ȘI UTILIZATORILOR* *A. Situația actuală a pieței serviciilor de încredere din RM* Piața serviciilor de încredere din Republica Moldova se află deja într-o situație precară, determinată de politicile netransparente și de concentrarea excesivă în jurul furnizorului public: 1. Disfuncționalități frecvente ale semnăturii electronice. Agenții economici din Republica Moldova raportează în mod constant probleme cu funcționarea semnăturii electronice - perioade de indisponibilitate, erori tehnice, incompatibilități - care afectează direct capacitatea de a depune raportări electronice către instituțiile statului (declarații fiscale, raportări financiare, acte procedurale). 2. Dependența de un furnizor unic (vendor lock-in). Concentrarea serviciilor la un singur furnizor public creează o dependență strategică periculoasă: orice defecțiune tehnică paralizează întregul ecosistem de servicii electronice. 3. Absența concurenței = absența inovației. Fără presiune concurențială, nu există niciun stimulent economic pentru AGE de a îmbunătăți calitatea serviciilor sau de a investi în tehnologii noi. 4. Descurajarea prestatorilor UE. Prestatorii de servicii de încredere calificați din spațiul UE, înscriși în Trusted List, sunt descurajați să intre pe piața moldovenească din cauza lipsei de recunoaștere automată și a prezenței unui monopol de stat. *B. Riscuri de securitate și dependență tehnologică* Concentrarea întregii infrastructuri de identitate digitală la o singură instituție publică generează riscuri majore de securitate: - Single point of failure: compromiterea sau indisponibilitatea sistemelor AGE paralizează întreaga identificare electronică din țară;	

		- Dependență de furnizori externi ai AGE: în practică, AGE contractează dezvoltarea soluțiilor sale tehnice către terți, creând dependențe în lanț; - Lipsa diversificării reduce reziliența sistemului național în fața atacurilor cibernetice. *VII. ASPECTE PRIVIND DREPTUL CONCURENȚEI ȘI AJUTORUL DE STAT* Mecanismele instituite prin proiectul de lege ridică probleme serioase din perspectiva dreptului concurenței și a regimului ajutoarelor de stat. *A. Cumulul inadmisibil de roluri al AGE - fără precedent european* Analiza proiectului de lege relevă că Agenția de Guvernare Electronică concentrează un număr de roluri care, în practica europeană, sunt distribuite obligatoriu între entități distincte, tocmai pentru a evita conflictele de interese și abuzul de poziție dominantă. AGE cumulează, fără a se limita la acestea, următoarele funcții: (i) Promotor al politicilor de digitalizare. AGE elaborează și promovează politicile publice de digitalizare, stabilind prioritățile și direcțiile strategice ale sectorului. Acest rol îi conferă capacitatea de a modela cadrul de reglementare în propriul avantaj. (ii) Posesor și operator al Platformei de Interoperabilitate (MConnect). AGE deține și operează platforma de interoperabilitate - un monopol de stat prin care tranzitează toate schimburile de date între sistemele informaționale publice și private. Prin proiectul de lege, se pretinde că această platformă va fi utilizată și pentru emiterea atestatului electronic al atributelor pentru portofelele digitale - în condițiile în care, conform eIDAS 2.0 (art. 45d), atestatele electronice ale atributelor trebuie emise de fiecare deținător de registre (surse autentice), nu de un intermediar unic. (iii) Posesor și administrator al Portalului EVO. AGE deține și administrează Portalul guvernamental integrat EVO, impus ca canal unic de înregistrare a beneficiarilor (art. 6 alin. 4). Acest lucru elimină orice alternativă de canal digital.	

		(iv) Furnizor desemnat al portofelului digital. Prin art. 5 alin. (1), AGE este desemnată direct, prin lege organică, ca furnizor al portofelului pentru identitatea digitală. (v) Entitate care stabilește reguli, le execută și le controlează simultan. AGE participă la elaborarea cadrului normativ, operează infrastructura pe baza regulilor pe care le-a contribuit la elaborare, și beneficiază de recunoaștere automată fără a parcurge procedurile impuse celorlalți. Această tripletă - a stabili reguli, a le executa și a le controla - este antiteza principiului separării funcțiilor. Nicio practică europeană nu admite un astfel de cumul. În statele membre UE, funcțiile de promotor de politici, operator de platforme, furnizor de servicii de încredere și autoritate de supraveghere sunt exercitate de entități distincte. *B. Ajutor de stat ilegal* Finanțarea bugetară directă a AGE pentru activități care se desfășoară pe o piață concurențială constituie un ajutor de stat în sensul art. 3 din Legea concurenței nr. 183/2012 și al art. 339–342 din Acordul de Asociere RM-UE: - acordă un avantaj economic selectiv (doar AGE beneficiază de finanțare bugetară directă); - prin resurse de stat (bugetul public); - care denaturează sau amenință să denatureze concurența; - și afectează schimburile comerciale (în contextul Acordului de Asociere). *C. Abuz de poziție dominantă - analiză detaliată* Prin cumulul fără precedent de roluri descris mai sus, AGE dobândește o poziție dominantă absolută pe piața serviciilor de încredere din RM. Abuzul se manifestă prin: 1. Bariere de intrare artificiale: absența unei proceduri clare, transparente și nediscriminatorii de certificare, combinată cu recunoașterea automată a AGE prin lege. 2. Controlul accesului la resurse esențiale: AGE controlează platforma de interoperabilitate (MConnect) și portalul EVO - infrastructuri esențiale (essential facilities) pentru orice prestator. Re-	

		fuzul sau condiționarea accesului constituie abuz de poziție dominantă în sensul jurisprudenței europene (doctrina essential facilities). 3. Subvenționare încrucișată: AGE utilizează finanțarea bugetară primită pentru funcțiile sale publice (promovarea politicilor, interoperabilitate) pentru a subvenționa activitățile sale comerciale (furnizarea portofelelor digitale) - interzisă de dreptul concurenței. 4. Prețuri de ruinare: gratuitatea impusă prin art. 5 alin. (10) pct. 8), combinată cu finanțarea bugetară a AGE, creează un mecanism de prețuri de ruinare (predatory pricing): AGE poate oferi gratuit ceea ce prestatorii privați trebuie să furnizeze contra cost. 5. Excluderea verticală: prin controlul simultan al platformei de interoperabilitate (infrastructură), al portalului de înregistrare (distribuție) și al portofelului digital (serviciu final), AGE realizează o integrare verticală completă care exclude orice concurență pe fiecare nivel al lanțului de valoare.	
	9.5	*VIII. PROPUNERI CONCRETE DE MODIFICARE* Pentru remedierea neconformităților fundamentale identificate, formulăm următoarele propuneri concrete: Propunerea 1: Eliminarea desemnării nominale a AGE din art. 5 alin. (1) și înlocuirea cu o procedură transparentă și nediscriminatorie de desemnare a furnizorului/furnizorilor. Propunerea 2: Instituirea unui mecanism explicit de compensare bugetară către toți prestatorii calificați pentru gratuitatea semnăturii electronice calificate, eliminând subvenționarea ascunsă a furnizorului public. Propunerea 3: Eliminarea canalului unic de înregistrare (Portalul EVO) din art. 6 alin. (4) și deschiderea ecosistemului către orice mijloc electronic acceptat de organismul de supraveghere. Propunerea 4: Trimitere expresă la standardele europene (ETSI EN 319 411-2, ETSI TS 119 471/472, ISO/IEC 18013-5) în certificarea portofelelor digitale.	**Se acceptă parțial.** Propunerea 1: În urma procesului de avizare, art. 5 alin. (1) a fost revizuit într-o formulare neutră instituțional și tehnologic, eliminând referința expresă la o anumită entitate publică. Totodată, proiectul stabilește posibilitatea furnizării portofelelor pentru identitatea digitală atât de organisme din sectorul public desemnate de Guvern, cât și de persoane juridice de drept privat, cu respectarea cerințelor prevăzute de lege. Suplimentar, proiectul consacră expres principiul liberei alegeri a utilizatorului, garantând dreptul acestuia de a selecta liber portofelul pentru identitatea digitală utilizat și excluzând obligativitatea utilizării unui anumit furnizor.

		Propunerea 5: Ancorarea nivelurilor de asigurare în Regulamentul de implementare (UE) 2015/1502, nu în acte discreționare ale Guvernului. Propunerea 6: Recunoașterea automată a prestatorilor calificați din Trusted List UE, cu notificare simplă către organismul de supraveghere. Propunerea 7: Excluderea SIS ca organism de supraveghere și transferul atribuțiilor către un departament specializat în cadrul MDED, cu autonomie funcțională sau unui alt organ de reglementare în domeniu. Propunerea 8: Introducerea unui articol nou (art. 4[1]) privind libera alegere a furnizorului de către utilizator, cu interdicția impunerii unui furnizor anume și dreptul la portabilitatea datelor. Propunerea 9: Clauză tranzitorie pentru prestatorii existenți, care să protejeze drepturile dobândite și să asigure continuitatea serviciilor. *IX. CONCLUZII ȘI SOLICITĂRI* Proiectul de lege privind identificarea electronică și serviciile de încredere, în forma sa actuală, sub pretextul transpunerii Regulamentului eIDAS 2.0, instituie un mecanism de monopolizare a unui sector strategic, contrar: - Constituției Republicii Moldova (art. 126 - libera concurență); - Legii nr. 100/2017 cu privire la actele normative (art. 21–30 - AIR); - Legii concurenței nr. 183/2012 (art. 3, 11 - ajutor de stat, abuz de poziție dominantă); - Acordului de Asociere RM-UE (art. 47, 50, 102); - Regulamentului (UE) 2024/1183 - eIDAS 2.0 (principiul neutralității concurențiale); - Programului național de aderare 2025–2029 și Planului de creștere 2025–2027. *SOLICITĂM:*	Propunerea 2: Instituirea unui mecanism general și expres de compensare bugetară pentru toți prestatorii de servicii de încredere calificați depășește obiectul de reglementare al proiectului de lege, care stabilește cadrul juridic aplicabil identificării electronice și serviciilor de încredere, și nu mecanismele de finanțare sau de subvenționare a activităților economice desfășurate de prestatori. În același timp, gratuitatea anumitor servicii pentru utilizatori nu implică automat obligația statului de a institui un mecanism universal de compensare pentru operatorii privați, în special în condițiile existenței unui ecosistem concurențial și a libertății operatorilor economici de a-și stabili propriile modele de afaceri și portofolii de servicii. Prin urmare, instituirea unui asemenea mecanism nu este considerată oportună și necesară în cadrul prezentei reglementări. Propunerea 3: În urma avizării, prevederea care făcea referire expresă la Portalul guvernamental integrat EVO a fost eliminată, iar art. 6 alin. (2) a fost reformulat într-o manieră neutră tehnologic, stabilind că procesul de înregistrare se desfășoară în format electronic, în modul stabilit de Guvern. Propunerea 4: Standardele tehnice europene aplicabile certificării portofelelor pentru identitatea digitală, inclusiv standardele ETSI și ISO relevante cuprinse în actele de implementare adoptate de Comisia Europeană în aplicarea Regulamentului (UE) nr. 910/2014, urmează să fie transpuse și detaliate prin Hotărâri de Guvern.

		1. Efectuarea integrală a Analizei Impactului de Reglementare conform art. 21–30 din Legea nr. 100/2017, cu evaluarea impactului asupra concurenței, a sectorului privat și a bugetului de stat, și publicarea rezultatelor AIR pentru dezbatere publică. 2. Modificarea substanțială a proiectului de lege în conformitate cu propunerile formulate în secțiunea VIII a prezentei sesizări, în special prin: a) eliminarea desemnării nominale a AGE și instituirea unei proceduri concurențiale transparente; b) recunoașterea automată a prestatorilor calificați din Trusted List UE; c) înlocuirea SIS cu o autoritate civilă de supraveghere; d) ancorarea standardelor tehnice în normele europene (ETSI, ISO/IEC); e) introducerea principiului liberei alegeri a furnizorului. 3. Organizarea unei dezbateri publice efective cu participarea sectorului privat, a asociațiilor profesionale și a experților independenți. 4. Asigurarea conformării proiectului cu angajamentele internaționale ale Republicii Moldova, în special cu Acordul de Asociere RM-UE.	Introducerea expresă în lege a unor standarde tehnice specifice nu este oportună, întrucât acestea sunt susceptibile de actualizări periodice și evoluții tehnice continue. Menținerea neutralității tehnologice și a flexibilității cadrului normativ impune reglementarea acestora la nivel subsecvent, prin hotărâri ale Guvernului și specificații tehnice dedicate. Propunerea 5: Regulamentul de punere în aplicare (UE) 2015/1502 urmează a fi transpus printr-o Hotărâre de Guvern ce va fi aprobată anterior intrării în vigoare a legii. Prin urmare, nivelurile de asigurare aplicabile mijloacelor de identificare electronică sunt propuse a fi stabilite prin lege, iar specificațiile și procedurile tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică vor fi stabilite în conformitate cu standardele europene relevante, fără a fi necesară reiterarea expresă a acestora în textul legii. Propunerea 6: Normele propuse la art. 22 alin. (6) și (7) prevăd expres că prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene își păstrează statutul de calificat pe teritoriul Republicii Moldova fără necesitatea unor proceduri suplimentare de notificare sau verificare, iar organismul de supraveghere va introduce și actualiza automat statutul acestora în lista sigură națională. Prin urmare, proiectul asigură deja un mecanism de recunoaștere automată compatibil cu Trusted List-ul Uniunii Europene. Propunerea 7: Obiecția este reținută ca fiind relevantă din perspectiva alinierii la bunele

			practici europene privind exercitarea funcțiilor de supraveghere de către autorități civile specializate. Totuși, Serviciul de Informații și Securitate exercită deja atribuții în domeniul respectiv, iar proiectul urmărește asigurarea continuității instituționale în contextul transpunerii accelerate a Regulamentului (UE) nr. 910/2014. În lipsa unei alte autorități publice care să dispună, la această etapă, de capacitățile tehnice și instituționale necesare pentru preluarea integrală a mandatului, se menține soluția propusă în proiect. Totodată, se va analiza, într-o etapă ulterioară, posibilitatea transferului acestor atribuții către o autoritate civilă specializată, inclusiv prin consolidarea capacităților instituționale necesare. Propunerea 8: Art. 5 alin. (2) consacră expres principiul liberei alegeri a furnizorului de portofel pentru identitatea digitală, iar art. 5 alin. (5) pct. 7 garantează exercitarea dreptului utilizatorului la portabilitatea datelor. Prin urmare, obiectivele urmărite de propunere sunt deja reflectate în textul proiectului, fără a fi necesară introducerea unui articol distinct suplimentar. Propunerea 9: Art. 70 alin. (1) stabilește expres că prestatorii de servicii de încredere care au obținut anterior statutul de prestator calificat conform Legii nr. 124/2022 își păstrează acest statut, cu obligația prezentării periodice a rapoartelor de audit al conformității.

			Astfel, proiectul asigură continuitatea juridică a activității prestatorilor existenți, protecția drepturilor dobândite și evitarea perturbării serviciilor deja furnizate pe piață.
Ministerul Mediului (Nr.13-05/1537 din 12.05.2026)	10.	Lipsa de obiecții și propuneri.	
Ministerul Finanțelor (Nr.04-06/383 din 11.05.2026)	11.	*Referitor la Nota de fundamentare* În informațiile prezentate la compartimentul 4.2 privind impactul financiar și argumentarea costurilor estimative, autorul indică că eventuale costuri pentru dezvoltarea, integrarea și adaptarea platformelor, sistemelor și serviciilor urmează a fi acoperite din contul resurselor 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, însă fără prezentarea detaliilor în acest sens. În același timp, proiectul prevede următoarele: La Capitolul II Secțiunea 1 Art.5. se relatează că „...Instituția Publică Agenția de Guvernare Electronică asigură disponibilitatea unui portofel pentru identitatea digitală...”. Art.6 alin.(2) indică că „Procesul de înregistrare se desfășoară prin intermediul Portalului guvernamental integrat EVO și este eficient din punct de vedere al costurilor...”. Art.69 alin. (4) stabilește că „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”. Astfel, în vederea implementării acțiunilor ce urmează a fi asigurate de „IP Agenția de Guvernare Electronică”, autorul urmează să estimeze costurile necesare și să identifice sursa de acoperire a acestora.	**Se acceptă.** Nota de fundamentare a fost modificată conform propunerilor recepționate în proces de avizare.

		Cu titlu de informare, în bugetul Cancelariei de Stat la subprogramul bugetar 0303 ”E-transformare a Guvernării” sunt planificate mijloace financiare în sumă de 2200,0 mii lei pentru implementarea măsurii nr.10, reforma 3 din pilonul 2 ”Consolidarea conectivității prin telecomunicații și infrastructură digitală” în vederea dezvoltării serviciului EvoSign în calitate de portofel de identitate digitală la standardele UE. Suplimentar, în propunerile Cancelariei de Stat la proiectul CBTM pentru perioada anilor 2027-2029 se solicită alocațiile suplimentare în acest sens în sumă totală de 15,7 mil lei, inclusiv pe ani: 2027 - 11,8 mil lei, 2028 - 1,9 mil lei, 2029 - 2,0 mil lei, în limita de cheltuieli fiind identificată suma de 4,3 mil lei. Totodată, conform Hotărârii Guvernului 306/2025, în Clusterul 3, Anexa B, Capitolul 10, Acțiunea 7 „Implementarea Portofelului de identitate digitală în conformitate cu EUDI” se indică anul implementării acțiunii decembrie 2027 și costuri estimitive 34,7 mil lei, fără a fi precizată sursa de acoperire a acestor cheltuieli (bugetul de stat și/sau asistență externă). Reieșind din cele relatate, autorul urmează să facă claritate vis-a-vis de argumentarea economico-financiară a proiectului prin prisma celor relatate mai sus, precum și acțiunilor incluse în Criteriile de referință de închidere a negocierilor la aderare (Matrice) care este la moment la etapa de definitivare.	
Asociația Națională a Companiilor din Domeniul TIC (Nr. 766 din 12.05.2026)	12.1	Art. 6 alin. (2) – Înregistrarea exclusiv prin EVO ATIC consideră necesară clarificarea procedurii de înregistrare a beneficiarilor prin EVO, inclusiv pentru companiile deja integrate în ecosisteme digitale și pentru entitățile reglementate. Propunere: Solicităm clarificarea procedurii de înregistrare a beneficiarilor prin EVO și instituirea unor mecanisme simplificate pentru entitățile deja reglementate sau integrate în infrastructuri digitale guvernamentale și sectoriale. Considerăm importantă evitarea duplicării obligațiilor administrative și reutilizarea informațiilor deja disponibile autorităților competente.	**Se acceptă.** Proiectul a fost revizuit, fiind stabilit că procesul de înregistrare a beneficiarilor are loc în mod electronic, urmând ca instrumentele și condițiile să fie stabilite de Guvern.
	12.2	Art. 6 alin. (3) – Limitarea datelor solicitate la cele declarate inițial	**Nu se acceptă.** Dispoziția de la art. 6 alin. (3) instituie o regulă de protecție a datelor și de minimizare a

		Limitarea datelor ce pot fi solicitate exclusiv la cele declarate inițial poate genera dificultăți operaționale și riscuri de conformitate pentru furnizorii de servicii digitale și financiare. Propunere: Art. 6 alin. (3), în măsura în care limitează datele solicitate de beneficiar la cele declarate inițial, poate genera dificultăți în procesele de conformitate, prevenire a fraudei și gestionare a riscurilor. Datele necesare nu sunt întotdeauna statice și pot varia în funcție de profilul de risc, natura serviciului, tranzacției sau solicitările autorităților competente. Solicităm completarea articolului cu o derogare expresă pentru situațiile în care sunt necesare verificări suplimentare conform legislației aplicabile.	acestora, având ca scop asigurarea proporționalității și a predictibilității în procesul de utilizare a portofelelor pentru identitatea digitală, prin limitarea solicitării de date exclusiv la cele declarate în etapa de înregistrare. Norma trebuie interpretată sistemic, în corelație cu cadrul general aplicabil privind protecția datelor cu caracter personal, securitatea cibernetică și obligațiile legale ale beneficiarilor de servicii, care pot impune, în mod distinct și direct, solicitarea unor date suplimentare în temeiul altor acte normative. În acest context, reglementarea propusă nu exclude aplicarea obligațiilor legale imperative privind conformitatea, prevenirea fraudelor sau cerințele autorităților competente, acestea operând în temeiul legislației speciale, fără a necesita o derogare expresă în textul articolului. Prin urmare, completarea propusă nu se acceptă, întrucât ar afecta coerența normei și ar introduce o excepție redundantă față de cadrul normativ general aplicabil.
	12.3	Art. 5 – Portofelul AGE și menținerea fluxurilor alternative Proiectul nu clarifică suficient dacă utilizarea portofelului pentru identitatea digitală exclude sau nu alte fluxuri de identificare. Propunere: Solicităm clarificarea expresă că utilizarea portofelului pentru identitatea digitală este voluntară pentru utilizator și nu exclude menținerea unor fluxuri alternative de identificare și verificare a identității, inclusiv fluxuri eKYC existente, identificare asistată de operator sau identificare fizică, acolo unde acestea sunt necesare potrivit cadrului sectorial aplicabil.	**Nu se acceptă.** Art. 5 alin. (16) stabilește în mod expres caracterul voluntar al utilizării portofelelor pentru identitatea digitală, precum și principiul fundamental potrivit căruia neutilizarea acestora nu poate conduce la restricționarea sau dezavantajarea accesului la servicii publice sau private, la piața muncii ori la desfășurarea activităților economice. Totodată, același alineat prevede explicit menținerea posibilității de acces la servicii prin alte mijloace de identificare și autentificare existente, asigurând astfel existența unor

			canale alternative de identificare, inclusiv cele reglementate de cadrul sectorial aplicabil. Mai mult, art. 5 alin. (1) a fost revizuit și formulat într-o manieră generală și neutră instituțional, stabilind în mod clar că portofelele pentru identitatea digitală pot fi furnizate atât de un organism din sectorul public desemnat de Guvern, cât și de persoane juridice de drept privat, cu respectarea cerințelor prevăzute de lege. În aceste condiții, cadrul normativ asigură deja pluralitatea modalităților de furnizare a portofelelor și, coroborat cu alin. (16), garantează accesul utilizatorilor la servicii prin mijloace alternative de identificare și autentificare. În acest context, clarificarea suplimentară propusă este deja acoperită de textul proiectului și ar conduce la redundanță normativă, fără a adăuga valoare juridică suplimentară.
	12.4	Art. 63 – Documente electronice și semnături necalificate în fluxurile de plată În practică, numeroase servicii digitale utilizează mecanisme moderne de autentificare și autorizare care nu reprezintă semnături electronice calificate. Propunere: Solicităm clarificarea faptului că prevederile privind documentele electronice și semnăturile electronice nu afectează valabilitatea mecanismelor moderne de autentificare și autorizare deja utilizate în sectorul digital și financiar, inclusiv PIN, biometrie, token, autentificare multifactor, confirmare în aplicație sau alte mecanisme conforme standardelor de securitate aplicabile.	**Nu se acceptă.** Art. 63 reglementează efectele juridice ale documentelor electronice și ale semnăturilor electronice, inclusiv regimul aplicabil semnăturilor electronice care nu sunt calificate. Din cuprinsul acestuia rezultă expres că 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 în cazurile prevăzute de actele normative sau atunci când părțile au convenit în acest sens. Această soluție normativă este preluată și menținută în linie cu reglementarea existentă

			din Legea nr. 124/2022, asigurând continuitatea cadrului juridic și predictibilitatea raporturilor juridice. În acest context, rezultă în mod clar că legea permite utilizarea semnăturilor electronice necalificate în relațiile juridice, în condițiile stabilite de lege sau prin acordul părților, fără a afecta regimul juridic al altor mecanisme tehnice de autentificare și autorizare utilizate în fluxurile digitale. Prin urmare, clarificarea suplimentară propusă este redundantă, întrucât situația juridică este deja reglementată în textul proiectului.
	12.5	Art. 6 alin. (1) – Înregistrarea beneficiarilor în lista gestionată de organismul de supraveghere Obligația de înregistrare poate genera sarcini administrative suplimentare pentru entitățile deja reglementate sau integrate în infrastructuri digitale existente. Propunere: Solicităm introducerea unui regim diferențiat pentru entitățile deja autorizate sau supravegheate de autorități competente. În cazul acestor entități, înregistrarea ca beneficiar al portofelului ar trebui să poată fi realizată prin mecanisme simplificate și prin schimb de informații între autorități, fără duplicarea documentelor și fără crearea unor obligații administrative inutile.	**Nu se acceptă.** Obligația de înregistrare a beneficiarilor în lista gestionată de organismul de supraveghere derivă direct din cadrul european aplicabil și are ca scop instituirea unui mecanism unic de evidență al entităților care utilizează portofelele pentru identitatea digitală. La momentul actual, o astfel de listă nu există, iar proiectul de lege stabilește tocmai cadrul juridic necesar pentru crearea și operaționalizarea acesteia. Totodată, procesul de înregistrare este conceput ca unul simplificat, digital și proporțional, fără a genera sarcini administrative excesive, întrucât beneficiarul este obligat să furnizeze exclusiv un set minim de informații strict necesare, limitate la: datele de identificare, datele de contact și utilizarea preconizată a portofelului, conform art. 6 alin. (2). Mai mult, soluția legislativă urmărește facilitarea integrării beneficiarilor în ecosistemul portofelelor pentru identitatea digitală și inte-

			roperabilitatea cu soluțiile existente, fără a institui un regim diferențiat suplimentar pentru anumite categorii de entități, întrucât acest lucru ar afecta uniformitatea și aplicarea coerentă a cadrului de înregistrare.
	12.6	Art. 10 alin. (2) – Obligația furnizorilor privați de a accepta portofelele digitale Implementarea obligației de acceptare a portofelului poate implica modificări tehnice și operaționale semnificative pentru furnizorii privați. Propunere: Propunem ca obligația de acceptare a portofelului digital să intre în vigoare doar după publicarea specificațiilor tehnice complete, clarificarea cerințelor de interoperabilitate și securitate și acordarea unei perioade rezonabile de integrare tehnică și testare.	**Se acceptă parțial.** Art. 10 alin. (2) a fost revizuit în proces de avizare.
	12.7	Lipsa clarificării privind relația cu Regulamentul BNM 281 și procesul eKYC Proiectul nu clarifică suficient raportul dintre identificarea prin portofel și procesele existente de onboarding și verificare la distanță. Propunere: Solicităm clarificarea raportului dintre identificarea prin portofelul pentru identitatea digitală și cerințele aplicabile identificării și verificării identității la distanță în diferite sectoare reglementate. În special, este necesar să fie stabilit dacă datele transmise prin portofel pot substitui integral sau parțial fluxurile eKYC existente și în ce condiții acestea pot fi reutilizate în procesele de onboarding digital.	**Nu se acceptă.** Proiectul de lege stabilește cadrul general privind identificarea electronică și portofelele pentru identitatea digitală, fără a interveni asupra regimurilor sectoriale specifice de conformitate, inclusiv asupra cerințelor aplicabile proceselor de identificare și verificare a identității la distanță (eKYC), reglementate prin acte normative ale autorităților de supraveghere competente. În acest sens, utilizarea portofelelor pentru identitatea digitală constituie un mecanism de identificare electronică recunoscut în condițiile prezentei legi și ale cadrului european aplicabil, însă nu modifică în mod automat obligațiile de conformitate stabilite prin reglementările sectoriale, acestea rămânând aplicabile în continuare în funcție de domeniul de activitate și de riscurile specifice fiecărui sector.

			Totodată, proiectul nu instituie substituirea automată a proceselor eKYC existente, ci permite, în funcție de cadrul normativ sectorial aplicabil, utilizarea datelor și atributelor furnizate prin portofel în măsura în care acestea sunt acceptate de reglementările specifice fiecărui domeniu. În acest context, detalierea interoperabilității între portofelul pentru identitatea digitală și procesele sectoriale de onboarding și verificare a identității urmează a fi realizată, după caz, prin acte normative sectoriale și standarde tehnice aplicabile, în funcție de particularitățile fiecărui domeniu reglementat.
	12.8	Lipsa clarificării privind SCA / autentificarea strictă a utilizatorilor Nu este clar în ce măsură autentificarea prin portofel satisface cerințele de autentificare strictă aplicabile anumitor servicii digitale și financiare. Propunere: Solicităm clarificarea expresă a modului în care autentificarea utilizatorului prin portofelul pentru identitatea digitală se raportează la cerințele de autentificare strictă aplicabile serviciilor digitale și financiare. În lipsa acestei clarificări, există riscul implementării unor fluxuri redundante de autentificare, care pot afecta experiența utilizatorului și eficiența proceselor digitale.	**Nu se acceptă.** Proiectul de lege stabilește cadrul juridic pentru identificarea electronică și portofelele pentru identitatea digitală, fără a interveni asupra regimurilor sectoriale specifice privind autentificarea strictă a utilizatorilor (SCA), aplicabile în domenii precum cel financiar sau al serviciilor digitale reglementate de autoritățile competente. Autentificarea prin portofelul pentru identitatea digitală constituie un mecanism de identificare electronică în sensul prezentei legi, a cărui utilizare și acceptare în diferite fluxuri operaționale depinde de cerințele specifice stabilite de cadrul normativ sectorial aplicabil fiecărui domeniu. În acest sens, proiectul nu derogă și nu substituie cerințele privind autentificarea strictă, acestea rămânând aplicabile în continuare în funcție de nivelul de risc și de reglementările sectoriale incidente. Totodată, interoperabilitatea și potențiala utilizare a portofelului ca

			factor de autentificare în cadrul schemelor SCA țin de implementarea tehnică și de standardele aplicabile la nivel sectorial, care vor fi transpuse și detaliate prin acte normative și specificații tehnice ulterioare. Prin urmare, reglementarea propusă este intenționat neutră din punct de vedere tehnologic și funcțional, iar clarificarea suplimentară nu este necesară la nivel de lege.
	12.9	Lipsa clarificării privind date incomplete, expirate sau revocate Proiectul nu reglementează suficient situațiile în care datele sau atestatele prezentate prin portofel sunt incomplete, expirate sau insuficiente. Propunere: Solicităm reglementarea expresă a situațiilor în care datele sau atestatele prezentate prin portofel sunt incomplete, expirate, revocate sau insuficiente pentru furnizarea serviciului solicitat. Beneficiarii trebuie să poată solicita date suplimentare, aplica fluxuri alternative de identificare sau refuza furnizarea serviciului atunci când nu pot îndeplini obligațiile legale aplicabile.	**Nu se acceptă.** Proiectul de lege reglementează cadrul general de utilizare a portofelelor pentru identitatea digitală și al atestatelor electronice ale atributelor, acestea fiind emise și gestionate prin mecanisme care includ în mod intrinsec verificarea valabilității, integrității și statutului acestora (inclusiv expirare, revocare sau invalidare). În plus, verificarea în timp real a autenticității și valabilității datelor și atestatelor reprezintă o funcționalitate esențială a infrastructurii de încredere, fiind asigurată prin mecanismele tehnice și instituționale prevăzute de lege și de standardele europene aplicabile. Totodată, proiectul nu restricționează dreptul beneficiarilor de a aplica cerințele legale sectoriale aplicabile sau de a utiliza, după caz, fluxuri alternative de identificare în situațiile în care acestea sunt prevăzute de legislația specială. Aceste aspecte țin de reglementarea sectorială și de condițiile specifice de furnizare a serviciilor, nefiind necesară detalierea lor la nivelul legii generale privind identificarea electronică.

			Prin urmare, cadrul normativ propus este suficient și proporțional, iar introducerea unor prevederi suplimentare privind fiecare scenariu operațional posibil ar depăși nivelul de reglementare al prezentei legi și ar afecta coerența tehnico-juridică a acesteia.
	12.10	Lipsa clarificării privind indisponibilitatea portofelului sau a serviciilor de validare Nu sunt prevăzute reguli clare pentru situațiile în care portofelul digital, API-urile sau serviciile de validare sunt indisponibile. Propunere: Solicităm includerea unor reguli privind indisponibilitatea portofelului pentru identitatea digitală, a API-urilor sau a mecanismelor de validare. În asemenea cazuri, beneficiarii trebuie să poată utiliza metode alternative de identificare, verificare și autentificare, fără a fi considerați neconformi.	**Nu se acceptă.** Proiectul de lege instituie cadrul general privind funcționarea portofelelor pentru identitatea digitală și a mecanismelor de validare aferente, iar cerințele de disponibilitate, continuitate a serviciului și reziliență sunt acoperite prin obligațiile generale aplicabile furnizorilor și prin standardele de securitate și interoperabilitate. Totodată, utilizarea portofelelor are caracter voluntar, iar accesul la servicii publice și private nu este condiționat exclusiv de utilizarea acestora, fiind garantată posibilitatea utilizării unor mijloace alternative de identificare și autentificare, conform cadrului normativ aplicabil. În plus, o parte semnificativă a aspectelor operaționale privind gestionarea situațiilor de indisponibilitate, continuitatea serviciului și condițiile tehnice de utilizare vor fi detaliate în cadrul normativ subsecvent, inclusiv prin standarde tehnice, specificații de implementare și acte ale Guvernului. De asemenea, condițiile concrete de utilizare a serviciilor, inclusiv procedurile de acces alternativ și limitările operaționale aplicabile, vor fi stabilite de fiecare furnizor de portofel prin termenii și condițiile proprii, în conformitate cu legea și cadrul de reglementare aplicabil.

	12.11	Art. 68 „Sancțiuni” Considerăm necesară revizuirea prevederilor art. 68 privind sancțiunile, întrucât mecanismul sancționator propus nu prevede criterii suficiente pentru individualizarea sancțiunilor și poate conduce la aplicarea disproporționată a amenzilor. Contrar art. 16 (1) din Regulamentul UE nr. 91/2014 (eIDAS 2.0), care prevede obligația statelor de a stabili în legislația națională reguli aplicabile sancțiunilor, asigurând că acestea sunt eficace, proporționale și disuasive, proiectul de lege a stabilit doar amenzi la nivelul maxim, care sunt aplicabile pentru orice tip de încălcare a legii, fără a stabili nici un criteriu de individualizare a sancțiunilor. Propunem introducerea unor cerințe clare de individualizare și determinare a nivelului amenzii, de ex. natura, gravitatea încălcărilor, numărul utilizatori afectați, intenția etc., inclusiv posibilitatea introducerii unui avertisment în caz de încălcare minoră. Totodată, nivelul maxim al amenzii trebuie revizuit conform realităților economice din Republica Moldova și stabilit ca un plafon maxim (care permite aplicarea unei amenzi sub acest pafon) cu indicarea exactă a prevederile din lege ale căror încălcare va atrage sancționarea.	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.
	12.12	Art. 69 – Termene de implementare necorelate Obligațiile aplicabile beneficiarilor pot deveni efective înainte ca infrastructura tehnică să fie complet disponibilă și testată. Propunere: Solicităm corelarea termenelor de intrare în vigoare a obligațiilor pentru beneficiarii privați cu disponibilitatea efectivă a infrastructurii, publicarea documentației tehnice complete, lansarea sandbox-ului și finalizarea testelor-pilot. Considerăm necesară acordarea unei perioade rezonabile de integrare tehnică și tranziție.	**Nu se acceptă.** Proiectul de lege nu instituie obligații de utilizare pentru beneficiarii privați, utilizarea portofelelor pentru identitatea digitală având caracter voluntar, iar accesul la servicii publice și private rămâne garantat prin mijloace alternative de identificare și autentificare. În acest sens, nu se poate reține premisa potrivit căreia ar exista obligații ale beneficiarilor privați care ar deveni aplicabile anterior disponibilității infrastructurii sau fără o perioadă de tranziție adecvată, întrucât legea nu condiționează activitatea acestora de utilizarea portofelului.

			Totodată, prin dispozițiile tranzitorii și finale ale proiectului este stabilită în mod expres obligația Guvernului de a asigura elaborarea, adoptarea și punerea în aplicare a întregului cadru normativ secundar necesar înainte de intrarea în vigoare a legii, inclusiv a actelor tehnice și operaționale de implementare. Prin urmare, corelarea suplimentară a termenelor în sensul propus nu este necesară, întrucât arhitectura normativă deja asigură atât caracterul voluntar al utilizării, cât și pregătirea infrastructurii și a cadrului de implementare până la momentul aplicării legii.
	12.13	Art. 4 – Pseudonimele în tranzacțiile electronice Utilizarea pseudonimelor poate genera interpretări neuniforme în raport cu obligațiile de identificare aplicabile anumitor servicii. Propunere: Solicităm clarificarea expresă că utilizarea pseudonimelor în tranzacțiile electronice nu afectează obligațiile legale privind identificarea reală a utilizatorilor, verificarea identității și păstrarea datelor de identificare, acolo unde acestea sunt prevăzute de legislația aplicabilă.	**Nu se acceptă.** Art. 4 reglementează utilizarea pseudonimelor exclusiv în contextul interacțiunilor și tranzacțiilor electronice în cadrul ecosistemului digital, fără a afecta obligațiile de identificare prevăzute de legislația aplicabilă în funcție de natura serviciului sau a raportului juridic. Utilizarea pseudonimelor nu derogă de la cerințele legale privind identificarea reală a utilizatorilor, verificarea identității sau păstrarea datelor de identificare, acolo unde acestea sunt impuse de cadrul normativ sectorial (de exemplu, în domeniul financiar, al prevenirii spălării banilor sau al serviciilor reglementate). În consecință, regimul juridic aplicabil identificării rămâne neschimbat, iar pseudonimizarea reprezintă doar un mecanism tehnic de protecție a datelor și de minimizare a expunerii identității în interacțiunile digitale, fără a substitui obligațiile de conformare existente.

	12.14	Lipsa clarificării privind răspunderea pentru date greșite sau compromise Solicităm clarificarea regimului de răspundere în cazul în care datele sau atributele prezentate prin portofel sunt incorecte, expirate, compromise sau validate eronat. Beneficiarii care utilizează mecanismele oficiale de validare și acționează cu bună-credință trebuie să beneficieze de o limitare rezonabilă a răspunderii pentru erori provenite din surse autentice sau infrastructuri oficiale. ATIC susține dezvoltarea unui ecosistem modern și interoperabil de identitate digitală și servicii de încredere, aliniat standardelor europene și capabil să accelereze digitalizarea serviciilor publice și private din Republica Moldova. În același timp, considerăm esențial ca implementarea cadrului legal și tehnic să fie realizată gradual, în strânsă cooperare cu sectorul privat și autoritățile competente, astfel încât să fie asigurate: •interoperabilitatea și securitatea soluțiilor implementate; •claritatea obligațiilor aplicabile beneficiarilor; •continuitatea serviciilor digitale existente; •protecția adecvată a utilizatorilor și a datelor acestora; •evitarea barierelor tehnice și administrative disproporționate. ATIC își exprimă disponibilitatea de a participa în continuare la consultările și grupurile de lucru dedicate definitivării cadrului normativ și operațional aferent implementării identității digitale și serviciilor de încredere.	**Se acceptă.** Proiectul a fost completat cu Capitolul VI „Răspunderea juridică, procedura de constatare şi sancțiunile” din care rezultă limitele de răspundere pentru fiecare subiect.
Ministerul Justiției (Nr. nr. 04/2-5098 din 11.05.2026**)**	13.1	La art. 3: cu referire la denumirea articolului, cuvântul „Definiții” se va substitui cu cuvântul „Noțiuni”, în vederea ajustării la terminologia utilizată în legislația națională. Totodată alineatul introductiv se va indica după cum urmează: „În sensul prezentei legi, următoarele noțiuni semnifică:”. Adițional, noțiunile propuse se vor expune în ordinea alfabetică, conform rigorilor tehnicii legislative. Se va reține că definirea noțiunilor se justifică doar în cazul în care la momentul adoptării actului normativ se știe cu certitudine că, un termen nu este definit în alte acte normative și este pasibil de mai multe interpretări.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	13.2	La pct. 17, noțiunea „date cu caracter personal”, se va expune după cum urmează „date cu caracter personal - astfel cum este definit la art. 4 din Legea nr. 195/2024 privind protecția datelor cu caracter personal”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.3	La art. 5: La alin. (4) expresia „justificate în mod corespunzător” nu este suficient de clară, motiv pentru care propunem să fie revăzută pentru a evita dificultăți la aplicare. La alin. (19) expresia „fără întârzieri nejustificate” nu determină un termen limită pentru publicarea informațiilor, fapt pentru care se va revizui (valabil și pentru restul cazurilor similare). alin. (23), referința la „art. 16” necesită a fi reexaminată, întrucât nu corespunde cu toate trimiterile care sunt făcute la art. 5a, alin (22) din Regulamentul (UE) nr. 910/2014 (obiecție valabilă și pentru trimiterea de la art. 7 alin. (1) din proiect).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.4	La art. 6 alin. (3) textul „lit. (c)” se va substitui cu textul „lit. c)”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.5	La art. 7: La alin (2), cuvintele „perioadă de maximum cinci ani” se vor substitui cu cuvintele „perioadă de până la cinci ani”. La alin. (3) propunem ca cuvintele „poate să fie certificată” să fie substituite cu cuvintele „se certifică”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.6	La art. 9: La alin. (1), textul „alin. (8)” se va substitui cu textul „alin. (9)”, în vederea asigurării corectitudinii trimiterii. Dispoziția alin. (4) este formulată incomplet și neclar, nefiind exprimată explicit acțiunea pe care urmează să o întreprindă organismul de supraveghere. Prin urmare, se va reformula alineatul prin indicarea acțiunii concrete.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.7	La art. 10, în vederea corectitudinii gramaticale, sintagma „Uniunea Europeană” se va substitui cu sintagma „Uniunii Europene” (obiecție valabilă și pentru alin. (2) din acest articol).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.8	La art. 11 alin. (1) diviziunile se vor numerota cu utilizarea unei singure paranteze rotunde - a), b), c). La fel, în tot textul proiectului se va revedea însemnarea unor astfel de diviziuni.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	13.9	La art. 15 alin. (2), cuvintele „va stabili” se vor substitui cu cuvântul „stabilește”, în scopul expunerii verbelor la timpul prezent, în conformitate cu art. 54 alin. (1) lit. j) al Legii nr. 100/2017.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.10	La art. 16 alin. (2) cuvintele „este anulată” se vor substitui cu cuvintele „se anulează”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.11	La art. 17 alin. (1), în vederea asigurării clarității normei, referința la „cadrul normativ aplicabil” se va completa cu referința nemijlocită a actului normativ relevant.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.12	La art. 20 pct. 2) textul „alin. 1)” se va substitui cu textul „pct. 1)”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.13	La art. 21 alin. (6), se constată că norma face trimitere la „cerințele prevăzute la art. 11 din Legea nr. 48/2023 privind securitatea cibernetică”, în timp ce articolul respectiv reglementează măsuri de securitate, în acest sens, se va corela cu terminologia utilizată din Legea nr. 48/2023 privind securitatea cibernetică.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.14	La art. 24 alin. (3) lit. b), textul „alin. (3)” se va substitui cu textul „alin. (2)”, pentru corectitudinea trimiterii.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.15	La art. 35 alin. (1) lit. a) menționăm că, într-o enumerare de referințe, denumirea elementului structural nu se repetă.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.16	La art. 49 alin. (2) este inutilă precizarea „lit. (a)-(f)”, deoarece alin. (1) nu conține alte diviziuni.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	14.17	La art. 55 alin. (2) lit. k) cu este clar ce presupune expresia „datele privind societățile”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.18	Art. 68 este în dezacord cu art. 20 din Constituție. Menționăm că, în jurisprudența sa, Curtea Constituțională a subliniat că, potrivit principiului constituțional al legalității, legiuitorul nu poate reglementa o sancţiune în aşa fel, încât să lipsească instanţa de judecată de posibilitatea de a individualiza sancțiunea, ținând cont	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.

		de circumstanţele cazului. În astfel de situaţie, competenţele instanţei ar fi limitate, creându-se precondiţii pentru încălcarea drepturilor constituţionale ale subiecţilor, inter alia, a dreptului constituţional la un proces echitabil. În lipsa mecanismelor de individualizare a sancţiunii instanţa de judecată este lipsită de posibilitatea de a efectua un control judiciar efectiv şi, în final, justiţiabilii nu pot beneficia de dreptul la un proces echitabil (Hotărârea Curții Constituționale nr. 10/2016 (individualizarea sancţiunii), § 77 și 78). Astfel, se va ține cont că o sancţiune nu poate fi exact determinată, fiind necesar de stabilit limita minimă și maximă a acesteia.	
	13.19	La art. 69: La alin. (1) cuvintele „care se pun în aplicare din momentul aderării” se vor substitui cu cuvintele „care intră în vigoare la data aderării”. La alin. (3) se va indica sursa publicării Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	13.20	Cu titlu general: Se constată utilizarea frecventă în textul proiectului a unor formulări vagi sau cu caracter eventual, precum „atunci când este posibil”, „dacă este cazul”, „în mod corespunzător”, „par să fi fost încălcate”, care nu corespund exigențelor de claritate, precizie și previzibilitate ale normei juridice stabilite de Legea nr. 100/2017. Astfel de formulări sunt de natură să afecteze caracterul imperativ al normelor și pot genera incertitudini în procesul de aplicare. În acest sens, se recomandă revizuirea textului proiectului prin substituirea acestor expresii cu termeni normativi clari, care să exprime fără echivoc drepturi și obligații. De asemenea, se constată utilizarea unor trimiteri generale la „cadrul normativ aplicabil”, fără indicarea expresă a actelor relevante, precum și existența unor necorelări terminologice și trimiteri inexacte între dispozițiile proiectului și alte acte normative incidente. Astfel de carențe contravin principiului securității juridice și cerințelor de calitate a actului normativ.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

Ministerul Energiei (Nr. 02-1229 din 13.05.2026)	14.1	Proiectul de lege conține un număr semnificativ de formulări cu caracter general și vag, precum „după caz”, „în mod corespunzător”, „dacă este cazul”, „justificat”, „în mod adecvat” sau alte expresii similare. Utilizarea frecventă a acestor noțiuni deschise afectează claritatea și previzibilitatea normei juridice. Astfel, art. 17 alin. (4) din proiect, considerăm necesar de a-l completa prin introducerea unui mecanism de informare standardizată a utilizatorilor serviciilor de încredere. În forma actuală, noțiunea de „informare corespunzătoare” este una generală și poate determina interpretări neuniforme în practică, în special în contextul stabilirii răspunderii prestatorilor. Lipsa unor criterii minime sau a unui model de referință poate conduce la situații în care informarea este realizată formal, fără a asigura în mod efectiv înțelegerea restricțiilor privind utilizarea serviciului de către utilizatori sau terți. Prin urmare, se propune instituirea posibilității ca Guvernul sau autoritatea de supraveghere să elaboreze și să aprobe modele standardizate de informare privind restricțiile de utilizare a serviciilor de încredere.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	14.2	Proiectul de lege conține unele prevederi referitoare la termene procedurale, în special în materia verificărilor, evaluărilor sau măsurilor dispuse de autoritatea de supraveghere, care nu sunt suficient de clar delimitate în timp. În anumite cazuri, sunt stabilite termene inițiale (de exemplu, termene de 3 luni), însă acestea pot fi ulterior prelungite fără a fi prevăzută o limită maximă sau criterii clare pentru durata prelungirii (de exemplu art. 22 alin. (4), art. 24 alin. (5)).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	14.3	Redacția actuală a art. 26 alin. (1) este formulată într-un mod general, ceea ce poate conduce la interpretări excesiv de largi în practică. În special, textul nu distinge suficient între admisibilitatea ca probă și forța probantă a diferitelor tipuri de semnături electronice. În lipsa unei astfel de clarificări, există riscul ca semnăturile electronice simple sau avansate care prezintă un nivel mai redus de securitate și pot fi mai ușor contestate sau chiar contrafăcute să fie tratate în mod similar cu semnătura electronică calificată, ceea ce poate afecta securitatea raporturilor juridice și poate genera incertitudine în activitatea instanțelor de judecată.	**Nu se acceptă.** Prevederile art. 26 din proiectul de lege reprezintă transpunerea fidelă a art. 25 din Regulamentul (UE) nr. 910/2014, care stabilește principiile privind efectele juridice și admisibilitatea ca probă a semnăturilor electronice. Norma consacră, în conformitate cu Regulamentul eIDAS, principiul nediscriminării semnăturilor electronice, potrivit căruia unei semnături electronice nu i se poate refuza

		Deși alin. (2) consacră echivalența juridică a semnăturii electronice calificate cu semnătura olografă, proiectul nu prevede expres că aceasta beneficiază de un regim probator privilegiat, spre deosebire de celelalte tipuri de semnături electronice. Astfel, propunem de a expune alin. (1), în următoarea redacție: „(1) Semnăturile electronice, altele decât semnătura electronică calificată, pot fi admise ca mijloc de probă, însă forța lor probantă se apreciază de către instanța de judecată în funcție de circumstanțele cauzei, inclusiv de nivelul de securitate, de modalitatea de identificare a semnatarului și de garanțiile tehnice asociate.”	efectul juridic sau admisibilitatea ca probă exclusiv pentru motivul că este în format electronic sau că nu este calificată. Totodată, alin. (2) stabilește expres regimul juridic distinct al semnăturii electronice calificate, prin recunoașterea efectului juridic echivalent semnăturii olografe. Aspectele privind aprecierea forței probante a mijloacelor de probă, inclusiv a diferitelor tipuri de semnături electronice, țin de competența instanței de judecată și sunt reglementate de legislația procesuală aplicabilă, nefiind necesară reiterarea acestora în prezenta lege.
	14.4	Propunem revizuirea prevederilor art. 37, art. 46, art. 48, art. 52, art. 59 și art. 61 prin prisma propunerilor la art. 26 din proiect.	**Nu se acceptă.** A se vedea argumentele autorului proiectului expuse la propunerea precedentă.
	14.5	Referitor la art. 67, se constată că textul nu stabilește în mod expres natura raportului juridic dintre subiecții răspunderii prevăzuți de această normă, și anume organismul de supraveghere, emitentul mijloacelor de identificare electronică și partea care execută procedura de autentificare. În lipsa unei precizări, nu este clar dacă răspunderea acestora este solidară, subsidiară sau individuală, ceea ce poate genera dificultăți în aplicarea practică a dispozițiilor privind repararea prejudiciului. De asemenea, formularea referitoare la „orice persoană fizică sau juridică” și la „tranzacții transfrontaliere” nu este însoțită de elemente de delimitare suficiente privind condițiile angajării răspunderii, în special sub aspectul stabilirii legăturii de cauzalitate dintre faptă și prejudiciu. Se propune, în acest sens, completarea articolului cu dispoziții care să clarifice natura răspunderii juridice a subiecților implicați, precum și introducerea unor precizări referitoare la condițiile generale de angajare a răspunderii și la raportul dintre eventualii coautori ai prejudiciului.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	14.6	În ceea ce privește art. 68, se constată că acesta stabilește limitele maxime ale sancțiunilor aplicabile prestatorilor de servicii de încredere, însă nu conține criterii de individualizare a sancțiunilor în funcție de circumstanțele concrete ale încălcării. Lipsa unor asemenea criterii, precum gravitatea faptei, durata încălcării, caracterul intenționat sau neglijent al conduitei, gradul de cooperare al subiectului sancționat sau impactul asupra utilizatorilor și asupra securității serviciilor, poate conduce la dificultăți în aplicarea unitară a dispozițiilor privind sancționarea. Se propune completarea articolului cu prevederi care să stabilească în mod expres criteriile de individualizare a sancțiunilor, în vederea asigurării unei aplicări proporționale și previzibile a acestora.	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.
Cancelaria de Stat (Nr. CS-1812-10-108-1186)	15.1	În vederea asigurării calității și aplicabilității viitoarei legi, considerăm necesară reținerea câtorva observații. Se impune corelarea textului cu cadrul normativ național conex, în special cu Legea nr. 142/2018 privind schimbul de date și interoperabilitatea, Legea nr. 467/2003 privind informatizarea și resursele informaționale de stat, Legea nr. 195/2024 privind protecția datelor cu caracter personal și Legea nr. 48/2023 privind securitatea cibernetică, întrucât intersecțiile cu materia reglementată sunt substanțiale.	**Se acceptă.** Proiectul de lege a fost corelat cu cadrul normativ conex.
	15.2	Atribuirea, prin art. 64 al proiectului, a calității de organism de supraveghere Serviciului de Informații și Securitate necesită fundamentare suplimentară din perspectiva compatibilității cu mandatul SIS prevăzut de Legea nr. 753/1999, autorul urmând să obțină avizul instituției asupra normelor relevante. Totodată, deși la pct. 4.2 al notei de fundamentare se afirmă că proiectul nu implică direct cheltuieli suplimentare, sunt enumerate costuri privind dezvoltarea portofelului de identitate digitală și integrarea sistemelor informaționale; pentru respectarea art. 30 alin. (4) din Legea nr. 100/2017, se impune completarea notei cu estimări cantitative și surse de finanțare, urmând ca proiectul să fie remis spre avizare Ministerului Finanțelor.	**Se acceptă.** Proiectul în proces de expertizare și avizare repetată urmează a fi remis către SIS pentru avizare. De asemenea, pct. 4.2 al notei de fundamentare a fost revizuit reieșind din propunerile recepționate în proces de avizare. Proiectul a fost avizat și de Ministerul Finanțelor.
	15.3	Sub aspect tehnico-redacțional, semnalăm necesitatea completării tabelului de concordanță cu indicarea, pentru fiecare articol, a gradului de compatibilitate și a justificării abaterilor, precum și	**Se acceptă.** Tabelul de concordanță a fost revizuit conform propunerilor.

		operarea corecturilor în nota de fundamentare (la pct. 2.2 – „oferireacetățenilor" → „oferirea cetățenilor"; la pct. 3.1 – „organim" → „organism"; la pct. 5.2 – reformularea gramaticală a frazei privind transpunerea); trimiterile la actele Uniunii Europene se vor unifica, cu indicarea numărului CELEX. Cancelaria de Stat avizează pozitiv, cu observații expuse mai sus, proiectul de lege privind identificarea electronică și serviciile de încredere, urmând ca autorul să integreze observațiile formulate supra.	
AmCham Moldova (Nr. 57 din 14.05.2026)	16.1	La art. 3, punctul 3 definiția propusă pentru noțiunea de „arhivare electronică" corespunde, în linii generale, abordării europene prevăzute de cadrul eIDAS, întrucât include elementele esențiale precum stocarea, integritatea și asigurarea autenticității pe termen lung a documentelor electronice. Cu toate acestea, aplicabilitatea practică a acestei reglementări ar putea beneficia de o analiză suplimentară în corelație cu stadiul actual de dezvoltare a Sistemului informațional „e-Arhiva". Din informațiile disponibile, sistemul se află încă în proces de implementare, iar cadrul normativ secundar aferent este în curs de elaborare. În acest context, ar fi utilă clarificarea unor aspecte precum calendarul de operaționalizare completă, instituțiile responsabile de supraveghere și certificare, precum și standardele tehnice și cerințele de interoperabilitate aplicabile.	**Nu se acceptă.** Definiția noțiunii de „arhivare electronică" de la art. 3 punctul 3 are un caracter conceptual și stabilește cadrul general al regimului juridic aplicabil, fiind aliniată principiilor europene relevante, inclusiv celor din cadrul eIDAS. Aspectele privind implementarea practică, calendarul de operaționalizare a Sistemului informațional „e-Arhiva", instituțiile responsabile, precum și standardele tehnice și cerințele de interoperabilitate țin de etapa de executare și reglementare subsecventă a legii, prin acte normative ale Guvernului și ale autorităților competente. În acest context, includerea unor detalii operaționale în textul legii ar depăși nivelul normativ al definiției și ar afecta caracterul său general și stabil.
	16.2	La articolul 3, punctul 28 definiția documentului electronic este formulată în mod larg și tehnologic neutru, fiind compatibilă cu abordarea eIDAS. Totuși, pentru a asigura coerența cadrului normativ, ar putea fi utilă raportarea acesteia la prevederile Codului civil, care reglementează forma actelor juridice și condițiile de validitate ale acestora. În forma actuală, nu rezultă cu suficientă claritate diferențele de efect juridic dintre documentele electronice nesemnate, cele semnate cu semnătură electronică avansată	**Nu se acceptă.** Definiția noțiunii de „document electronic" de la art. 3 pct. 28 are un caracter general și tehnologic neutru, fiind menită să stabilească sfera de aplicare a regimului juridic al documentelor electronice, în conformitate cu abordarea consacrată la nivel european.

		și cele semnate cu semnătură calificată. De asemenea, ar putea fi clarificată relația dintre documentul electronic și cerința de „formă scrisă” prevăzută de legislația civilă.	Aspectele privind efectele juridice ale documentelor electronice, condițiile de echivalență cu înscrisurile pe suport de hârtie, precum și diferențele dintre tipurile de semnături electronice sunt reglementate în mod expres și exhaustiv la art. 63 din proiectul de lege, care stabilește regimul juridic detaliat al acestora. În acest context, raportarea definiției la prevederile Codului civil sau detalierea efectelor juridice în cuprinsul definiției nu este necesară, întrucât ar conduce la suprapuneri normative și ar afecta coerența structurii actului, care delimitează distinct definițiile generale de regimul juridic aplicabil.
	16.3	La articolul 3, punctul 38 definiția portofelului pentru identitatea digitală este, în esență, aliniată conceptelor introduse la nivel european prin eIDAS 2.0. Totodată, ținând cont de rolul acestui instrument ca element central al ecosistemului de identitate digitală, s-ar putea avea în vedere consolidarea reglementării sub aspectul securității și al gestionării riscurilor. În special, norma ar putea beneficia de clarificări privind noțiunea de „vulnerabilitate”, tipurile de evaluări necesare și standardele tehnice aplicabile (de exemplu, standarde ISO sau ETSI). De asemenea, ar putea fi utilă precizarea existenței unor mecanisme de audit, inclusiv independent, pentru verificarea conformității. În acest context, se recomandă examinarea oportunității includerii unei enumerări indicative a categoriilor de vulnerabilități ce urmează a fi evaluate, care ar putea cuprinde aspecte de securitate cibernetică, protecția datelor cu caracter personal, funcționalitatea sistemului și conformitatea cu cadrul normativ aplicabil.	**Nu se acceptă.** Definiția portofelului pentru identitatea digitală de la art. 3 pct. 38 este deliberat formulată într-o manieră tehnologic neutră și aliniată cadrului eIDAS 2.0, pentru a evita instituirea unei cadru legal rigid și pentru a permite adaptarea continuă la evoluțiile standardelor tehnice internaționale și europene. Elementele invocate în obiecție, precum tipurile de vulnerabilități, standardele ISO/ETSI aplicabile, metodologiile de evaluare a securității, auditul (inclusiv independent) și cerințele de conformitate, nu țin de nivelul actului normativ primar, ci fac parte din cadrul tehnic și operațional de implementare. În ceea ce privește certificarea portofelelor, proiectul de lege stabilește în mod expres necesitatea certificării acestora ca mecanism de asigurare a conformității și securității, urmând ca procedurile detaliate de certificare, standardele aplicabile, metodologiile de evaluare și cerințele

			tehnice să fie reglementate prin acte normative subsecvente aprobate de Guvern. Totodată, instituirea unei enumerări exhaustive sau indicative a vulnerabilităților la nivel de lege ar fi neadecvată, întrucât domeniul securității cibernetice este unul dinamic, iar o astfel de abordare ar limita capacitatea de adaptare la noi riscuri și amenințări emergente. În consecință, cadrul propus menține un nivel de reglementare adecvat unei legi-cadru, urmând ca detaliile tehnice privind securitatea, auditul și evaluarea riscurilor să fie stabilite prin reglementări secundare și standarde tehnice aplicabile.
	16.4	La articolul 7 alin. (2) prevederea referitor la efectuarea periodică a evaluării vulnerabilităților constituie un element important pentru asigurarea securității portofelelor pentru identitatea digitală. Cu toate acestea, formularea actuală este una generală și ar putea beneficia de o detaliere suplimentară privind domeniul și conținutul evaluării. În particular, ar putea fi clarificat dacă evaluarea vizează exclusiv componentele tehnice sau include și aspecte organizaționale și juridice, precum și dacă există o metodologie standardizată sau cerințe minime aplicabile. În vederea asigurării unei aplicări uniforme, se consideră oportună analizarea posibilității de a preciza domeniile principale ale evaluării, cum ar fi securitatea IT, protecția datelor, integritatea operațională și conformitatea legală.	**Nu se acceptă.** Art. 7 alin. (2) stabilește deja în mod clar cadrul juridic al certificării portofelelor pentru identitatea digitală, inclusiv durata de valabilitate a certificării, obligația de efectuare periodică a evaluării vulnerabilităților și consecința juridică a neconformităților identificate (anularea certificării). Acest mecanism este formulat în concordanță cu abordarea eIDAS 2.0 și cu principiile generale de securitate și management al riscurilor aplicabile serviciilor de încredere. În ceea ce privește detalierea conținutului evaluării vulnerabilităților, a metodologiilor aplicabile și a standardelor tehnice de referință, acestea nu constituie elemente de reglementare la nivel de lege-cadru, ci țin de cadrul tehnic și normativ subsecvent, care urmează a

			fi stabilit de Guvern prin acte de implementare, inclusiv în corelare cu standardele europene și internaționale aplicabile. Totodată, necesitatea certificării portofelelor este prevăzută expres la nivelul legii, iar modul concret de certificare, inclusiv cerințele tehnice detaliate, procedurile de audit și standardele de conformitate, vor fi dezvoltate ulterior prin reglementări secundare, asigurând astfel flexibilitatea necesară adaptării la evoluțiile tehnologice și de securitate.
	16.5	La articolul 50 alin. (5) prevederea referitoare la includerea „adresei persoanei fizice sau juridice" în certificatul calificat pentru autentificarea unui site internet ar putea genera unele dificultăți de interpretare și aplicare. În special, ar putea fi utilă clarificarea noțiunii de adresă (domiciliu, reședință sau sediu). Totodată, ar putea fi avută în vedere alinierea la standardele tehnice internaționale aplicabile certificatelor pentru autentificarea siteurilor, unde accentul este pus, în principal, pe identificarea domeniului și a titularului. În acest context, s-ar putea analiza oportunitatea unei formulări flexibile, care să prevadă includerea datelor de adresă în măsura în care acestea sunt disponibile și relevante pentru identificare, evitând astfel eventuale dificultăți practice sau prelucrarea excesivă de date.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	16.6	La articolul 63 alin. (3) considerăm că textul „printr-un înscris distinct semnat olograf sau cu semnătură electronică calificată" restricționează interacțiunea exclusiv digitală dintre unii prestatori de servicii și clienți, și urmează a fi exclus. În prezent, mai mulți prestatori de servicii sunt focusați pe dezvoltarea experienței digitale a clienților pe toată durata relației de afaceri, inclusiv inițierea acesteia (prin digital onboarding) și acordarea produselor și serviciilor prin aplicații mobile și alte instrumente electronice. Soluțiile informatice utilizate de prestatorii de servicii nu sunt bazate neapărat pe semnături electronice calificate (e.g., servicii bancare/acordarea produselor), iar deservirea exclusiv digitală a clienților exclude per se semnături olografe. Suplimentar,	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.

		norma în redacție propusă intră în conflict cu art. 318 din Codul civil - (3) Actul juridic scris se încheie în formă electronică dacă este semnat cu semnătura electronică avansată calificată a persoanei care încheie actul, dacă acordul părților sau legea nu prevede cerința de utilizare a unui alt tip de semnătură electronică. Astfel, Codul civil nu stabilește că acordul părților se semnează cu semnături electronice calificate sau olografe, fapt care-l considerăm corect.	
	16.7	La articolul 68 alin. (2) „Sancțiuni" este disproporționat, abuziv și nu a realizat o transpunere corectă a acquis-ului comunitar, fiind contrar cerințelor Regulamentului UE nr. 91/2014, modificat și completat prin Regulamentul (UE) 2024/1183 (eIDAS 2.0), deoarece, contrar art. 16 (1) din Regulamentul UE, care prevede obligația statelor de a stabili în legislația națională reguli/criterii aplicabile sancțiunilor (asigurând că acestea sunt eficace, proporționale și disuasive), proiectul de lege a stabilit doar amenzi la nivelul maxim, care sunt aplicabile pentru orice tip de încălcare a legii, fără a stabili nici un criteriu de individualizare a sancțiunilor. În alte domenii relevante, precum protecția datelor cu caracter personal sau prevenirea spălării banilor, sunt utilizate modele diferențiate, bazate pe natura și gravitatea încălcării. În acest sens, se recomandă examinarea oportunității introducerii unor criterii de individualizare (de exemplu, gravitatea faptei, durata, impactul asupra utilizatorilor), precum și a unor mecanisme complementare (avertismente), care ar putea contribui la o aplicare proporțională a sancțiunilor. Totodată, nivelul maxim al amenzii trebuie revizuit la realitățile economice din Republica Moldova și stabilit ca o sumă variabilă, care nu poate depăși un plafon maxim, cu indicarea exactă a prevederile din lege ale căror încălcare va atrage sancționarea.	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.
Agenția de Guvernare Electronică (Nr. 3007 – 125 din 18.05.2026)	17.1	Art. 1 urmează a fi redactat în corespundere cu art. 51 alin. (5) și (6) din Legea nr. 100/2017 cu privire la actele normative, și anume „Articolul poate fi divizat în alineate, constituite, de regulă, dintr-o singură propoziţie sau frază, prin care se reglementează o dispoziţie specifică ansamblului normelor articolului. Dacă dispoziţia alineatului nu poate fi exprimată într-o singură	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		propoziţie sau frază, pot fi utilizate mai multe propoziţii sau fraze.”. Totodată, recomandăm revizuirea termenului de „site internet”, în contextul reglementărilor prevăzute în Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, care utilizează la moment termenul de „pagină web” sau a Legii comunicațiilor electronice nr. 72/2025 și Hotărârii Guvernului nr. 728/2023 cu privire la site-urile web oficiale ale autorităților publice și cerințele minime privind profilurile de socializare ale acestora care utilizează termenul de „site web”. În aceeași ordine de idei menționăm că termenul dat în versiunea în limba engleză a Regulamentul (UE) nr. 910/2014 este de „certificate services for website authentication”, iar propunerea expusă în prezentul punct din aviz reflectă mai corect, sub aspectul traducerii, noțiunea de „site web” .	
	17.2	Prin Legea nr. 327/2025 pentru modificarea unor acte normative (îmbunătățirea managementului finanțelor publice), Parlamentul a operat modificări substanțiale la Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014, conform cărora, începând cu 1 ianuarie 2027: -noțiunea de „autoritate/instituție publică la autogestiune” este înlocuită cu noțiunea de „instituție publică”, iar statutul acesteia se definește în funcție de sursele de finanțare – respectiv, instituție bugetară (finanțată din venituri bugetare) sau instituție publică finanțată integral din venituri proprii (constituite din prestarea contra plată a serviciilor conform statutului instituției); -principiile de gestionare a finanțelor de către instituțiile publice finanțate integral din venituri proprii sunt reglementate prin art. 453 din Legea nr. 181/2014; -nomenclatorul lucrărilor și serviciilor contra plată, mărimea tarifelor, calculate în baza metodologiei de calculare a tarifelor aprobată de Guvern, sunt stabilite de către fondatorul instituției, iar metodologia respectivă urmează a fi promovată independent de fiecare autoritate publică în calitate de fondator.	**Nu se acceptă.** În baza propunerilor recepționate în proces de avizare prevederile art. 5 alin. (1) din proiect au fost revizuite fiind exclusă referința la AGE.

		Luând în considerare cele menționate, ținând cont de perspectiva includerii AGE în categoria „instituției publice finanțate integral din venituri proprii”, fapt care impune adaptarea concomitentă a întregului cadru normativ secundar care reglementează activitatea instituției și mecanismele contractuale prin care aceasta prestează servicii electronice guvernamentale, pentru a asigura certitudine juridică rolului AGE în procesul de creare, administrare, mentenanță și dezvoltare a portofelului pentru identitate digitală, alin. (1) al art. 5 se va expune cu următorul cuprins: „(1) În scopul asigurării accesului securizat, fiabil și neîntrerupt al persoanelor fizice și juridice la servicii publice și, după caz, private, cu menținerea controlului deplin asupra datelor proprii, Instituția Publică Agenția de Guvernare Electronică, în calitate de deținător, dezvoltă și asigură disponibilitatea unui portofel pentru identitate digitală.”	
	17.3	Trimiterea de la art. 9 alin. (1) și anume „mecanismele de validare menționate la art. 5 alin. (8)” este una eronată, pe motiv că mecanismele de validare sunt reglementate la art. 5 alin. (9), pe când alin. (8) tratează „funcționalitățile suplimentare ale portofelului stabilite de Guvern”. În acest sens, recomandăm ajustarea trimiterii conform celor enunțate.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	17.4	Norma de la art. 9 alin. (4) este una incompletă, fiind lipsită de un predicat și sens normativ. Astfel, propunem următoarea redacție pentru alin. (4), cu următorul cuprins: „(4) Organismul de supraveghere asigură, fără întârzieri nejustificate, operarea modificărilor corespunzătoare în lista menționată la art. 8.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	17.5	La art. 12 alin. (2) lit. a) și b) descrierea pentru „nivelul de asigurare scăzut” și „nivelul de asigurare substanțial” sunt definite prin formularea expresiei „asigură un grad substanțial de încredere”, ceea ce face indistincte cele două niveluri. Aceasta constituie o eroare de transpunere a art. 8 alin. (2) lit. (a) din Regulamentul (UE) nr. 910/2014, care stabilește că nivelul scăzut „asigură un grad limitat de încredere” („limited degree of confidence”). În acest sens, recomandăm ajustarea normelor conform celor enunțate.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	17.6	În conformitate cu Măsura nr.10 Reforma nr.3 Pilonul 2 din Anexa 1 a Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025-2027, aprobată prin Hotărârea Guvernului nr.60/2025, Măsura 15.2 din Foaia de parcurs privind „Reforma administrației publice” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană), aprobată prin Hotărârea Guvernului nr.274/2025, dar și Acțiunea 7 Anexa B Capitolul 10 din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotărârea Guvernului nr.306/2025, până la sfârșitul anului 2027, AGE urmează să asigure implementarea Portofelului de identitate digitală în conformitate cu eIDAS 2.0 (Regulamentul UE 2024/1183). Luând în considerare angajamentele asumate de Republica Moldova prin documentele de politici sus-menționate, ținând cont de faptul că Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere nu reglementează portofelul pentru identificare digitală, propunem ca proiectul de lege să intre în vigoare pe parcursul anului 2027, dar nu la expirarea a 18 luni de la data publicării în Monitorul Oficial al Republicii Moldova a proiectului de lege, așa cum este prevăzut în redacția actuală a art.69 alin.(1). Subsecvent, AGE va putea asigura implementarea portofelului pentru identitate digitală în conformitate cu proiectul de lege care transpune Regulamentul UE 2024/1183, iar Republica Moldova va putea raporta către Comisia Europeană îndeplinirea angajamentelor asumate nu doar pe partea de transpune a cadrului normativ eIDAS 2.0, dar și a implementării acestui cadru în partea care se referă la portofelul pentru identitate digitală.	**Se acceptă.** Termenul de intrare în vigoare a legii a fost redus de la 18 luni la 12 luni, urmând ca intrarea în vigoare a legii să se producă pe parcursul anului 2027.
	17.7	Conform pct. 4.2 din nota de fundamentare, sursa de finanțare nu este cuantificată exact și nu sunt identificate alocările bugetare necesare. La subiect, aducem la cunoștință că pentru asigurarea implementării portofelului pentru identitate digitală și integrarea acestuia în ecosistemul național de servicii publice electronice, AGE îi revin atribuții de dezvoltare, implementare, mentenanță și operare	**Se acceptă.** Nota informativă a fost modificată conform propunerii.

		a componentelor tehnice, precum și de asigurare a interoperabilității cu sistemele informaționale de stat și, după caz, ale furnizorilor privați. În același timp, Agenția asigură conformarea la standardele aplicabile și participă la inițiative europene relevante (inclusiv consorții de pilotare) pentru testarea soluțiilor interoperabile și pregătirea recunoașterii transfrontaliere. Cheltuielile estimate pentru anii 2027-2030 aferente implementării portofelului pentru identitate digitală vizează licențe, suport, dezvoltare, mentenanță, operaționalizare și certificare. Structura acestora reflectă atât componente recurente, necesare pentru funcționarea continuă, cât și cheltuieli punctuale aferente certificării periodice a soluției și a mecanismului de înregistrare și verificare a identității, realizată o dată la doi ani. În temeiul celor expuse, conform art. 30 alin. (1) lit. f) din Legea nr. 100/2017, considerăm oportună completarea Notei de fundamentare cu costurile financiare aferente implementării portofelului pentru identitate digitală pentru perioada 2027–2030, în cuantum total de circa 63,5 mil lei. Pentru anul 2026 este deja aprobată suma de 2.200.000 MDL, spre finanțare din resursele Planului de creștere, pentru achiziționarea licențelor SAM pentru dezvoltarea semnăturii electronice „la distanță”.	
I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” (Nr. 1.4/951/26 din 20.05.2026)	18.1	La art. 3 din proiect: 1.1. La pct. 8, definiția noțiunii de „beneficiar” se va expune conform definiției de la pct. 6 a art. 3 din 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. Astfel, se propune expunerea noțiunii de „beneficiar” în următoare redacție: „beneficiar - persoană fizică sau juridică care beneficiază de identificarea electronică, de portofelele pentru identitatea digitală sau de alte mijloace de identificare electronică sau de un serviciu de încredere”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.2	La pct. 35 lit. c), cuvântul „finanțată” se va substitui cu „finanțat”, cuvântul „acestora” se va substitui cu „acestuia”, sintagma „ori	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		au” se va substitui cu „ori are”. De asemenea, cuvântul „jumătate” se va substitui cu textul „peste 50%”, conform definiției de la pct. 8 a art. 3 din Regulamentul (UE) nr. 910/2014.	
	18.3	Definiția noțiunii de „portofel pentru identitatea digitală” se va expune conform definiției de la pct. 42 a art. 3 din Regulamentul (UE) nr. 910/2014. Or, în redacția actuală se contrazice inclusiv cu prevederile art. 5 alin. (5) pct. 5 din proiectul de lege supus avizării.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.4	De la pct. 43 se va exclude articolul „un”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.5	Suplimentar, se propune excluderea noțiunilor de „serviciu de platformă esențial”, „utilizator comercial”, „sursa autentică”, or aceste noțiuni nu sunt reglementate de Regulamentul (UE) nr. 910/2014 transpus și potrivit art. 54 alin. (4) din Legea 100/2017 cu privire la actele normative, în cazul în care se impune utilizarea unor noţiuni sau termeni consacrați din tratatele internaționale la care Republica Moldova este parte ori din legislaţia Uniunii Europene (în continuare UE), în proiect se asigură corespunderea acestora termenilor sau, respectiv, noțiunilor consacrate din legislația națională.	**Se acceptă parțial.** Noțiunea „sursa autentică” este definită în art. 3 pct. 47 din Regulamentul (UE) nr. 910/2014.
	18.6	La art. 5: 2.1.În scopul, reproducerii și transpunerii complete a prevederilor Regulamentului (UE) nr. 910/2014, alin. (1) se va expune în următoare redacție: „(1) În scopul garantării faptului că toate persoanele fizice și juridice din Republica Moldova au un acces securizat, fiabil și neîntrerupt la servicii publice și private, păstrând totodată controlul deplin asupra datelor lor, Guvernul va asigura prin actele sale normative, funcționarea cel puțin unui portofel pentru identitatea digitală.”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.7	La alin. (17), cuvântul „comportamentul” se va substitui cu „comportamentului”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.8	La alin. (18), anterior cuvântului „furnizorii” se va completa cu prepoziția „de”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	18.9	Din art. 6 alin. (2) se va exclude textul: „se desfășoară prin intermediul Portalului guvernamental integrat EVO și”, or cadrul normativ european nu stabilește careva mecanisme suplimentare, în afara de cele din Regulamentul (UE) nr. 910/2014 pentru procesul de înregistrare. Totodată, formularea dată poate crea impedimente în procesul de asigurare a interoperabilității între portofele, inclusiv europene	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.10	De la art. 7 alin. (1), se va exclude cuvântul „acreditate”, întrucât din definiția noțiunii de „organism de evaluare a conformității” reiese necesitatea deținerii unei acreditări.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.11	Conform cadrului UE, suspendarea și retragerea portofelelor pentru identitate digitală, în cazul încălcărilor sau compromiterii componentelor, nu este realizată de către furnizori, delimitând atribuțiile pentru funcționarea transparentă și sigură a serviciului. Astfel, alin. (1) și (2) din art. 9 din proiect urmează a fi expuse în următoare redacție: „(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, organismul de supraveghere suspendă fără întârziere nejustificată furnizarea și utilizarea portofelelor pentru identitatea digitală. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați. (2) În cazul în care încălcarea securității sau compromiterea menționată la alin. (1) nu este remediată în termen de trei luni de la suspendare, organismul de supraveghere retrage portofelele pentru identitatea digitală și le revocă valabilitatea. Furnizorii portofelelor pentru identitatea digitală informează în mod corespunzător utilizatorii și beneficiarii afectați.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.12	La alin. (4) al art. 9, anterior cuvântului „modificările” se va completa cu cuvântul „publică”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunerile recepționate în proces avizare.

	18.13	La art. 10: 7.1.La alin. (1), sintagma „Uniunea Europeană” se va substitui cu „Uniunii Europene”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.14	La alin. (2), textul „solicită identificarea sau autentificarea electronică a utilizatorilor” se va substitui cu textul „solicită autentificarea strictă a utilizatorilor,”, conform prevederilor art. 5f alin. (2) din Regulamentul (UE) nr. 910/2014.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunerile recepționate în proces avizare.
	18.15	La art. 11 alin. (1) lit. c), cuvântul „organismele” se va substitui cu cuvântul „organismul”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.16	La art. 12 alin. (2) lit. a), sintagma „grad substanțial” se va substitui cu „grad limitat”, iar sintagma „reduce substanțial riscul” se va substitui cu „reduce riscul”, conform prevederilor art. 8 alin. (2) lit. (a) din Regulamentul (UE) nr. 910/2014.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.17	Având în vedere că la art. 9 alin. (3) din Regulamentul (UE) nr. 910/2014, se stabilește un termen limitat în interiorul căruia Comisia publică lista sistemelor de identificare electronică care au fost notificate în temeiul alin. (1), urmează ca același termen să se reglementeze la alin. (2) al art. 13 din proiectul de lege	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.18	La alin. (3) al art. 15, cuvântul „cadru” se va substitui cu „cadrul”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.19	La alin. (1) al art. 17, sintagma „prezenta lege” se va substitui cu „prezentei legi”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.20	La art. 21 lipsește prevederea care determină modul de stabilire a standardelor de referință, specificațiilor și procedurilor (cum este menționat în art. 20 alin. (4) din Regulamentul 910/2014). În acest sens, se propune completarea art. 21 din proiect cu un alineat nou cu următorul conținut: „(9) Guvernul va stabili o lista de referință, 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	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		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 conformității prestatorilor de servicii de încredere calificați și pentru furnizarea raportului menționat la alineatul (1)".	
	18.21	Cu referire la alin. (6)-(8) din art. 22 din proiect, reieșind din faptul că prestatorii de servicii de încredere din UE au trecut procesul de notificare și auditurile necesare și sunt incluși în lista sigură UE, impunerea notificării suplimentare către organismul de supraveghere din Republica Moldova creează impedimente în autorizarea, funcționarea serviciilor de încredere calificate UE pe teritoriul Republicii Moldova și poate fi calificată drept opunerea la recunoașterea serviciilor de încredere UE. Astfel, se propune expunerea alin. (6)-(7) din art. 22 din proiect, în următoarea redacție: „(6) Prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene păstrează statutul de calificat pe teritoriul Republicii Moldova, fără necesitatea desfășurării notificării sau procedurilor de verificare. (7) Organismul de supraveghere, va introduce în lista sigură națională și în Registru de evidență a prestatorilor de servicii de încredere calificați, pe prestatorii de servicii de încredere calificați din statele membre ale Uniunii Europene și va actualiza automat statutul acestora."	**Se acceptă parțial.** Nu a fost acceptată propunerea privind includerea acestor prestatori în lista sigură națională. Acest instrument are rolul de a reflecta prestatorii aflați sub jurisdicția și supravegherea organismului național de supraveghere, respectiv prestatorii pentru care acesta exercită atribuții de monitorizare, control și aplicare a măsurilor prevăzute de lege. În cazul prestatorilor stabiliți în statele membre ale Uniunii Europene, competențele de supraveghere și actualizare a statutului acestora aparțin autorităților competente din statele respective, informațiile oficiale fiind publicate și actualizate prin intermediul listelor de încredere naționale și al Listei de încredere a Uniunii Europene (EU Trusted List). Prin urmare, pentru a evita dublarea mecanismelor de evidență și pentru a asigura utilizarea informațiilor oficiale furnizate de autoritățile competente ale statelor membre, proiectul a fost completat cu o soluție alternativă, potrivit căreia organismul de supraveghere preia informațiile relevante din listele de încredere naționale ale statelor membre și le publică pe pagina sa oficială, asigurând actualizarea acestora în funcție de modificările operate în listele respective. Această abordare permite informarea utilizatorilor și facilitarea verificării statutului prestatorilor europeni,

			fără a crea un regim paralel de înregistrare sau supraveghere la nivel național.
	18.22	La alin. (3) lit. b) al art. 24, trimiterea la „alin. (3)” se va substitui cu „alin. (2)”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.23	În scopul oferirii unor instrumente și criterii pentru semnătura electronică avansată, se propune alin. (2) al art. 27 din proiect să fie expus în următoarea redacție: „(2) Guvernul stabilește listă de standarde de referință și specificații și proceduri pentru semnăturile electronice avansate. În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele referitoare la semnăturile electronice avansate.”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.24	Art. 28 din proiect, transpune eronat și contrar prevederilor Regulamentului (UE) nr. 910/2014, limitând utilizarea serviciilor de încredere avansate și avansate bazate pe certificat calificat. Omisiunea depistată poate fi interpretată de către UE ca fiind neconformarea în proces de transpunere. Astfel, se propune expunerea art. 28 în următoare redacție: „Articolul 28. Semnăturile electronice în cadrul serviciilor publice (1) În cazul în care se solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, se recunosc 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 (4). (2) În cazul în care se 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, se recunosc semnăturile electronice 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 (4). (3) Nu se solicită o semnătură electronică la un nivel de securitate mai	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		ridicat decât cel al semnăturii electronice calificate pentru utilizarea în cadrul unui serviciu online prestat de un organism din sectorul public. (4) Guvernul aprobă, formate de referință ale semnăturilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative.”	
	18.25	Din momentul în care Regulamentul (UE) nr. 910/2014 nu prevede posibilitatea suspendării certificatului cheii publice, se consideră inoportună includerea acestei prevederi în art. 29 alin. (4) din proiect. Astfel, se propune excluderea acestui alineat.	**Nu se acceptă.** Deși regula generală instituită de regulament vizează emiterea, revocarea și expirarea certificatelor calificate, art. 28 alin. (5) recunoaște în mod expres dreptul statelor membre de a stabili, prin legislația națională, norme privind suspendarea temporară a certificatelor calificate pentru semnătură electronică, cu condiția respectării cerințelor prevăzute la lit. a) și b) ale alineatului respectiv. Prin urmare, suspendarea temporară a certificatelor nu este exclusă de cadrul european, ci reprezintă o opțiune normativă lăsată la discreția statelor, în vederea gestionării situațiilor în care există incertitudini temporare privind utilizarea certificatului, fără a fi necesară revocarea definitivă a acestuia. Menținerea mecanismului de suspendare în proiect este justificată atât din perspectiva protecției titularilor certificatelor, cât și a proporționalității măsurilor aplicabile. Suspendarea temporară oferă o soluție intermediară între menținerea valabilității certificatului și revocarea acestuia, fiind utilă în situații precum suspiciunea compromiterii dispozitivului de creare a semnăturii, pierderea temporară a controlului asupra mijloacelor de autentificare sau alte circumstanțe care necesită blocarea imediată a utilizării certificatului până la clarificarea situației.

			Totodată, proiectul transpune condițiile prevăzute de art. 28 alin. (5) din Regulamentul (UE) nr. 910/2014, stabilind expres că certificatul suspendat își pierde valabilitatea pe durata suspendării și că statutul de suspendare trebuie să fie vizibil prin intermediul serviciului de verificare a statutului certificatelor. În aceste condiții, excluderea mecanismului de suspendare ar elimina un instrument recunoscut de cadrul european pentru gestionarea riscurilor asociate utilizării certificatelor calificate, fără a exista o obligație legală în acest sens.
	18.26	Setul de date specificat la art. 30 alin. 2) lit. b), art. 41 alin. 2) lit. b), art. 50 alin. 2) lit. b) și art. 54 alin. 2) lit. b), se va expune conform cerințelor din Anexele I, III, IV și V la Regulamentul (UE) nr. 910/2014, după cum urmează: „a) în cazul unei persoane juridice: denumirea și, după caz, numărul de identificare de stat, b) în cazul unei persoane fizice: numele persoanei;”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.27	Din aceleași considerente, la art. 41 alin. 3) și art. 50 alin. 3), se va exclude textul „/prenumele”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.28	Potrivit art. 28 alin. (2) din Regulamentul (UE) 910/2014 certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa I (cerințele). Pentru transpunerea corectă a prevederilor Regulamentului (UE) 910/2014 se propune: 21.1. expunerea art. 31 alin. (5) din proiect în următoare redacție: „(5) Guvernul stabilește 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 la alin. (2) și (3).”	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.

	18.29	21.2. completarea art. 32 cu un alineat nou cu următorul conținut: „(2) Guvernul stabilește o listă de standarde de referință și specificații și proceduri în scopul aplicării alineatului (1) de la prezentul articol.”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	18.30	21.3. expunerea art. 35 alin. (2) din proiect în următoare redacție: „(2) Guvernul stabilește listă de standarde de referință și 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.”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	18.31	21.5. expunerea art. 40 alin (7) din proiect în următoare redacție: „(7) Guvernul stabilește listă de standarde de referință și specificații și proceduri pentru certificatele calificate pentru sigiliul electronic. În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele prevăzute în alin. (1).”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	18.32	21.6. expunerea art. 47 alin. (2) din proiect în următoare redacție : „(2) Guvernul stabilește o listă de standarde de referință și specificații și proceduri pentru legătura dintre dată și oră și date și pentru stabilirea exactității surselor orei indicate. 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).”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	18.33	21.7. articolele 54, 55, 56, 60, se vor completa cu prevederile despre necesitatea elaborării listelor standardelor și specificațiilor de către Guvern.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.34	22. Regulamentul (UE) 910/2014 determină separat cerințele pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate. Astfel, se propune la art. 34 din proiect, separarea în diferite articole, cerințele pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate calificate.	**Nu se acceptă.** Art. 34 din proiectul de lege transpune integral și corelat prevederile art. 32 și art. 32a din Regulamentul (UE) nr. 910/2014 referitoare la

			cerințele pentru validarea semnăturilor electronice calificate și a semnăturilor electronice avansate bazate pe certificate calificate. Reglementarea într-un singur articol a ambelor categorii de cerințe a fost realizată în mod intenționat, având în vedere caracterul complementar al dispozițiilor respective și necesitatea asigurării unei structuri coerente, concise și sistematizate a normelor privind validarea semnăturilor electronice. Separarea acestora în articole distincte nu este necesară din perspectiva clarității sau aplicabilității normei, întrucât conținutul actual permite delimitarea suficientă a cerințelor aplicabile fiecărei categorii de semnături electronice, menținând în același timp coerența tehnico-legislativă a proiectului.
	18.35	23. Art. 39 din proiect, transpune eronat și contrar prevederilor art. 37 din Regulamentul (UE) 910/2014, limitând astfel utilizarea serviciilor de încredere avansate și avansate bazate pe certificat calificat. Omisiunea depistată poate fi interpretată de către UE ca fiind neconformarea în proces de transpunere. Astfel, se propune expunerea art. 39 în următoare redacție: „Articolul 39. Sigiliile electronice în cadrul serviciilor publice (1) În cazul în care se solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, sunt recunoscute 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 menționate la alineatul (4). (2) În cazul în care se 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 sunt recunoscute sigiliile electronice avansate bazate pe un certificat calificat și sigiliile electronice calificate care întrebuințează cel puțin formatele sau	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		metodele definite în actele menționate la alineatul (4). (3) Nu se solicită sigiliu electronic la un nivel de securitate mai ridicat decât cel al sigiliului electronic calificat pentru utilizarea serviciu online prestat de un organism din sectorul public. (4) Guvernul definește, formate de referință ale sigiliilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative.”.	
	18.36	Din cuprinsul alin. (6) al art. 40 se va exclude cuvântul „acesta”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.37	Alin. (1) al art. 48 se va completa cu cuvântul „calificată”, astfel cum este prevăzut la art. 43 alin. (1) din Regulamentul (UE) nr. 910/2014.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.38	Din cuprinsul alin. (3) al art. 51, se va exclude cuvântul „își”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.39	Din cuprinsul alin. (4) al art. 51 și alin. (1) al art. 68, se va exclude cuvântul „competent” fiind de prisos. Or, la art. 64 s-a determinat expres că rolul de „organism de supraveghere”, în cadrul aferent portofelului pentru identitatea digitală cât și pentru serviciile de încredere, este exercitat de aceeași autoritate.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.40	La alin. (2) lit. c) al art. 55, cuvântul „genul” se va substitui cu „sexul”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.41	În cuprinsul art. 56, sintagma „organismul public” se va substitui cu „organismul din sectorul public”, conform terminologiei definite la art. 3.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.42	La alin. (5) al art. 63, după sintagma „documentul electronic” se va completa cu „semnat cu semnătură electronică calificată”, având în vedere prevederile alin. (1) al aceluiași articol.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.43	La art. 64 alin. (2):	
	18.44	31.1.La lit. a) și b), după sintagma „Republica Moldova”, respectiv „Republicii Moldova”, se va completa cu sintagma „și asigurarea”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	18.45	31.2.La lit. c), sintagma „sunt informate” se va substitui cu sintagma „este informat”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.46	31.3.La lit. h) se va exclude cuvântul „să”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.47	La art. 64: 32.1.Se impune eliminarea prevederilor de la alin. (3) pct. 2) lit. d), întrucât acestea introduc sarcini suplimentare pentru organismele de supraveghere, care nu își regăsesc temeiul în art. 46b din Regulamentul (UE) nr. 910/2014. Având în vedere natura obligatorie și direct aplicabilă a normelor unionale, Regulamentul (UE) nr. 910/2014 nu conferă statelor membre marja de apreciere necesară pentru instituirea unor competențe sau obligații adiționale în sarcina acestor organisme.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.48	La alin. (4), trimiterea la „alin. (4)” se va substitui cu trimitere la „alin. (3)”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	18.49	Sintagma „notificate Comisiei Europene” este confuză în contextul alin. (1) al art. 67 întrucât în cuprinsul proiectului nu se regăsesc prevederi cu privire la obligativitatea notificării Comisiei Europene despre careva obligații. În acest sens se va reformula alin. (1).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
Ministerul Agriculturii și Industriei Alimentare (Nr. 2026PLP-1561 din 25.05.2026)	19.1	La alin. (1) al art. 69, textul „18 de luni” se va substitui cu „18 luni”. În această ordine de idei, se va ajusta corespunzător Tabelul de concordanță și se va asigura că trimiterile utilizate coincid cu prevederile din proiectul de lege.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	19.2	1) Obiecții argumentate și explicite pe marginea cărora trebuie să se ajungă la un acord: La art. 5 alin. (19), norma propusă este lipsită de claritate în ceea ce privește locul unde organismul de supraveghere publică va publica informația indicată în textul alineatului. De asemenea, observăm că Regulamentul Uniunii Europene, care se transpune prin proiect, la art. 5a alin. (18) lit. a), nu indică informația cu privire la „mecanismul de întocmire și menținere a listei beneficiarilor înregistrați”, ci indică informația	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		cu privire la „organismul responsabil cu întocmirea și menținerea listei beneficiarilor înregistrați”. În această ordine de idei, considerăm necesară redactarea alineatului pentru a-i asigura claritatea. La art. 11 alin. (1) lit. c), atragem atenția că Regulamentul UE la art. 6 alin. (1) lit. (c) nu stabilește condiția pentru recunoaștere ca 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. Or, în procesul de aplicare a viitoarei Legi, orice organism public din sectorul public care nu dispune de infrastructura tehnică necesară poate invoca această condiție pentru a refuza recunoașterea, golind de conținut norma instituită prin Lege.	
	19.3	2) Propuneri care poartă caracter de recomandare: La art. 5 alin. (1), dorim să atragem atenția că una dintre funcțiile Guvernului, stabilită în Legea nr. 136/2017 cu privire la Guvern, constă în organizarea executării legii, care, în particular, se materializează prin desemnarea sau crearea autorităților ori a instituțiilor responsabile de aplicarea legilor. Din această perspectivă, apreciem că, prin indicarea în lege a instituției publice care are sarcina de a asigura disponibilitatea unui portofel pentru identitate digitală, se încalcă competența Guvernului de a decide cea mai bună modalitate de organizare a executării legii. Astfel propunem substituirea textului „Instituția Publică Agenția de Guvernare Electronică asigură” prin textul „Guvernul desemnează o entitate publică care va asigura”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	19.4	La art. 64 alin. (1), în opinia Ministerului, desemnarea Serviciului de Informații și Securitate în calitate de organism de supraveghere poate determina o reticență din partea statelor membre în a coopera cu acesta în procesul de aplicare a Legii, având în vedere că atribuțiile Serviciului țin de securitatea națională, care se realizează prin mecanisme mai puțin transparente.	**Se acceptă de principiu.** Obiecția este reținută ca fiind relevantă din perspectiva alinierii la bunele practici europene privind separarea funcțiilor de supraveghere în domeniul serviciilor de încredere și al portofelelor pentru identitatea digitală, acestea fiind exercitate, în mod obișnuit, de autorități civile specializate.

			Totuși, la etapa actuală, Serviciul de Informații și Securitate exercită deja atribuții de supraveghere în domeniul vizat, iar proiectul de lege urmărește asigurarea continuității instituționale, în contextul angajamentelor Republicii Moldova de transpunere într-un termen restrâns a Regulamentului (UE) nr. 910/2014 și a cadrului aferent. În lipsa unei autorități publice alternative care să dispună în prezent de capacitățile instituționale necesare pentru preluarea integrală a acestui mandat, se optează pentru menținerea soluției propuse în proiect. Totodată, se reține necesitatea analizării, în perioada imediat următoare, a opțiunilor de reconfigurare instituțională a funcției de supraveghere, inclusiv prin identificarea și consolidarea capacităților unei autorități civile specializate, în vederea unei eventuale preluări a acestui mandat într-un cadru ulterior de ajustare legislativă.
Asociația Băncilor din Moldova (Nr. 02-08/162 din 03.06.2026)	20.1	I. Cu privire la semnătura electronică Cu referire la art. 63 alin. (3) din Proiect, Asociația Băncilor din Moldova propune modificarea acestuia și expunerea în următoarea redacție: Clauză proiect : ” 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. Clauză propusă:	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		„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.” În acest sens, considerăm necesară excluderea sintagmei „printr-un înscris distinct semnat olograf sau cu semnătură electronică calificată”. Introducerea obligației de a încheia un înscris distinct, semnat olograf sau cu semnătură electronică calificată, pentru recunoașterea validității semnăturilor electronice simple, avansate sau a altor mijloace electronice de exprimare a consimțământului constituie o barieră administrativă și juridică disproporționată. O asemenea condiție este contrară obiectivelor de digitalizare și simplificare a relațiilor juridice promovate atât la nivel național, cât și la nivel european. În forma actuală, soluția propusă în Proiect creează o condiție suplimentară care reduce în mod nejustificat aplicabilitatea practică a semnăturilor electronice non-calificate și limitează dezvoltarea serviciilor digitale. În practică, cerința privind existența unui înscris distinct ar transforma utilizarea instrumentelor electronice moderne într-un proces birocratic și hibrid, incompatibil cu necesitatea prestării rapide și eficiente a serviciilor financiare și digitale. Sectorul bancar utilizează în mod curent mecanisme digitale de autentificare și confirmare, inclusiv confirmări în aplicațiile bancare, coduri OTP, autentificare multifactorială, autentificare biometrică, confirmări efectuate prin platforme securizate de internet banking și mobile banking, precum și alte mijloace tehnice de exprimare a consimțământului clientului. Aceste mecanisme sunt esențiale pentru prestarea serviciilor bancare la distanță, inclusiv pentru contractarea și administrarea conturilor, depozitelor, cardurilor, creditelor, plăților și altor produse sau servicii financiare.	

		Reglementarea propusă nu este pe deplin corelată cu principiile consacrate de Codul civil al Republicii Moldova privind libertatea contractuală și autonomia de voință a părților. Cu titlu de referință, Articolul 318 din Codul civil, stabilește: (1)Actul juridic scris sau autentic are formă electronică dacă se cuprinde într-un document electronic care întrunește condițiile legii, (2)Tipurile de semnături electronice care pot fi aplicate unui document electronic, gradul de protecție al fiecărui tip și valoarea juridică sunt determinate de lege. (3)Actul juridic scris se încheie în formă electronică dacă este semnat cu semnătura electronică avansată calificată a persoanei care încheie actul, dacă acordul părților sau legea nu prevede cerința de utilizare a unui alt tip de semnătură electronică. Prin urmare, Codul civil recunoaște expres dreptul părților de a conveni asupra tipului de semnătură electronică utilizat în raporturile dintre acestea. În acest context, impunerea suplimentară a unui înscris distinct restrânge nejustificat libertatea contractuală deja garantată de cadrul legislativ existent și creează o formalitate suplimentară care nu este necesară în toate cazurile. De asemenea, Legea nr. 157/2014 privind încheierea și executarea contractelor la distanță privind serviciile financiare de consum recunoaște validitatea consimțământului exprimat prin mecanisme electronice, inclusiv prin coduri OTP, confirmări efectuate prin platforme securizate sau alte mijloace tehnice de autentificare. În aceste condiții, obligarea consumatorului de a semna în prealabil un înscris distinct, olograf sau cu semnătură calificată, pentru a putea utiliza ulterior o semnătură electronică simplă sau avansată, lipsește de efect util mecanismele moderne de contractare la distanță și afectează accesibilitatea serviciilor digitale. Cerința unui înscris distinct este, de asemenea, dificil de conciliat cu practicile internaționale și cu tendințele europene de reglementare în domeniul serviciilor de încredere și al identificării electronice. Regulamentul eIDAS reprezintă principalul reper normativ european în materie, iar Republica Moldova urmărește	

		alinierea la standardele acestuia. Logica eIDAS promovează neutralitatea tehnologică și recunoașterea diferitelor modalități de exprimare a consimțământului în mediul electronic, inclusiv prin mecanisme de tip click-wrap, autentificare multifactorială sau confirmări prin SMS și aplicații digitale. În același timp, formularea actuală a Proiectului poate genera dificultăți semnificative de implementare pentru instituțiile financiare, prestatorii de servicii de plată, societățile fintech și alte companii care utilizează procese digitale de onboarding și contractare la distanță. Impunerea unei formalități suplimentare va conduce inevitabil la creșterea costurilor operaționale, la diminuarea eficienței proceselor digitale și la descurajarea inovației. Considerăm important de subliniat și impactul potențial asupra obiectivelor de incluziune financiară asumate de Republica Moldova. Proiectul Strategiei Naționale de Incluziune Financiară a Republicii Moldova 2030 și Conceptul SNIF 2030 consacră necesitatea facilitării accesului populației la servicii financiare digitale, dezvoltării canalelor electronice de interacțiune și reducerii barierelor administrative în accesarea serviciilor financiare. În același sens, actele strategice naționale, inclusiv Strategia Națională de Dezvoltare „Moldova Europeană 2030” și planurile naționale de dezvoltare, tratează incluziunea financiară ca obiectiv important și promovează extinderea accesului la servicii financiare, digitalizarea plăților, dezvoltarea serviciilor electronice și creșterea nivelului de educație financiară. Or, introducerea unor formalități suplimentare pentru utilizarea semnăturilor electronice altele decât cele calificate riscă să creeze bariere suplimentare pentru consumatori, în special pentru persoanele din zone rurale, utilizatorii cu acces limitat la infrastructura digitală, categoriile vulnerabile și cetățenii Republicii Moldova aflați în afara țării, pentru care serviciile financiare digitale reprezintă adesea cea mai accesibilă sau unica soluție practică. În consecință, norma propusă riscă să producă un efect de regres digital, prin descurajarea utilizării instrumentelor moderne de semnare și autentificare electronică. Acest efect poate afecta competitivitatea mediului de afaceri, accesul consumatorilor la	

		servicii financiare rapide și accesibile, precum și eforturile naționale de digitalizare a economiei. Totodată, menținerea acestei condiții poate crea premise pentru interpretări neuniforme și incertitudine juridică privind validitatea actelor juridice încheiate prin mijloace electronice, în special în raporturile comerciale și de consum în care utilizarea semnăturilor electronice simple sau avansate reprezintă deja o practică consacrată. Având în vedere cele expuse, Asociația Băncilor din Moldova consideră oportună excluderea sintagmei „printr-un înscris distinct semnat olograf sau cu semnătură electronică calificată”, astfel încât norma să asigure un echilibru adecvat între securitatea juridică, libertatea contractuală și necesitatea dezvoltării serviciilor digitale moderne. Soluția propusă nu exclude posibilitatea utilizării semnăturii electronice calificate în cazurile în care aceasta este necesară și prevăzută expres de actele normative. Dimpotrivă, ea permite păstrarea unui cadru flexibil, proporțional și compatibil cu evoluțiile tehnologice, în care nivelul de formalism juridic este adaptat naturii actului, riscurilor operațiunii și voinței părților.	
	20.2	Pe lângă aspectele ce țin de regimul juridic al semnăturilor electronice, considerăm necesară clarificarea unor prevederi ale Proiectului referitoare la utilizarea pseudonimelor, beneficiarii portofelului pentru identitatea digitală, lista sistemelor de identificare electronică notificate și metodele alternative de identificare. Aceste clarificări sunt importante pentru evitarea interpretărilor neuniforme, corelarea Proiectului cu cadrul normativ sectorial aplicabil băncilor și asigurarea unei implementări coerente în practică. 1. Cu privire la art. 4 alin. (1) – utilizarea pseudonimelor în tranzacțiile electronice Cu referire la art. 4 alin. (1) din Proiect, potrivit căruia utilizarea pseudonimelor alese de utilizatori în cadrul tranzacțiilor electronice este permisă, propunem completarea art. 3 cu o definiție a noțiunii de „pseudonim”.	**Nu se acceptă.** Proiectul reglementează în mod suficient utilizarea pseudonimelor prin dispozițiile art. 4 alin. (2) și (3), care prevăd expres că utilizarea pseudonimelor nu aduce atingere obligațiilor legale de identificare a utilizatorilor acolo unde acestea sunt prevăzute de cadrul normativ aplicabil și nu poate fi opusă cerințelor de identificare impuse de lege. Noțiunea de „pseudonim” este utilizată în proiect în sensul consacrat de Regulamentul (UE) nr. 910/2014 (eIDAS) și de Regulamentul (UE) 2024/1183 (eIDAS2), acte normative ale căror prevederi sunt transpuse prin prezentul proiect. Introducerea unei definiții proprii în legislația națională, cu un conținut distinct

		Considerăm necesar ca definiția să clarifice sensul noțiunii, perimetrul de utilizare al pseudonimului și faptul că acesta nu este utilizat în scopul ascunderii identității persoanei. În lipsa unei definiții clare, prevederea poate genera interpretări neuniforme, inclusiv percepția greșită că pseudonimul ar putea fi utilizat pentru eludarea obligațiilor de identificare a persoanei, de cunoaștere a clientului, de trasabilitate sau de conformare cu cerințele aplicabile în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. În acest sens, propunem completarea art. 3 cu o definiție orientativă în următoarea redacție: „Pseudonim – identificator ales sau atribuit unui utilizator, utilizat în cadrul tranzacțiilor electronice pentru interacțiunea acestuia în mediul digital, fără afișarea directă a tuturor datelor de identificare, cu menținerea posibilității de identificare a persoanei în condițiile legii. Utilizarea pseudonimului nu are ca scop și nu produce efectul ascunderii identității utilizatorului față de prestatorii de servicii, autoritățile competente sau alte persoane îndreptățite să solicite identificarea potrivit cadrului normativ aplicabil.” O asemenea completare ar asigura aplicarea uniformă a legii și ar reduce riscurile de înțelegere greșită a scopului creării și utilizării pseudonimelor.	față de cel utilizat la nivel european, ar putea genera neconcordanțe între cadrul național și cel al Uniunii Europene, contrar obiectivului de armonizare urmărit prin Proiect. Referitor la îngrijorarea exprimată cu privire la potențiala utilizare a pseudonimului în scopul eludării obligațiilor de identificare este de menționat că aceasta este acoperită în mod expres de art. 4 alin. (2) din proiect, care prevede că utilizarea pseudonimelor nu aduce atingere obligațiilor legale privind identificarea utilizatorilor, acolo unde aceasta este prevăzută de cadrul normativ aplicabil. Această prevedere acoperă, implicit, și obligațiile ce decurg din legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului, precum și orice alte obligații sectoriale de identificare, inclusiv cele aplicabile instituțiilor de credit. Astfel, utilizarea pseudonimelor nu exonerează persoanele de obligațiile de identificare, de cunoaștere a clientelei (KYC), de trasabilitate sau de alte cerințe prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului ori de alte acte normative sectoriale. De asemenea, formularea propusă introduce elemente ce țin de efectele juridice și de raporturile dintre utilizator, prestatori și autorități, aspecte care sunt deja reglementate prin art. 4 alin. (2) și care rezultă din legislația sectorială aplicabilă.
	20.3	2. Cu privire la art. 6 alin. (4) – corelarea portofelului pentru identitatea digitală cu serviciile specifice și cadrul PCSBFT Cu referire la art. 6 alin. (4) din Proiect, potrivit căruia prevederile alin. (1) și (2) nu aduc atingere cadrului normativ aplicabil	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		prestării serviciilor specifice, considerăm necesară clarificarea expresă a acestei norme. În special, propunem ca textul să includă referințe explicite la categoriile de servicii specifice care nu sunt afectate de prevederile alin. (1) și (2), inclusiv serviciile financiare, serviciile de plată, serviciile bancare și alte servicii reglementate sectorial. Totodată, considerăm necesară menționarea expresă a faptului că utilizarea portofelului pentru identitatea digitală nu substituie și nu limitează aplicarea cadrului normativ special privind prevenirea și combaterea spălării banilor și finanțării terorismului. Astfel, alin. (4) ar putea fi completat cu o formulare de tipul: „Prevederile alin. (1) și (2) nu aduc atingere cadrului normativ special aplicabil prestării serviciilor reglementate, inclusiv serviciilor financiare, bancare, de plată sau altor servicii supuse unor cerințe sectoriale speciale, precum și obligațiilor prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului.” Această clarificare este importantă deoarece, în lipsa unor referințe explicite, norma poate genera incertitudine juridică și interpretări divergente cu privire la aplicabilitatea cerințelor din legislația PCSBFT în contextul utilizării portofelului pentru identitatea digitală, inclusiv în ceea ce privește obligațiile de identificare, verificare, monitorizare și raportare.	
		3. Cu privire la art. 6 alin. (6) – actualizarea datelor beneficiarilor portofelului pentru identitatea digitală Cu referire la art. 6 alin. (6) din Proiect, potrivit căruia beneficiarii înregistrați informează fără întârziere organismul de supraveghere cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alin. (2), considerăm oportună automatizarea proceselor de actualizare a datelor. În acest sens, propunem ca Proiectul să prevadă posibilitatea sau obligația preluării automate a informațiilor modificate din registrele de stat relevante, în măsura în care aceste informații sunt deja înregistrate în sistemele informaționale de stat.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		O asemenea soluție ar permite asigurarea calității, acurateței și actualității datelor, reducerea sarcinii administrative asupra beneficiarilor și creșterea eficienței schimbului de informații între părțile implicate în procesul de identificare electronică și prestare a serviciilor de încredere. În același timp, automatizarea actualizărilor ar contribui la diminuarea riscurilor generate de raportări întârziate, incomplete sau eronate, în special în situațiile în care modificările relevante sunt deja disponibile în registre oficiale ale statului.	
	20.4	4. Cu privire la art. 13 alin. (2) – lista sistemelor de identificare electronică notificate Cu referire la art. 13 alin. (2) din Proiect, care vizează publicarea de către organismul de supraveghere a listei sistemelor de identificare electronică notificate, considerăm necesară clarificarea impactului acestei liste asupra cadrului normativ existent privind identificarea la distanță și alegerea furnizorilor de soluții de identificare electronică. În special, este necesară clarificarea relației dintre lista sistemelor de identificare electronică notificate și reglementările sectoriale aplicabile, inclusiv Hotărârea BNM nr. 281/2024 privind identificarea la distanță. Nu este clar dacă includerea unui sistem în lista publicată de organismul de supraveghere va influența sau condiționa alegerea furnizorilor de către entitățile raportoare. De asemenea, nu este clar dacă sistemele incluse în listă vor beneficia de un regim preferențial sau de o recunoaștere implicită în procesul de aprobare ori utilizare a soluțiilor de identificare la distanță. În acest context, propunem completarea Proiectului cu prevederi care să clarifice expres că: 1.includerea unui sistem de identificare electronică în lista sistemelor notificate nu limitează dreptul entităților de a selecta și utiliza alte soluții conforme cu cadrul normativ aplicabil; 2.lista sistemelor notificate nu instituie, prin ea însăși, un regim exclusiv sau preferențial, cu excepția cazurilor expres prevăzute de lege;	**Se acceptă parțial.** Pentru claritate art. 13 din proiect a fost completat cu noi prevederi din care rezultă cerințele față de sistemele de identificare electronice eligibile pentru includerea în lista respectivă.

		3.efectele juridice ale includerii unui sistem în lista respectivă trebuie definite clar; 4.utilizarea unor soluții care nu se regăsesc în listă rămâne permisă, în măsura în care acestea respectă cerințele legale și normative aplicabile, inclusiv cerințele sectoriale stabilite de autoritățile competente. În lipsa acestor clarificări, prevederea poate genera incertitudini în aplicare și riscuri de interpretare privind selectarea furnizorilor de soluții de identificare electronică, inclusiv în sectorul financiar-bancar.	
	20.5	5. Cu privire la art. 24 alin. (2) – utilizarea altor metode de identificare Cu referire la art. 24 alin. (2) din Proiect, care prevede utilizarea altor metode de identificare ce asigură identificarea persoanei cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității, considerăm necesară clarificarea acestei norme. În forma actuală, nu este clar ce metode concrete sunt avute în vedere, în special în contextul identificării prin mijloace electronice. De asemenea, nu este definit rolul organismului de evaluare a conformității, respectiv dacă acesta reprezintă autoritatea de reglementare, o autoritate publică competentă sau entități acreditate care certifică soluțiile tehnice. Totodată, nu este clar dacă soluțiile de identificare prin mijloace electronice care dețin certificări sau au fost implementate în conformitate cu cadrul normativ național, inclusiv cu Hotărârea BNM nr. 281/2024, se încadrează în această categorie sau în alte prevederi ale Proiectului.	**Nu se acceptă.** Prevederea art. 24 alin. (2) lit. c) are rolul de a asigura neutralitatea tehnologică a cadrului normativ și de a permite utilizarea unor metode de identificare alternative față de cele expres prevăzute la lit. a), b) și d), cu condiția ca acestea să ofere un nivel ridicat de încredere și să fie supuse unei evaluări independente a conformității. Proiectul nu urmărește enumerarea exhaustivă a tuturor soluțiilor tehnice de identificare care pot fi utilizate în practică, întrucât o asemenea abordare ar limita capacitatea cadrului normativ de a răspunde evoluțiilor tehnologice și apariției unor noi metode de identificare electronică. Totodată, noțiunea de „organism de evaluare a conformității” este deja definită în proiect. Potrivit definiției prevăzute la art. 3, organismul de evaluare a conformității reprezintă o persoană juridică independentă, acreditată în Republica Moldova sau într-un stat membru al Uniunii Europene, competentă să efectueze evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate prestate de acesta,

			precum și certificarea portofelelor pentru identitatea digitală și a mijloacelor de identificare electronică. Prin urmare, rolul și domeniul de competență al acestor organisme sunt deja stabilite în mod expres de proiect. De asemenea, art. 24 reglementează exclusiv procedurile de verificare a identității aplicabile de către prestatorii de servicii de încredere calificați în procesul emiterii certificatelor calificate și al prestării serviciilor de încredere calificate. În acest context, cerința privind confirmarea conformității unor metode alternative de identificare de către un organism de evaluare a conformității urmărește asigurarea unui nivel ridicat și uniform de încredere pentru procesele de identificare utilizate de prestatorii de servicii de încredere calificați. Cerințele tehnice detaliate privind metodele de identificare admise, nivelurile de asigurare și procedurile de evaluare a conformității urmează să fie stabilite prin actele de punere în aplicare adoptate de Guvern. În acest context, prin hotărâre de Guvern urmează a fi transpus Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) din Regulamentul (UE) nr. 910/2014.
	20.6	III. Cu privire la sancțiuni Cu referire la art. 68 din Proiect, Asociația Băncilor din Moldova propune completarea cu un alineat nou (21) în următoarea redacție:	**Se acceptă.** Proiectul a fost modificat conform propunerilor recepționate în proces de avizare.

		„La stabilirea sancțiunii, organismul de supraveghere ține cont în special de: natura, gravitatea și durata încălcării; caracterul intenționat sau neglijent al faptei; măsurile întreprinse pentru limitarea prejudiciului; gradul de cooperare cu organismul de supraveghere; eventualele încălcări anterioare; impactul încălcării asupra beneficiarilor serviciilor de încredere; capacitatea economică a prestatorului.” Considerăm că regimul sancționator propus de Proiect este excesiv și disproporționat în raport cu specificul activităților reglementate, cu dimensiunea pieței serviciilor de încredere din Republica Moldova și cu principiile generale care guvernează răspunderea juridică. Stabilirea unei amenzi de până la 5 000 000 EUR sau până la 1% din cifra anuală de afaceri pentru orice încălcare a prevederilor legii, indiferent de natura și gravitatea acesteia, instituie un mecanism sancționator excesiv de sever. Un asemenea mecanism este susceptibil să producă consecințe economice ireversibile asupra prestatorilor de servicii de încredere, inclusiv insolvabilitatea sau excluderea acestora de pe piață, chiar și în cazul unor abateri formale sau lipsite de consecințe prejudiciabile semnificative. Principiul proporționalității impune ca sancțiunea aplicată să fie adecvată gravității faptei, necesară pentru atingerea scopului legitim urmărit și să nu depășească ceea ce este rezonabil necesar pentru protejarea interesului public. În lipsa unei diferențieri între încălcările minore și cele grave, textul Proiectului creează posibilitatea aplicării unor sancțiuni identice pentru fapte cu grade de pericol social fundamental diferite. Astfel, în actuala redactare, pot fi tratate în mod similar o eroare procedurală sau tehnică neintenționată, o întârziere formală de notificare, o neconformitate administrativă minoră, o breșă gravă de securitate, falsificarea intenționată a certificatelor ori compromiterea deliberată a serviciilor de încredere. O asemenea abordare este incompatibilă cu principiul individualizării răspunderii juridice și ignoră diferențele evidente dintre formele de vinovăție, gravitatea consecințelor și impactul concret al faptelor săvârșite.	

		Mai mult, Proiectul se îndepărtează de logica generală a sistemului sancționator național consacrat de Codul penal și Codul contravențional, care operează în mod constant cu individualizarea răspunderii în funcție de gravitatea faptei, intenția făptuitorului, prejudiciul și pericolul social. În legislația națională, inclusiv în domenii cu un grad ridicat de risc social sau economic, sancțiunile sunt individualizate în funcție de circumstanțele concrete ale cauzei și de conduita persoanei vizate. În consecință, considerăm necesară păstrarea unei abordări coerente și armonizate cu principiile deja consacrate în dreptul național, evitând instituirea unui regim sancționator autonom, excesiv și disproporționat în raport cu restul cadrului normativ. Redacția actuală nu conține criterii clare și obligatorii pe care autoritatea de supraveghere să le aplice la individualizarea sancțiunii. Lipsa unor asemenea criterii conferă autorității o marjă excesiv de largă de apreciere și creează premise reale pentru aplicarea arbitrară sau neuniformă a sancțiunilor. În forma actuală, legea nu obligă autoritatea să țină cont de elemente esențiale precum gravitatea și durata încălcării, existența intenției sau a simplei neglijențe, măsurile întreprinse pentru limitarea prejudiciului, gradul de cooperare al prestatorului, existența unor încălcări repetate, impactul efectiv asupra beneficiarilor serviciilor de încredere ori capacitatea economică a operatorului. În lipsa unor repere legale obiective, prestatorii nu pot anticipa în mod rezonabil consecințele juridice ale conduitei lor, ceea ce afectează principiul securității juridice și previzibilității normei. Totodată, potrivit jurisprudenței constante a Curții Europene a Drepturilor Omului, sancțiunile administrative care prezintă un grad ridicat de severitate pot fi asimilate sancțiunilor cu caracter „penal” în sensul autonom al art. 6 din Convenția Europeană a Drepturilor Omului. În consecință, aplicarea unor asemenea sancțiuni atrage incidența garanțiilor specifice materiei penale, inclusiv exigențe sporite privind legalitatea incriminării și a sancțiunii, claritatea și previzibilitatea normei, precum și proporționalitatea măsurii represive.	

		În jurisprudența sa constantă, Curtea Europeană a reținut că o normă care permite aplicarea unor sancțiuni severe trebuie formulată cu suficientă precizie și claritate pentru a exclude riscul arbitrariului și pentru a permite persoanei vizate să prevadă, într-o măsură rezonabilă, consecințele juridice ale conduitei sale. Exigența previzibilității este cu atât mai riguroasă atunci când norma conferă autorităților marje largi de apreciere în stabilirea și individualizarea sancțiunii, în lipsa unor criterii obiective și verificabile stabilite de lege. În același sens, art. 23 alin. (2) din Constituția Republicii Moldova consacră obligația statului de a adopta norme clare, accesibile și previzibile, astfel încât destinatarii legii să își poată adapta conduita în mod corespunzător. Curtea Constituțională a Republicii Moldova a reiterat în mod constant că previzibilitatea legii constituie o componentă esențială a principiului securității juridice, inclusiv prin Hotărârea nr. 22 din 19 decembrie 2023 și Hotărârea nr. 3 din 14 ianuarie 2021. Or, în lipsa unor criterii legale clare de individualizare a sancțiunii și a unei clasificări a încălcărilor în funcție de gravitatea lor, norma propusă riscă să permită aplicarea neuniformă și discreționară a sancțiunilor, ceea ce afectează exigențele de previzibilitate și securitate juridică. Mai mult, absența unor repere normative obiective poate conduce la tratamente diferențiate pentru situații comparabile, contrar principiului egalității în fața legii, și poate determina instituirea unor ingerințe disproporționate în drepturile persoanelor vizate. În aceste condiții, reglementarea propusă ridică probleme serioase de compatibilitate atât cu standardele dezvoltate în jurisprudența Curții Europene a Drepturilor Omului, cât și cu exigențele constituționale referitoare la calitatea legii și proporționalitatea restrângerii exercițiului drepturilor. Nu în ultimul rând, considerăm că un regim sancționator excesiv poate avea efecte negative asupra dezvoltării pieței serviciilor de încredere și asupra procesului de digitalizare. Instituirea unor sancțiuni disproporționat de mari poate descuraja intrarea pe piață a unor noi prestatori, poate reduce concurența și poate genera	

		costuri excesive de conformare, afectând inclusiv inovarea și dezvoltarea serviciilor digitale. În contextul unei piețe emergente precum cea a Republicii Moldova, cadrul normativ trebuie să asigure un echilibru rezonabil între necesitatea protejării securității și încrederii în serviciile digitale și necesitatea menținerii unui mediu regulatoriu predictibil, echitabil și sustenabil pentru operatori. Din aceste considerente, completarea art. 68 alin. (2) cu criterii clare de individualizare a sancțiunilor este necesară pentru asigurarea proporționalității, previzibilității și aplicării uniforme a regimului sancționator. O asemenea completare ar permite autorității de supraveghere să diferențieze între încălcările minore, remediabile, și încălcările grave, care afectează securitatea serviciilor de încredere sau drepturile beneficiarilor.	
Consiliul Concurenței (Nr. DJ-06/550-998 din 05 iunie 2026)	21.	Lipsa de obiecții și propuneri.	
Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător (Nr. 38-78-5449 din 13 mai 2026)	22.1.	Articolul 5, alin. (1) prevede că Agenția de Guvernare Electronică asigură disponibilitatea unui portofel pentru identitatea digitală, iar furnizorii privați pot pune la dispoziție asemenea portofele în condițiile legii. Problema este că norma poate crea un avantaj pentru furnizorul public, fără să prevadă expres tratament egal pentru furnizorii privați, acces nediscriminatoriu la infrastructură și reguli clare de interoperabilitate. Se recomandă completarea articolului cu prevederi care să stabilească expres că furnizorii publici și privați activează în condiții egale, transparente și nediscriminatorii. Alineatul (4) prevede că organismul de supraveghere poate decide ca anumite componente ale codului sursă să nu fie publicate, dacă publicarea ar putea afecta securitatea, integritatea sau funcționarea sistemului. Formulările generale, precum „cazuri justificate în mod corespunzător” și „ar putea afecta”, sunt problematice și oferă organismului de supraveghere o marjă prea largă de apreciere și poate duce la decizii discreționare.	**Se acceptă parțial.** În baza propunerilor recepționate în proces de avizare art. 5 alin. (1) din proiectul de lege a fost revizuit.
	22.2.	Procedura prevăzută la art. 22 are natura juridică a unui regim permisiv, chiar dacă proiectul folosește termenul de „notificare”.	**Se acceptă parțial.**

		Prestatorul nu poate începe activitatea doar prin simpla informare a organismului de supraveghere, ci numai după verificarea conformității, acordarea statutului de calificat și includerea în lista sigură. Prin urmare, procedura produce efecte similare unui act permisiv. În aceste condiții, proiectul trebuie corelat cu Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător, inclusiv sub aspectul normelor de procedură pentru emiterea actelor permisive. Este necesar ca legea să stabilească expres termenul de examinare, lista exhaustivă a documentelor, temeiurile de refuz, efectele depășirii termenului, procedura de contestare și, după caz, aplicabilitatea aprobării tacite.	În baza propunerilor recepționate în pro-ces de avizare art. 22 din proiectul de lege a fost revizuit.
	22.3.	Art. 24 conține mai multe formulări generale și obligații care pot genera incertitudine pentru prestatori și marjă largă de apreciere pentru organismul de supraveghere. Utilizarea unor noțiuni precum „mijloace adecvate”, „nivel ridicat de încredere”, „măsuri corespunzătoare”, „sisteme demne de încredere” sau „impact semnificativ” nu oferă suficientă claritate privind standardele concrete pe care trebuie să le respecte prestatorii. În lipsa unor criterii obiective sau a unor limite clare, aceleași obligații pot fi interpretate și aplicate diferit de la un caz la altul. Multe obligații esențiale sunt lăsate la nivelul Guvernului, inclusiv metodele de verificare a identității și atributelor. Această abordare reduce previzibilitatea reglementării și face dificilă estimarea costurilor și cerințelor de conformare pentru operatorii economici. La fel, aici se acordă organismului de supraveghere competențe foarte largi de intervenție, inclusiv posibilitatea de a solicita informații suplimentare și de a stabili condiții pentru implementarea modificărilor serviciilor. În lipsa unei liste exhaustive a documentelor și informațiilor care pot fi solicitate, autoritatea poate extinde de la caz la caz cerințele procedurale, ceea ce este problematic din perspectiva principiilor aplicabile actelor permisive și a previzibilității pentru întreprinzători.	**Se acceptă parțial.** În baza propunerilor recepționate în pro-ces de avizare art. 24 din proiectul de lege a fost revizuit.
	22.4.	Ce ține de capitolul V proiectul concentrează în sarcina Serviciului de Informații și Securitate funcții de supraveghere și control, inclusiv și de autorizare - acordarea statutului de prestator de servicii de încredere calificat, verificarea conformității, includerea	**Se acceptă parțial.** În baza propunerilor recepționate în pro-ces de avizare capitolul V din proiectul de lege a fost revizuit.

		în lista sigură, supravegherea, controlul, solicitarea de informații, impunerea măsurilor de remediere, suspendarea sau retragerea statutului. Această concentrare creează un risc de conflict instituțional de interese, deoarece aceeași autoritate admite operatorul pe piață, îl controlează ulterior și poate decide suspendarea sau încetarea activității acestuia. Această soluție nu este suficient corelată cu principiul delimitării funcțiilor de reglementare, control și inspecție de stat de funcțiile de prestare a serviciilor de evaluare a conformității și altor servicii (eliberare acte permisive), consacrat de Legea nr. 424/2004. Chiar dacă evaluarea conformității este efectuată formal de organisme acreditate, SIS păstrează un rol determinant în verificare, acordarea permisiunii, stabilirea condițiilor și retragerea statutului, ceea ce poate afecta imparțialitatea și previzibilitatea procedurii. La fel, un moment important este că SIS nu este indicat expres în Legea nr. 131/2012 ca organ de control pentru acest domeniu, deși proiectul îi atribuie competențe tipice de control asupra activității de întreprinzător. În lipsa includerii în cadrul general al controlului de stat sau a unei derogări exprese și justificate, apare incertitudine privind aplicarea garanțiilor procedurale prevăzute pentru persoanele supuse controlului. Se recomandă revizuirea arhitecturii instituționale prin separarea clară a funcțiilor de autorizare conform Legii nr.160/2011, supraveghere/control și evaluare a conformității, precum și corelarea proiectului cu Legea nr. 131/2012. Dacă SIS urmează să exercite atribuții de control, statutul său trebuie reglementat expres, cu limite clare, proceduri transparente, garanții de contestare și mecanisme de prevenire a conflictului de interese instituțional.	
	22.5.	Articolul 68 prevede amenzi foarte mari: până la echivalentul în lei al sumei de 5 000 000 euro pentru persoanele fizice și, pentru persoanele juridice, până la 5 000 000 euro sau până la 1% din cifra de afaceri anuală totală la nivel mondial, aplicându-se valoarea cea mai mare. Problema principală este că articolul nu clarifică natura juridică a acestei răspunderi. Nu este clar dacă amenzile reprezintă sancțiuni contravenționale, penale sau un regim administrativ sancționator paralel. În lipsa acestei precizări, apar	**Se acceptă.** Proiectul a fost completat cu prevederi noi ținând cont de propunerile formulate, iar cuantumul maxim al amenzilor propuse au fost semnificativ reduse.

		incertitudini privind procedura de constatare, drepturile persoanei sancționate, termenul de prescripție, executarea sancțiunii și raportul cu Codul contravențional sau Codul penal. De asemenea, articolul nu stabilește criterii clare pentru calcularea amenzii. Nu este indicat cum se va ține cont de gravitatea încălcării, durata acesteia, prejudiciul produs, vinovăția, recidiva, cooperarea prestatorului sau măsurile de remediere luate. În aceste condiții, organismul de supraveghere primește o marjă foarte largă de apreciere, ceea ce poate duce la aplicarea neuniformă sau disproporționată a sancțiunilor.	
	22.6.	Secțiunea 2.2 din notă explică în mare parte că legislația națională trebuie ajustată la noile prevederi europene privind identificarea electronică și serviciile de încredere. Această justificare este relevantă, dar nu este suficientă pentru o analiză AIR. Autorii nu trebuie să se limiteze la ideea că „legislația europeană s-a schimbat", ci trebuie să arate concret ce probleme există în Republica Moldova și cum acestea afectează cetățenii, autoritățile publice și mediul de afaceri. Problema este formulată prea general. Se menționează că Legea nr. 124/2022 nu mai reflectă evoluțiile acquisului UE, însă nu se explică ce disfuncționalități concrete produce cadrul legal actual. Nu este clar dacă problema constă în lipsa portofelului digital, lipsa regulilor pentru atestatele electronice ale atributelor, lipsa mecanismelor de recunoaștere transfrontalieră, lipsa interoperabilității, lipsa procedurilor de certificare sau în capacitatea redusă a instituțiilor de a implementa noile cerințe. La fel, lipsesc informații despre numărul utilizatorilor actuali ai semnăturii electronice, numărul prestatorilor de servicii de încredere, numărul serviciilor publice integrate cu mecanisme de identificare electronică, volumul tranzacțiilor electronice, costurile administrative actuale sau problemele întâlnite în practică. De asemenea, nu sunt identificate suficient părțile interesate. Se prevede la general despre cetățeni, mediul de afaceri și autorități publice, dar nu analizează separat instituțiile publice, prestatorii de servicii de încredere, băncile, companiile de asigurări, furnizorii de utilități, platformele de comerț electronic, companiile IT,	**Se acceptă.** În baza propunerilor recepționate în pro-ces de avizare Secțiunea 2.2 din nota de fundamentare a fost revizuită.

		IMM-urile, persoanele fără competențe digitale, etc. Pentru fiecare categorie ar trebui indicat cum este afectată de problema de azi. Cauzele problemei sunt prezentate insuficient. Modificarea legislației europene nu este, în sine, singura cauză. Autorii trebuie să explice ce lipsește în sistemul național actual: reguli pentru portofelul digital, standarde de interoperabilitate, mecanisme de certificare, proceduri pentru beneficiarii privați, reguli privind utilizarea atributelor electronice, capacitate instituțională, infrastructură tehnică sau garanții pentru protecția datelor. De asemenea, secțiunea nu analizează nivelul de pregătire al instituțiilor și al sectorului privat. Pentru un proiect cu relevanță UE, HG nr. 574/2024 cere examinarea situației naționale și a gradului de pregătire pentru aplicarea cerințelor europene. Nota trebuie să arate dacă autoritățile, prestatorii, beneficiarii privați și infrastructura tehnică sunt pregătite pentru certificare, interoperabilitate, audit, protecția datelor și securitate cibernetică.	
	22.7.	Secțiunea 3 necesită a fi ajustată cerințelor Metodologiei AIR deoarece este prea generală și nu explică suficient legătura dintre problemele identificate, obiectivele urmărite și soluțiile concrete din proiect. Obiectivul general este formulat prea general, precum modernizarea, armonizarea cu acquis-ul UE, interoperabilitatea și crearea cadrului pentru portofelul digital. Aceste formulări nu arată suficient ce schimbare concretă se urmărește în Republica Moldova. Secțiunea nu stabilește obiective clare, măsurabile și verificabile (SMART). Principalele prevederi ale proiectului sunt enumerate, dar nu sunt explicate suficient. Se menționează portofelul digital, atestările electronice ale atributelor, arhivarea electronică, registrele electronice și gestionarea semnăturilor la distanță, însă nu se arată clar ce problemă rezolvă fiecare dintre aceste instrumente. Nota trebuie să explice mai simplu și mai concret de ce fiecare soluție este necesară și ce efect practic va avea pentru cetățeni, autorități și mediul de afaceri. Autorii trebuie să reflecte mai clar prevederile esențiale ale proiectului. De exemplu, proiectul prevede că AGE va asigura disponibilitatea unui portofel pentru identitatea digitală, iar furnizorii privați vor putea pune la dispoziție portofele digitale „în condițiile legii”.	**Se acceptă.** În baza propunerilor recepționate în pro-ces de avizare Secțiunea 3 din nota de fundamentare a fost revizuită.

		Această soluție trebuie explicată în nota de fundamentare: de ce a fost ales acest model mixt, ce rol are furnizorul public, ce spațiu real rămâne pentru furnizorii privați și ce garanții există pentru concurență loială. Un neajuns important este lipsa separării între obligațiile impuse de legislația UE și soluțiile alese la nivel național. Autorii trebuie să indice ce prevederi sunt transpuse direct din eIDAS/eIDAS 2.0 și ce prevederi reprezintă opțiuni naționale. De exemplu, desemnarea AGE, utilizarea EVO, modelul de supraveghere, regimul de certificare și gratuitatea pentru persoanele fizice trebuie explicate distinct, mai ales dacă presupun costuri sau efecte asupra pieței. Secțiunea 3.2 privind opțiunile alternative este insuficientă. Sunt analizate doar menținerea cadrului actual, modificarea Legii nr. 124/2022 și adoptarea unei legi noi. Autorii trebuie să analizeze și alternative reale de implementare. De exemplu, implementarea etapizată a portofelului digital, pilotarea inițială doar pentru anumite servicii publice, perioade tranzitorii pentru sectorul privat, aplicarea graduală a obligațiilor pentru IMM-uri, conectarea treptată prin EVO sau opțiuni diferite privind certificarea furnizorilor privați. Aceste alternative sunt importante pentru a demonstra că soluția aleasă este proporțională.	
	22.8.	Secțiunea 4.3 privind impactul asupra sectorului privat este insuficient dezvoltată și prezintă aproape exclusiv efectele pozitive ale proiectului, fără o analiză reală a costurilor, obligațiilor și riscurilor pentru companii, așa cum cere HG nr. 574/2024. Se afirmă că proiectul va crea un cadru modern și previzibil pentru utilizarea identității digitale și a serviciilor de încredere, însă aceste beneficii nu sunt „probate„ prin date sau estimări concrete. Nu se indică numărul aproximativ al entităților afectate, domeniile economice vizate și amploarea obligațiilor noi pentru sectorul privat. Secțiunea trebuie să conțină o analiză a costurilor de conformare. Proiectul prevede obligații concrete: înregistrarea prin Portalul EVO, implementarea mecanismelor de autentificare și validare, respectarea principiului minimizării datelor, implementarea măsurilor tehnice și organizatorice de securitate și conformarea la	**Se acceptă.** **În baza propunerilor recepționate în pro-ces de avizare Secțiunea 4.3 din nota de fundamentare a fost revizuită.**

		cerințele privind protecția datelor. Toate aceste obligații generează costuri pentru sectorul privat, însă nota nu estimează impactul financiar al acestora. De asemenea, nu sunt analizate costurile pentru prestatorii de servicii de încredere. Proiectul stabilește obligații de audit periodic, certificare, evaluări de conformitate și eventuale audituri suplimentare dispuse de organismul de supraveghere. La fel trebuie evidențiate costurile generate de actele permisive prevăzute de proiect. Proiectul instituie proceduri precum certificarea portofelelor pentru identitatea digitală, certificarea sistemelor de identificare electronică, notificarea sau înregistrarea beneficiarilor, acordarea statutului de prestator de servicii de încredere calificat și includerea în listele oficiale. Aceste proceduri reprezintă acte permisive sau mecanisme administrative obligatorii pentru accesul pe piață ori pentru prestarea anumitor servicii. Și nu în ultimul rând, alici nu se analizează deloc impactul asupra concurenței, deși proiectul conține prevederi care pot influența direct piața serviciilor de identificare electronică și a serviciilor de încredere. În special, proiectul prevede că AGE va asigura disponibilitatea unui portofel pentru identitatea digitală, în timp ce furnizorii privați vor putea furniza astfel de portofele „în condițiile legii„. Această soluție poate crea un avantaj concurențial pentru furnizorul public, prin acces la infrastructura statului, integrare cu registrele publice și finanțare bugetară.	
	22.9.	În Secțiunea 6 se limitează la menționarea publicării anunțului pe pagina MDED și pe platforma particip.gov.md, precum și la indicarea faptului că proiectul urmează a fi transmis spre avizare și consultare. Aceasta nu este suficient pentru a demonstra respectarea cerințelor HG nr. 574/2024 privind consultarea efectivă a părților interesate. Autorii trebuie să identifice concret actorii afectați de proiect și consultați în procesul de elaborare. HG nr. 574/2024 impune nu doar publicarea proiectului, ci și reflectarea opiniilor primite și modul în care acestea au fost analizate. Nota trebuie să indice ce observații sau obiecții au fost formulate, care dintre acestea au fost acceptate sau respinse și din ce motive. Un	**Se acceptă.** Proiectul a fost consultat și avizat de către toți subiecții interesați, inclusiv autorități publice, prestatori de servicii de încredere, organizații neguvernamentale și alte părți relevante.

		aspect important care lipsește este consultarea mediului de afaceri în legătură cu impactul economic și concurențial al proiectului. Proiectul introduce obligații pentru furnizorii privați, proceduri de certificare și mecanisme de înregistrare și interoperabilitate care pot genera costuri semnificative și pot afecta accesul pe piață. Nu este clar dacă proiectul a fost discutat cu prestatorii existenți de servicii de încredere sau cu potențialii furnizori de portofele digitale private, deși proiectul poate influența direct concurența pe această piață. De asemenea, nu este clar dacă au fost consultate autoritățile responsabile de protecția datelor și securitatea cibernetică asupra mecanismelor propuse privind portofelul digital și interoperabilitatea.	
Expertizare/Informare			
Agenția Servicii Publice (Nr. 01/5784 din 22.06.2026)	1.	Lipsa de obiecții și propuneri.	
Ministerul Educației și Cercetării Legiferare	2.	Lipsa de obiecții și propuneri.	
Ministerul Culturii Legiferare	4.	Lipsa de obiecții și propuneri.	
Ministerul Afacerilor Interne Legiferare	5.	Lipsa de obiecții și propuneri.	
Centrul de Armonizare a Legislației Legiferare	6.	Lipsa de obiecții și propuneri.	
Ministerul Mediului Legiferare	7.	Lipsa de obiecții și propuneri.	
Ministerul Energiei Legiferare	8.	Lipsa de obiecții și propuneri.	
	9.1	La alin. (1) al art. 5, anterior sintagmei „unui portofel” se va completa cu articolul „al”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” (Nr. 1.4/1139/26 din 19.06.2026)	9.2	La alin. (3) al art. 7, sintagma „se certifică” se va substitui cu sintagma „poate să fie certificată”, conform prevederilor art. 5c alin. (5) din 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.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.3	Preluând formularea autorului referitor la recunoașterea serviciilor de încredere calificate furnizate de prestatori de servicii calificate din state UE, stabilită în art. 22 alin. (6)-(7) din proiect, precum și pentru asigurarea recunoașterii portofelelor europene, se propune uniformizarea practicilor și asupra portofelelor pentru identitatea digitală calificată, completând art. 8 din proiect cu alineate noi cu următorul conținut: „(6) Portofelele europene pentru identitatea digitală certificate din Statele membre ale Uniunii Europene păstrează statutul de certificate pe teritoriul Republicii Moldova, fără necesitatea desfășurării notificării și procedurilor de verificare. (7) În scopul informării utilizatorilor și al facilitării verificării Portofelului european pentru identitatea digitală certificat, organismul de supraveghere preia informațiile relevante din lista a portofelelor europene pentru identitatea digitală certificată și le publică pe pagina sa oficială, asigurând actualizarea acestora în funcție de modificările operate în lista respective.”.	**Se acceptă.** Proiectul a fost completat conform propunerii.
	9.4	La alin. (2) al art. 16, sintagma „de cinci ani” urmează a fi substituită cu sintagma „de până la cinci ani”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.5	La alin. (1) al art. 17, sintagma „ce a suferit” se a substitui cu sintagma „care a suferit”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.6	Alin. (4) al art. 22 transpune eronat prevederile Regulamentului nr. 910/2014, or termenele și procedura enunțată se referă la supraveghere în contextul respectării cerințelor Directiva (UE) 2022/2555, și nu este realizată de organul de supraveghere. Astfel, se propune excludere sau reformularea acestei prevederi, uniformizării conform accepțiunii din actul transpus. În contextul aceleiași obiecții, se va revedea și alin. (5) al art. 24.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

	9.7	În tot contextul proiectului se propune revizuirea textului „lista sigură” or acesta reprezintă traducerea eronată a textului din Regulamentul transpus, care este expusă în actul original ca „lista de încredere” (trust list).	**Nu se acceptă.** Sintagma „lista sigură” se menține în textul proiectului, întrucât aceasta corespunde terminologiei oficiale utilizate în versiunea în limba română a actelor și resurselor Uniunii Europene aferente Regulamentului eIDAS, unde noțiunea trust list este tradusă ca „listă sigură”. Totodată, aceeași terminologie este utilizată și în legislația României, respectiv în Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea. În vederea asigurării unei transpuneri consecvente a acquis-ului Uniunii Europene și a uniformității terminologice cu actele normative naționale ale statelor membre, se consideră oportună menținerea sintagmei „lista sigură”.
	9.8	La alin. (2) al art. 39, cuvântul „actele” se va indica fără cratimă.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.9	La alin. (2) al art. 56, sintagma „organismul public” se va substitui cu „organismul din sectorul public”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.10	La alin. (6) al art. 63, după sintagma „documentul electronic” se va completa cu textul „semnat cu semnătură electronică calificată sau care are aplicat un sigiliu electronic calificat”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.11	La alin. (2) lit. d) a art. 64, sintagma „sunt informate” se va substitui cu sintagma „este informat”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	9.12	Cap. VI din proiect urmează a fi exclus și introdus în actele normative speciale care reglementează răspunderea civilă (fie codul Civil fie Contravențional). De menționat, nici cadrul UE transpus nu include așa prevederi, ci doar suma despăgubirilor. Subsecvent, potrivit art. 55 alin. (1) din Legea nr. 100/2017 privind actele normative, Reglementările de același nivel și având același obiect de reglementare se cuprind, de regulă, într-un singur act normativ.	**Nu se acceptă.** Capitolul VI reglementează mecanismele naționale necesare pentru aplicarea efectivă a dispozițiilor Regulamentului (UE) eIDAS. Deși regulamentul stabilește doar principiile și cerințele minime privind sancțiunile, acesta obligă statele să adopte cadrul normativ necesar pentru aplicarea lor. În acest sens, art. 16

			alin. (1) din regulament prevede expres că statele stabilesc normele privind sancțiunile aplicabile în cazul încălcării regulamentului, iar alin. (3) recunoaște competența acestora de a reglementa, potrivit propriului sistem juridic, mecanismele procedurale de constatare și aplicare a sancțiunilor. În consecință, proiectul de lege nu se limitează la preluarea cuantumului amenzilor, ci instituie cadrul procedural și instituțional necesar exercitării atribuțiilor organismului de supraveghere, inclusiv procedura de examinare a plângerilor, investigare, emitere a deciziilor, aplicare a măsurilor corective și a sancțiunilor, precum și regulile speciale privind răspunderea și dreptul la despăgubiri în domeniul identificării electronice și al serviciilor de încredere. Excluderea acestor dispoziții și dispersarea lor în alte acte normative ar afecta coerența și aplicabilitatea cadrului normativ de transpunere. Această abordare este conformă și practicii legislative naționale. Un exemplu relevant îl constituie Legea nr. 195/2024 privind protecția datelor cu caracter personal, prin care au fost transpuse dispozițiile Regulamentului (UE) 2016/679 (GDPR), lege ce cuprinde, în mod similar, norme privind competențele autorității naționale competente, procedurile de investigare, răspunderea, dreptul la despăgubiri și aplicarea sancțiunilor.
Serviciul de Informații și Securitate (Nr. IE/6428 din 29.06.2026)	10.1	În proiectul de lege, la art. 5 alin. (25) se menționează că ,,Guvernul stabilește o listă de standarde de referință”, însă conform prevederilor Programului Național de Aderare al Republicii Moldova la Uniunea Europeană (2025-2029), atribuția enunțată supra	**Nu se acceptă.** Atribuirea competenței de aprobare a actelor normative organismului de supraveghere nu este oportună, deoarece ar conduce la cumula-

		intră în competența organismului de supraveghere. Astfel, Serviciul este instituția responsabilă de implementarea politicilor în domeniul serviciilor de încredere, având și obligația de transpunere a actelor Uniunii Europene în domeniul respectiv. Aceeași obiecție se referă și la prevederile art. 7 alin. (1) și alin. (4), art. 15 alin. (2), art. 21 alin. (9), art. 24 alin. (2) și (3), art. 27 alin. (2), art. 28 alin. (4), art. 29 alin. (7), art. 31 alin. (5), art. 33 alin. (2) lit. a), art. 34 alin. (4), art. 35 alin. (2), art. 36 alin. (2), art. 38 alin. (2), art. 39 alin. (4), art. 40 alin. (7), art. 47 alin. (2), art. 49 alin. (4), art. 50 alin. (5), art. 54 alin. (5), art. 56 alin. (4) și alin. (5), art. 60 alin. (3), art. 62 alin. (2) din proiectul de lege, unde considerăm necesar de a înlocui cuvântul „Guvernul” cu cuvintele „Organismul de supraveghere”.	rea funcției de reglementare cu funcția de supraveghere și control. O asemenea concentrare a competențelor creează un risc de conflict instituțional de interese, întrucât aceeași autoritate ar stabili regulile aplicabile, ar admite operatorii pe piață, ar supraveghea respectarea propriilor reglementări și ar putea dispune măsuri restrictive, inclusiv suspendarea sau încetarea activității acestora. Menținerea unei separări instituționale între funcția de reglementare și funcția de supraveghere reprezintă o garanție a obiectivității, imparțialității, predictibilității și bunei administrări. Totodată, actele la care fac trimitere dispozițiile proiectului au caracter normativ și general, fiind destinate unui cerc nedeterminat de destinatari și stabilind reguli obligatorii de aplicare în domeniul identificării electronice și al serviciilor de încredere. Prin natura lor, asemenea acte țin de competența Guvernului, în calitate de autoritate care organizează executarea legilor și asigură implementarea unitară a politicilor publice. Astfel, Ministerul Dezvoltării Economice și Digitalizării urmează să fie desemnată în calitate de autoritate a administrației publice centrale de specialitate responsabilă de elaborarea și promovarea politicii de stat în domeniul identificării electronice și serviciilor de încredere și va fi responsabilă de elaborarea proiectele actelor normative necesare implementării prezentei legi și le va promova spre aprobare Guvernului. În acest mod este asigurată delimitarea clară dintre funcția de elaborare a politicilor și reglementărilor și funcția de supraveghere a respectării acestora.

			De asemenea, aprobarea actelor normative de către Guvern asigură o abordare unitară la nivelul întregii administrații publice, inclusiv coordonarea interinstituțională, consultarea autorităților și evaluarea impactului asupra altor domenii conexe, aspecte care nu pot fi realizate prin acte emise de organismul de supraveghere. Astfel, soluția propusă în proiect corespunde principiilor organizării administrației publice, tehnicii legislative și bunei guvernări, asigurând un echilibru între funcția de reglementare și cea de supraveghere și evitând concentrarea excesivă a competențelor în cadrul aceleiași autorități.
	10.2	La art. 8 a proiectului de lege se vor exclude normele de la alin. (2) și (3), deoarece acestea reprezintă o transpunere eronată a prevederilor art. 5d din Regulamentul UE 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. În acest sens, reglementările actului european obligă statele membre să ofere informații Comisiei Europene, iar în cazul normelor naționale enunțate la art. 8 alin. (2) a proiectului de lege, acestea reprezintă o informație care nu are caracter public. Totodată, în partea ce se referă la prevederile menționate la art. 8 alin. (3) „Orice parte interesată poate transmite organismului o cerere de eliminare de pe lista menționată la alin. (1)...”, accentuăm faptul că excluderea din listă nu poate fi efectuată de o parte interesată, ci doar de entitatea deținătoare a portofelelor pentru identitatea digitală certificată, sau de organismul de supraveghere. Subsecvent, prin prisma celor relatate supra, alin. (5) al art. 8 din proiectul de lege, se va modifica corespunzător reieșind din excluderea alin. (2) și (3).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	10.3	Totodată, Serviciul propune excluderea art. 13 din proiectul de lege, din considerentul că acesta reprezintă o transpunere eronată	**Nu se acceptă.**

		a prevederilor art. 9 din Regulamentul UE 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 abordare a Directivei 1999/93/CE (în continuare – Regulamentul EU 910/2024). În acest sens, prevederile din actul european obligă statele membre să notifice Comisia Europeană privind mijloacele de identificare electronică naționale. Astfel, Serviciul consideră irelevantă menținerea prevederilor de la art. 13 din proiectul de lege, în contextul în care prestatorii de servicii de încredere oferă informații aferente mijlocului de identificare utilizat și nivelului de asigurare a încrederii în procesul de obținere a statutului de prestator de servicii de încredere calificat.	Art. 13 transpune, adaptat la contextul instituțional al Republicii Moldova, mecanismul prevăzut la art. 9 din Regulamentul (UE) nr. 910/2014 privind notificarea sistemelor de identificare electronică. Întrucât Republica Moldova nu este stat membru al Uniunii Europene și nu poate notifica sistemele naționale Comisiei Europene, funcțiile prevăzute de regulament au fost adaptate prin atribuirea acestora organismului național de supraveghere, care ține evidența sistemelor de identificare electronică și publică lista acestora. Obiectul de reglementare al art. 13 nu se confundă cu procedura de calificare a prestatorilor de servicii de încredere. Notificarea sistemelor de identificare electronică și publicarea listei acestora urmăresc evidența oficială a sistemelor naționale de identificare electronică, verificarea îndeplinirii condițiilor privind nivelurile de asigurare și transparența informațiilor referitoare la sistemele utilizate în sectorul public. În schimb, procedura de calificare a prestatorilor de servicii de încredere vizează un alt obiect de reglementare și alte categorii de subiecți, respectiv prestatorii de servicii de încredere, neputând substitui mecanismul de notificare a sistemelor de identificare electronică. Menținerea art. 13 este necesară pentru instituirea unui mecanism național echivalent celui prevăzut de art. 9 din Regulamentul (UE) nr. 910/2014, pentru asigurarea unei evidențe oficiale a sistemelor de identificare electronică, a transparenței acestora și a compatibilității cadrului normativ național cu arhitectura eI-

			DAS. Totodată, această reglementare facilitează recunoașterea și interoperabilitatea viitoare a sistemelor naționale în contextul procesului de integrare europeană și al eventualei participări a Republicii Moldova la mecanismele europene prevăzute de regulament.
	10.4	Concomitent, întru armonizarea legislației naționale cu legislația europeană, și anume, transpunerea prevederilor de la art. 19a din Regulamentul UE 910/2024, Serviciul propune completarea art. 20 a proiectului de lege cu punctul 3), cu următorul conținut „Organismul de supraveghere stabilește o listă de standarde de referință și dacă este necesar specificații și proceduri. În cazul în care standardele și procedurile respective sunt respectate se prezumă că sunt respectate cerințele prevăzute la prezentul articol.”	**Se acceptă parțial.** Având în vedere argumentele prezentate la pct. 21.1 din prezenta sinteză, competențele de aprobare a listei de standarde de referință și dacă este necesar a specificațiilor și procedurilor urmează a fi atribuite Guvernului.
	10.5	Totodată, urmare a analizei prevederilor europene menționate la art. 30 alin. (4) din Regulamentul UE 910/2024, Serviciul propune modificarea conținutului art. 33 alin. (4) a proiectului de lege și expunerea acestuia în următoarea redacție „Organismul de supraveghere stabilește criterii specifice ce urmează a fi îndeplinite de către organismele de evaluare a conformității.”.	**Se acceptă parțial.** Având în vedere argumentele prezentate la pct. 21.1 din prezenta sinteză, competențele de aprobare a criterii specifice ce urmează a fi îndeplinite de către organismele de evaluare a conformității urmează a fi atribuite Guvernului.
	10.6	Subsidiar, pentru evitarea unor lacune legislative și instituirea unor mecanisme clare în domeniul serviciilor de încredere, care asigură transpunerea integrală a legislației Uniunii Europene, în conformitate cu reglementările art. 45e alin. (2) al Regulamentului UE 910/2024, Serviciul propune completarea art. 55 cu un nou aliniat, și anume, alin. (4) care va avea următorul conținut „Organismul de supraveghere stabilește o listă de standarde de referință și dacă este necesar specificații și proceduri pentru catalogul de atribuire, precum și sisteme pentru atestarea atributelor și procedurile de verificare pentru atestatele electronice calificate.”.	**Se acceptă parțial.** Având în vedere argumentele prezentate la pct. 21.1 din prezenta sinteză, competențele de aprobare a listă de standarde de referință și dacă este necesar specificații și proceduri pentru catalogul de atribuire, precum și sisteme pentru atestarea atributelor și procedurile de verificare pentru atestatele electronice calificate urmează a fi atribuite Guvernului.
	10.7	Suplimentar, considerăm imperativă modificarea art. 61 alin. (1) din proiectul de lege, și anume excluderea Serviciului de Informații și Securitate al Republicii Moldova ca organism cu atribuții	**Se acceptă parțial.** Prevederea de la art. 64 alin. (1) a fost modificată, stabilindu-se că Guvernul va desemna

		în domeniul supravegherii serviciilor de încredere. Totodată, Serviciul propune desemnarea în calitate de organism cu atribuții de supraveghere a Agenției Naționale pentru Reglementare în Comunicații (ARCOM). Subsecvent, considerăm Agenția pentru Reglementare în Comunicații (ARCOM) reprezintă autoritate eligibilă pentru exercitarea funcției de supraveghere a domeniului serviciilor de încredere, având statut de autoritate administrativă autonomă de reglementare și supraveghere și competențe în administrarea unor componente esențiale ale infrastructurii digitale naționale dintre care putem marca: - elaborarea reglementărilor în domeniul comunicațiilor electronice și poștale; - autorizarea furnizorilor de rețele și servicii de comunicații electronice și aprobarea condițiilor generale de licență; - gestionarea spectrului de frecvență radio cu destinație neguvernamentală; - aprobarea Planului național de numerotație și gestionarea resurselor de numerotație; - reglementarea utilizării domeniului național de nivel superior „.md. Totodată, o practică des întâlnită în statele europene este desemnarea autorității de reglementare a domeniului comunicațiilor electronice în calitate de autoritate responsabilă de domeniul serviciilor de încredere, de exemplu: Germania, Finlanda, Grecia, Lituania, Bulgaria, Austria, Luxemburg, Malta, Țările de Jos, Suedia și Ungaria. În acest context, considerăm că atribuțiile specifice organismului de supraveghere prevăzute în proiectul de lege au caracter predominant administrativ, tehnic și reglementare a pieței, fiind compatibile cu mandatul și competențele instituționale ale Agenției Naționale pentru Reglementare în Comunicații. Subsidiar, desemnarea unui serviciu de informații în calitate de organism de supraveghere poate genera riscuri de percepție instituțională, inclusiv în raport cu prestatori de servicii de încredere, investitori străini, parteneri europeni și utilizatori finali ai portofelului pentru identitatea digitală. Aceste riscuri nu țin neapărat	organismul responsabil de supravegherea cadrului pentru portofelul pentru identitatea digitală și a serviciilor de încredere. În acest sens, Guvernul urmează să efectueze o evaluare și să identifice entitatea care va fi desemnată, aceasta urmând să preia, odată cu intrarea în vigoare a legii, responsabilitățile de supraveghere exercitate în prezent de SIS.

		de existența unei incompatibilități juridice exprese, ci de necesitatea asigurării unui nivel înalt de transparență, predictibilitate, neutralitate instituțională și încredere în mecanismele de supraveghere a pieței. În special, implicarea unei instituții cu atribuții de securitate națională în proceduri precum avizarea, supravegherea, auditarea indirectă, acordarea sau retragerea statului calificat al prestatorilor poate fi percepută de operatorii economici drept un factor de incertitudine.	
	10.8	Serviciul consideră esențială și modificarea prevederilor de la art. 79 alin. (1) a proiectului de lege, în partea ce vizează suma maximă a amenzii ce poate fi aplicată, reieșind din prejudiciul cauzat la încălcarea obligațiilor de către un prestator de servicii de încredere, precum și în scop de descurajare la realizarea unor acțiuni cu repercusiuni grave în domeniul serviciilor de încredere și identificare electronică. În acest sens propunem stabilirea unei penalități de până la 5 mln. MDL sau 1% din cifra de afaceri.	**Nu se acceptă.** Nivelul amenzilor stabilit la art. 79 a fost determinat în baza principiului proporționalității sancțiunilor, ținând cont de natura obligațiilor încălcate, gravitatea potențială a faptelor, impactul asupra utilizatorilor, precum și de realitățile economice și dimensiunea pieței serviciilor de încredere și a serviciilor de identificare electronică din Republica Moldova. Majorarea plafonului sancțiunilor până la 5 milioane lei sau 1% din cifra de afaceri ar putea conduce la aplicarea unor penalități disproporționate în raport cu capacitatea economică reală a operatorilor pe această piață, care este una în dezvoltare și în care este de facto un singur prestator activ, și anume STISC. Un asemenea nivel al sancțiunilor poate avea un efect contrar celui urmărit, prin creșterea barierelor de intrare pe piață, reducerea interesului operatorilor economici de a presta astfel de servicii și, implicit, limitarea concurenței și a accesului utilizatorilor la servicii digitale sigure și accesibile. Totodată, cadrul sancționator propus diferențiază încălcările în funcție de gravitatea acestora, stabilind sancțiuni mai ridicate pentru faptele care pot genera riscuri semnificative

			pentru securitatea serviciilor, integritatea datelor și încrederea utilizatorilor. Astfel, pentru încălcările de natură tehnică și operațională cu impact major, art. 79 alin. (2) prevede deja un plafon superior al amenzilor, de până la 2 000 000 lei sau 0,75% din cifra totală de afaceri, luându-se în calcul valoarea cea mai mare. De asemenea, stabilirea unor sancțiuni excesiv de ridicate trebuie analizată în contextul particular al economiei Republicii Moldova, al dimensiunii întreprinderilor care activează în domeniu și al necesității de a asigura un echilibru între caracterul disuasiv al sancțiunii și menținerea unui mediu favorabil dezvoltării serviciilor digitale. Scopul regimului sancționator nu este de a afecta viabilitatea economică a prestatorilor, ci de a asigura respectarea obligațiilor legale, protejarea utilizatorilor și consolidarea nivelului de încredere în serviciile de identificare electronică și serviciile de încredere. Prin urmare, cuantumul amenzilor prevăzut la art. 79 reprezintă un echilibru adecvat între necesitatea prevenirii și sancționării încălcărilor grave și condițiile reale ale pieței naționale, fiind suficient pentru a asigura efectul preventiv și descurajator al sancțiunilor.
Ministerul Justiției (Nr. 04/2-6974 din 22.06.2026)	11.1	Aferent redacției proiectului de lege, se constată că o parte dintre obiecțiile și recomandările Ministerului Justiției, expuse prin scrisoarea nr. 04/2-5098 din 11 mai 2026, au fost luate în considerare la definitivarea acestuia. Totodată, unele obiecții indicate în sinteză ca fiind acceptate nu au fost implementate sau au fost preluate defectuos. De asemenea, proiectul a fost completat cu norme noi, inclusiv prin introducerea capitolului VI „Răspunderea juridică, procedura de constatare și sancțiunile”, ale cărui prevederi necesită o revizuire suplimentară.	**Se ia act.**

	11.2	La art. 3, se reiterează obiecția privind expunerea noțiunilor în ordine alfabetică. În redacția actuală, ordinea nu este respectată integral, inclusiv în cazul noțiunilor referitoare la atestatele electronice ale atributelor și la organismele din sectorul public.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.3	La art. 5: La alin. (1), cuvintele „Guvernul va asigura” se vor substitui cu cuvintele „Guvernul asigură”, în scopul expunerii verbelor la timpul prezent, în conformitate cu art. 54 alin. (1) lit. j) din Legea nr. 100/2017 cu privire la actele normative (în continuare – Legea nr. 100/2017). La alin. (7), expresia „fără întârziere” nu determină termenul-limită în care urmează a fi realizată informarea utilizatorilor. În acest sens norma se va completa cu un termen cert sau cu criterii care să permită determinarea acestuia. Observația dată este valabilă și pentru art. 6 alin. (7). La alin. (20) cuvintele „pagina sa oficială” se vor substitui cu cuvintele „pagina sa web oficială”.	**Se acceptă.** Proiectul a fost modificat conform propunerilor.
	11.4	La art. 6, în alin. (9), trimiterea generală la „cadrul normativ aplicabil” se va concretiza prin indicarea actului normativ relevant sau a categoriei determinate de acte normative care impun identificarea utilizatorului.	**Se acceptă parțial.** Se consideră oportună clarificarea sintagmei „cadrul normativ aplicabil”, în vederea evitării unei interpretări excesiv de largi și pentru asigurarea unei aplicări uniforme a prevederii. Totodată, având în vedere diversitatea domeniilor în care pot activa beneficiarii portofelelor pentru identitatea digitală și multitudinea actelor normative sectoriale care pot stabili obligații de identificare a utilizatorilor, enumerarea exhaustivă a actelor normative sau indicarea unor acte concrete nu este fezabilă și ar putea conduce la limitarea aplicabilității normei. În acest sens, prevederea a fost reformulată după cum urmează: „Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care legislația aplicabilă serviciului sau activității

			desfășurate de aceștia nu impune identificarea utilizatorului.”
	11.5	La art. 8 alin. (3), cuvântul „organismului” se va completa cu cuvintele „de supraveghere”.	La propunerea SIS prevederile de la art. 8 alin. (3) au fost excluse.
	11.6	La art. 9 alin. (3) și (4) sintagma „24 de ore lucrătoare” urmează a fi revizuită, deoarece aceasta nu este specifică tehnicii legislative de stabilire și calculare a termenelor. Noțiunea de „ore lucrătoare” poate genera interpretări neuniforme în aplicare, întrucât nu este clar dacă termenul se calculează în raport cu programul de lucru al furnizorului portofelului pentru identitatea digitală sau potrivit unui alt reper temporal. În cazul în care intenția autorului este de a institui un termen echivalent cu 3 zile lucrătoare, acest fapt urmează a fi indicat expres în textul normei, prin utilizarea formulei „nu mai târziu de 3 zile lucrătoare”. Dacă însă se urmărește instituirea unui termen strict de 24 de ore, acesta trebuie prevăzut ca termen calculat în ore, prin formula „nu mai târziu de 24 de ore”. Prin urmare, pentru asigurarea clarității, previzibilității și aplicării uniforme a normei, se propune substituirea sintagmei „24 de ore lucrătoare” cu una dintre următoarele formule, în funcție de intenția de reglementare: „nu mai târziu de 24 de ore”, dacă se are în vedere un termen calculat în ore; sau „nu mai târziu de 3 zile lucrătoare”, dacă se are în vedere un termen calculat pe zile lucrătoare. Observația dată este valabilă și pentru restul cazurilor similare din proiect.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.7	La art. 13: La alin. (1) pct. 5) se va revedea textul „criteriile prevăzute la alin. (2)”, deoarece la alin. (2) sunt enumerate condițiile pentru includere în listă a unui sistem de identificare electronică, dar nu criteriile. La alin. (2) se va revedea textul „lista prevăzută la alin. (1)”, deoarece la alineatul la care se face trimitere nu este menționată vreo listă. La alin. (4), trimiterea la lista prevăzută în alin. (2) este incorectă, întrucât alineatul menționat stabilește condițiile de eligibilitate,	**Se acceptă.** Proiectul a fost modificat conform propunerilor.

		iar publicarea listei este reglementată la alin. (3). În consecință, trimiterea se va corecta.	
	11.8	La art. 16 alin. (1), trimiterea la cerințele în materie de securitate cibernetică prevăzute la art. 12 alin. (2) se va reexamina. Art. 12 alin. (2) descrie nivelurile de asigurare ale mijloacelor de identificare electronică (criteriile ce urmează a fi îndeplinite), fără a stabili distinct cerințe în materie de securitate cibernetică (valabil și pentru art. 24 alin. (2) lit. a), alin. (3) lit. a)).	**Se acceptă.** Proiectul a fost modificat conform propunerilor.
	11.9	La secțiunea 1 din capitolul III se va revedea denumirea acesteia, or, potrivit art. 45 alin. (1) din Legea nr. 100/2017 cu privire la actele normative dispoziţiile generale ale actului normativ sunt prevederile care: a) determină obiectul, scopul şi domeniul de aplicare; b) orientează întreaga reglementare; c) explică termeni (noțiuni) și definesc concepte.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	11.10	La art. 17 alin. (1), referința la Codul civil al Republicii Moldova se va completa prin indicarea numărului actului normativ, după cum urmează: „Codul civil al Republicii Moldova nr. 1107/2002”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.11	La art. 21: La alin. (6), se reiterează obiecția privind corelarea cu terminologia art. 11 din Legea nr. 48/2023 privind securitatea cibernetică. Cuvintele „oricare dintre cerințele prevăzute la art. 11” se vor substitui cu o referință la măsurile de gestionare a riscurilor în materie de securitate cibernetică. La alin. (9), cuvintele „Guvernul va stabili” se vor substitui cu cuvintele „Guvernul stabilește”.	**Se acceptă.** Proiectul a fost modificat conform propunerilor.
	11.12	La art. 24: La alin. (2) pct. 3), pentru uniformizarea terminologiei, cuvântul „daune” se va substitui cu cuvintele „prejudiciile cauzate”. La alin. (2) pct. 8) textul „pct. 7” se va substitui cu textul „pct. 7)”	**Se acceptă.** Proiectul a fost modificat conform propunerilor.
	11.13	La art. 29 alin. (1) se va reformula pentru a prevedea o normă imperativă „Certificatele calificate pentru semnăturile electro-	**Se acceptă.** Proiectul a fost modificat conform propunerilor.

		nice trebuie să îndeplinească cerințele prevăzute la art. 30.” (valabil și pentru art. 31 alin. (1), art. 40 alin. (1), art. 50 alin. (1) ș.a.).	
	11.14	La art. 31 alin. (2) lit. c) se propune excluderea cuvintelor „în prezent”. Norma are caracter general și urmează să se aplice nu doar la momentul adoptării legii, ci pe întreaga durată de aplicare a acesteia. Utilizarea sintagmei „în prezent” poate crea incertitudine juridică, întrucât nu este clar dacă aceasta se referă la momentul adoptării legii sau la momentul certificării dispozitivului. În domeniul semnăturilor electronice și al securității cibernetice, nivelul tehnologic evoluează rapid, iar cerințele de protecție trebuie să rămână aplicabile în raport cu tehnologia disponibilă la momentul evaluării concrete, nu cu tehnologia existentă la data adoptării legii. Menținerea expresiei „în prezent” ar putea conduce la interpretarea eronată că dispozitivele trebuie raportate doar la nivelul tehnologic existent la momentul intrării în vigoare a legii, ceea ce ar diminua caracterul actual, dinamic și preventiv al normei.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.15	La art. 34 alin. (4) 8 atragem atenția că, expresia „inclusiv și” reprezintă un pleonasm, în care „inclusiv” conţine sensul „şi”, astfel că pentru o bună exprimare este suficient să spunem una din două: ori „şi”, ori „inclusiv”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.16	La art. 44 enumerarea articolelor la care se face referință se va indica prin cratimă „art. 34-36”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.17	La art. 67: La alin. (2) și (3), termenele pentru depunerea plângerii se regăsesc și la art. 73 alin. (5). Prin urmare, reglementarea se va concentra într-un singur articol, cu efectuarea trimiterilor corespunzătoare. La alin. (5), trimiterea la art. 71 alin. (3) este incorectă, întrucât norma respectivă nu reglementează actele organismului de supraveghere susceptibile de contestare. În consecință, trimiterea se va corecta prin raportare la dispozițiile privind măsurile și deciziile organismului de supraveghere.	**Se acceptă.** Proiectul a fost modificat conform propunerilor.

	11.18	La art. 71 alin. (5) atragem atenția că, legislația națională nu operează cu termenul „forța majoră”.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	11.19	La art. 76 alin. (2), formula „un termen de cel puțin două luni” nu determină termenul concret pentru achitarea voluntară. În acest sens, se va stabili un termen cert sau mecanismul de determinare a acestuia.	**Se acceptă.** Proiectul a fost modificat ținând cont de propunere.
	11.20	La art. 78 alin. (3), enumerarea începe cu lit. c), motiv pentru care, diviziunile se vor renumerota consecutiv, începând cu lit. a).	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.21	La art. 79 alin. (1), după suma „1 000 000” se va indica unitatea monetară.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.23	La art. 80: La alin. (1), intrarea în vigoare a capitolului VI la expirarea a 24 de luni de la publicare, în condițiile în care celelalte dispoziții intră în vigoare la expirarea a 12 luni, generează o perioadă în care obligațiile materiale sunt aplicabile fără mecanismul sancționator prevăzut de proiect. În consecință, termenele se vor corela, astfel încât să nu se creeze un vid normativ în ceea ce privește asigurarea respectării legii. La alin. (2) se vor revizui termenele acordate Guvernului pentru întreprinderea măsurilor necesare implementării legii, în special, cele de la lit. a) și b). În context, formula „până la intrarea în vigoare a prezentei legi” se va exclude. Alin. (3) se va completa în final cu textul „ , cu modificările ulterioare”, întrucât Legea nr. 124/2022, propusă spre abrogare, a fost supusă modificărilor.	**Se acceptă.** Proiectul a fost modificat conform propunerilor.
	11.24	La art. 81: La alin. (1), cuvintele „conform prevederilor legii” se vor substitui cu cuvintele „conform prevederilor prezentei legi”. La alin. (3), (4) și (5) se vor indica denumirile Legilor nr. 124/2022 și nr. 273/1994.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.25	Cu titlu general, proiectul se va revizui integral în vederea excluderii formulărilor nedeterminate, a corectării trimiterilor interne și a uniformizării terminologiei. Formulările „fără întârziere”,	**Se acceptă.** Proiectul a fost modificat conform propunerilor.

		„atunci când este cazul”, „dacă este necesar”, „în mod corespunzător”, „termen rezonabil” și trimiterile la „cadrul normativ aplicabil” se vor utiliza numai în cazurile în care conținutul și limitele acestora pot fi determinate cu certitudine din normă sau din actul normativ indicat expres.	
Centrul Național Anticorupție (Nr. 06/2/11587 din 26.06.2026)	12.1	**III. Analiza detaliată a factorilor de risc și a riscurilor de corupție ale proiectului** **Obiecție generală asupra proiectului** Unele norme din proiect reglementează anumite situații în cazul survenirii/îndeplinirii unor criterii/condiții. Astfel, spre exemplu, la art. 11 alin. (1) se utilizează textul „cu condiția să fie îndeplinite următoarele criterii”, la art. 12 alin. (2) se utilizează textul „îndeplinesc următoarele criterii” ș.a. Totodată, în alte norme din proiect, se menționează despre obligativitatea întrunirii cumulative a criteriilor/condițiilor enunțate în normă. Spre exemplu, norma statuată la art. 13 alin. (2) stabilește expres obligativitatea întrunirii cumulative a condițiilor. În acest sens, considerăm că pot fi situații descrise în norme ale căror criterii urmează să fie întrunite cumulativ, însă, redacțiile normelor pot crea interpretări defectuoase cu riscul aplicării confuze a normelor. **Recomandări:** În vederea eliminării riscului interpretării faptului dacă unele criterii urmează să fie întrunite cumulativ sau nu, propunem autorului reexaminarea tuturor normelor care reglementează aceste aspecte și identificarea individuală a cazurilor în care anumite criterii/condiții urmează să fie întrunite cumulativ. **Factori de risc:** ● Lacună de drept ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor **Riscuri de corupție:** ● Generale	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	12.2	**Art. 24 alin. (5) din proiect -** Articolul 24. Cerințe pentru prestatorii de servicii de încredere calificați (...)	**Se acceptă.**

		(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. **Obiecții:** Norma nu stabilește obligația organismului de supraveghere de justificare a solicitării unor informații suplimentare, precum și nu stabilește un termen real și obiectiv de conformare din partea prestatorului de servicii. În aceste condiții, există riscul ca unele solicitări de informații, precum și stabilirea anumitor condiții suplimentare să fie efectuate/solicitate fără a fi motivate justificativ. Astfel, norma riscă să fie aplicată în mod confuz și abuziv, în dependență de interes și scopul urmărit. **Recomandări:** Propunem autorului stabilirea obligativității organismului de supraveghere de justificare a solicitării informațiilor suplimentare și a stabilirii unor condiții suplimentare pentru acordarea permisiunii de a pune în aplicare modificările preconizate ale serviciilor de încredere calificate. La fel, propunem stabilirea unui termen de conformare, termen care să fie real și obiectiv pentru ca prestatorul de servicii să poată îndeplini solicitările înaintate. **Factori de risc:** ● Lacună de drept ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor **Riscuri de corupţie:** ● Generale	Norma a fost completată prin instituirea obligației organismului de supraveghere de a solicita informații suplimentare și de a stabili condiții suplimentare printr-o decizie motivată. Totodată, au fost stabilite termene clare pentru finalizarea verificării, inclusiv obligația de informare a prestatorului cu privire la motivele întârzierii și termenul de finalizare, durata totală a verificării neputând depăși patru luni de la data notificării.
	12.3	**IV. Concluzia expertizei** În nota de fundamentare se menționează: „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 ser-	**S-a luat act.**

		viciilor 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". Potrivit articolului 1 din proiectul legii: „Prezenta lege urmărește să asigure buna funcționare a pieței digitale naționale și facilitarea interoperabilității cu piața digitală europeană, precum 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 online". În proiect au fost atestate norme care induc confuzie în stabilirea procedurilor de exercitare a unor atribuții/drepturi/obligații ale subiecților responsabili de implementarea normelor proiectului. Astfel, în conținutul proiectului au fost identificare norme care stabilesc proceduri administrative confuze și ambigui privind: - modul de solicitare a informațiilor suplimentare în condițiile articolului 24 alin. (5) din proiect; - modul de îndeplinire a unor condiții/criterii în vederea aplicării normelor din proiect. În final, recomandăm autorului reexaminarea proiectului prin prisma prezentului raport de expertiză anticorupție și eliminarea factorilor și riscurilor de corupție identificați.	

Comentariile Comisiei Europene	1.	Există o lacună substanțială care merită semnalată: la fel ca în cazul Serbiei, este vorba despre plafonul sancțiunilor. Articolul 79 limitează amenzile la aproximativ 50.000–100.000 EUR sau 0,5–0,75% din cifra de afaceri, valori mult sub pragul minim de 5 milioane EUR / 1% din cifra de afaceri la nivel mondial impus de Regulamentul eIDAS; în plus, spre deosebire de standardul UE, procentele din legislația Republicii Moldova se aplică cifrei de afaceri naționale (nu celei globale), ceea ce restrânge și mai mult baza de calcul. Republica Moldova a recunoscut deja acest aspect în tabel, prezentându-l ca pe o abordare etapizată deliberată, și nu ca pe o dovadă de conformitate, astfel încât situația nu ar trebui să constituie o surpriză pentru autoritățile de la Chișinău.	**S-a luat act.** Comentariile referitor la acest articol au fost înserate în tabelul de concordanță.
	2.	O eroare de trimitere încrucișată în definițiile de la articolul 3 (trimitere la art. 60 în loc de art. 49).	**Se acceptă.** Corectat.
	3.	Denumirea inconsecventă a „portofelului de identitate digitală” în articolul 64.	**Se acceptă.** Corectat.
	4.	Aproximativ douăsprezece rânduri în care competențele de a adopta acte delegate, rezervate exclusiv Comisiei, erau marcate drept „Compatibile” în loc de „Neaplicabile”.	**Se acceptă.** Au fost operate modificările corespunzătoare.
		Articolele 67–70 și 72–77 (procedura privind plângerile/asigurarea respectării normelor) nu sunt incluse în tabel.	**Se acceptă.** Tabelul a fost completat.
	1	1. Evaluare generală	**S-a luat act.**

Comentariile Comisiei Europene (suplimentar)		Proiectul de lege reprezintă, în arhitectura sa generală, o transpunere solidă a Regulamentului eIDAS. Această evaluare prezintă concluziile pe baza tabelului de concordanță, a memorandumului explicativ și a unei verificări încrucișate independente (revizuirea expertului TAIEX). De asemenea, au fost identificate probleme de acuratețe a tabelului (rânduri clasificate greșit, referințe încrucișate, terminologie); acestea nu afectează conformitatea legii în sine și au fost abordate direct ca observații în tabelul de concordanță, mai degrabă decât reformulate aici.	
	2	2. Nivelurile de sancțiuni (articolul 79) Articolul 16(2) din Regulament prevede amenzi de cel puțin 5.000.000 EUR sau, pentru o persoană juridică, 5.000.000 EUR sau 1% din cifra de afaceri mondială, oricare dintre acestea este mai mare — un prag obligatoriu, nu o orientare. Articolul 79 din proiectul de lege plafonează amenzile la 1.000.000–2.000.000 MDL (≈ 50.000–100.000 EUR) sau 0,5–0,75% din veniturile/cifra de afaceri națională (nu mondială) — aproximativ 1–2% din pragul necesar, pe o bază mai restrânsă decât cea prevăzută în Regulament. Această prevedere este marcată „Compatibilă” în tabel. Observația proprie a Republicii Moldova pe același rând, însă, recunoaște direct lacuna, descriind o „abordare etapizată” către „convergența treptată” cu regimul UE — în esență, o recunoaștere a conformității parțiale. Două aspecte suplimentare: expunerea de motive a proiectului de lege afirmă o compatibilitate necondiționată cu Regulamentul și nu dezvăluie nicăieri această lacună, nici măcar în secțiunile sale de implementare — aceasta ar trebui să fie aliniată cu ceea ce admite deja tabelul de concordanță. Separat, articolul 79 alineatul (1) supune în mod explicit doar furnizorii de servicii de încredere calificați amenzilor pentru anumite categorii de încălcări, deși articolul 16 alineatul (2) impune ca atât furnizorii calificați, cât și cei necalificați să fie incluși în regulament.	**Se acceptă parțial.** În tabelul revizuit, transpunerea art. 16 alin. (2) a fost reclasificată din „Compatibil” în „Transpunere parțială”, cu prezentarea argumentelor aferente. Cuantumul amenzilor a fost calibrat în raport cu principiul proporționalității și cu particularitățile pieței naționale a serviciilor de încredere, ținând cont de dimensiunea acesteia, de gradul de maturitate al ecosistemului național de identitate digitală și de capacitatea economică a operatorilor vizați. Abordarea este similară celei utilizate la elaborarea Legii nr. 195/2024 privind protecția datelor cu caracter personal, prin care a fost asigurată transpunerea și aplicarea Regulamentului (UE) 2016/679 (GDPR), inclusiv în ceea ce privește calibrarea regimului sancționator la particularitățile și capacitatea pieței naționale. După cum a fost menționat și în comentariile din Tabelul de concordanță, convergența deplină cu cerințele europene este prevăzută într-un orizont temporal cert, până la data aderării Republicii Moldova la Uniunea Europeană. Până la acel moment, dispozițiile referitoare la regimul sancționator vor fi revizuite, după caz, astfel încât cuantumurile

			și mecanismele aplicabile să corespundă cerințelor europene incidente la data aderării. Totodată, până la aderare, cuantumurile amenzilor vor fi reevaluate periodic, ținând seama inclusiv de evoluția pieței și de datele reflectate în raportul anual al organismului de supraveghere, în temeiul art. 64 alin. (6). Suplimentar, comentarii referitor la acest articol au fost înserate în tabelul de concordanță.
	3	3. Domeniul de aplicare al cadrului de supraveghere și sancțiuni Cadrul de supraveghere și răspundere (articolele 64, 67-79) este construit în principal în jurul furnizorilor de portofele digitale de identitate și al furnizorilor de servicii de încredere. Cu toate acestea, proiectul de lege, în ansamblu, impune obligații unui set considerabil mai larg de entități - părți care utilizează reglementările, furnizori de scheme de identificare electronică, furnizori de browsere web, organisme din sectorul public responsabile de surse autentice și organisme care emit atestări electronice ale atributelor - și nu este clar dacă toate acestea intră sub incidența mandatului organismului de supraveghere sau se confruntă cu sancțiuni eficiente, proporționale și disuasive pentru nerespectare. Aceasta reprezintă o lacună în coerența cadrului de aplicare a legii și ar trebui abordată prin revizuirea împreună a articolelor 64 și 67-79 pentru a confirma că mandatul de supraveghere și regimul de sancțiuni se extind la fiecare categorie de entități reglementate de lege. În mod similar, articolele 67-70 și 72-77 (reclamații, contestații și proceduri de aplicare a legii) nu au rânduri corespondente nicăieri în tabelul de concordanță și ar trebui mapate explicit, chiar dacă concluzia este că sunt prevederi specifice la nivel național, fără un corespondent direct la nivelul UE.	**Se acceptă parțial.** Referitor la reflectarea art. 67–70 și 72–77 în tabelul de concordanță, articolele respective au fost incluse anterior în tabelul revizuit ca dispoziții procedurale naționale. Ele asigură aplicarea efectivă a art. 16 și a art. 46a–46b din Regulament, precum și dreptul la plângere și la o cale de atac efectivă. Referitor la sfera subiecților supuși supravegherii și sancționării (art. 64, 67–79), Regulamentul UE nu instituie un regim general de amenzi pentru toate categoriile de entități care intră în domeniul său de aplicare. Este important de subliniat că Regulamentul nu stabilește o listă generală și exhaustivă a subiecților cărora trebuie să li se aplice amenzi și nici nu impune extinderea regimului sancționator asupra tuturor participanților la ecosistemul identității digitale. Art. 16 alin. (2) conține în mod expres o referință la „prestatorii de servicii de încredere calificați și necalificați”, în raport cu care stabilește nivelul minim al plafonului maxim al amenzilor. În ceea ce privește celelalte categorii de entități, Regulamentul stabilește obligații și competențe de supraveghere distincte, dar nu impune, în mod expres, aplicarea unor amenzi. Proiectul de lege urmează

			această arhitectură. Domeniul său de aplicare, prevăzut la art. 2 alin. (1), corespunde, în esență, domeniului de aplicare al Regulamentului și vizează sistemele de identificare electronică, portofelele și serviciile de încredere. Mandatul organismelor de supraveghere prevăzut la art. 46a și 46b din Regulament este, în principal, orientat spre furnizorii de portofele și prestatorii de servicii de încredere. În acest context, regimul sancționator instituit prin proiect nu reprezintă o simplă transpunere mecanică a unor amenzi prevăzute pentru toate categoriile de entități, ci o opțiune legislativă națională, exercitată în limitele cadrului european și în funcție de natura obligațiilor aplicabile fiecărei categorii. Mai mult, proiectul depășește deja nivelul minim identificabil în Regulament, întrucât permite aplicarea amenzilor și furnizorilor de portofele, inclusiv autorităților publice atunci când acestea acționează în această calitate, potrivit art. 79 alin. (3). Pentru celelalte categorii de entități, Regulamentul instituie mecanisme proprii de supraveghere și măsuri de remediere, care au fost transpuse în proiect. În cazul beneficiarilor, aceștia sunt supuși obligației de înregistrare (art. 6), iar organismul de supraveghere poate suspenda sau anula înregistrarea în situațiile de utilizare ilegală sau frauduloasă a portofelului, potrivit art. 64 alin. (3) pct. 1) lit. b), care transpune art. 46a alin. (4) lit. f) din Regulament. Totodată, solicitările nejustificate de date pot fi semnalate din portofel autorității pentru protecția datelor cu caracter personal, în condițiile art. 5 alin.

			(5) pct. 4) lit. c), iar organismul de supraveghere are obligația de a informa această autoritate în termen de cel mult 24 de ore, potrivit art. 64 alin. (3) pct. 1) lit. c). În funcție de natura faptei, răspunderea acestora este asigurată inclusiv prin mecanismele prevăzute de Legea nr. 195/2024 privind protecția datelor cu caracter personal, iar beneficiarii din sectoarele reglementate rămân supuși și regimurilor sectoriale aplicabile.Instituirea unei amenzi suplimentare în temeiul prezentei legi, pentru aceleași conduite, ar putea conduce la suprapunerea regimurilor sancționatorii și, după caz, la dublarea consecințelor juridice pentru aceeași faptă. În plus, extinderea prematură a sancțiunilor pecuniare asupra beneficiarilor ar putea constitui un factor de descurajare a participării acestora la ecosistemul portofelului, în condițiile în care gradul de adoptare a beneficiarilor este esențial pentru utilitatea practică a portofelului. În ceea ce privește sistemele de identificare electronică, mijloacele de identificare din cadrul sistemelor incluse în lista națională sunt emise exclusiv de organisme din sectorul public, potrivit art. 13 alin. (2) lit. a). În linie cu mecanismul instituit de Regulament la art. 7–12, cadrul de conformare este bazat pe notificare, includerea în lista națională, certificare și măsuri de remediere, inclusiv anularea certificării în cazul în care vulnerabilitățile identificate nu sunt remediate, potrivit art. 16 alin. (2), precum și pe răspundere civilă, în condițiile art. 71 alin. (3) și (4). Prin urmare, pentru această categorie, mecanismul european este construit în jurul unor măsuri de conformare și

			remediere, și nu al unui regim distinct de amenzi. Pentru furnizorii de browsere web, Regulamentul atribuie organismului de supraveghere competențe specifice privind examinarea notificărilor și solicitarea încetării măsurilor de precauție, prevăzute la art. 45a alin. (4) și art. 46b alin. (4) lit. k). Aceste competențe sunt transpuse la art. 51 alin. (4) și art. 64 alin. (3) pct. 2) lit. g) din proiect. În plus, acești furnizori sunt, în principal, operatori globali care nu dispun de un sediu în Republica Moldova, ceea ce limitează în mod semnificativ eficiența practică a unei amenzi naționale. În aceste condiții, măsurile de supraveghere prevăzute de Regulament sunt mai adecvate pentru realizarea obiectivului de conformare. În cazul organismelor din sectorul public responsabile de surse autentice, obligațiile prevăzute la art. 45e și art. 45f alin. (2) și (3) din Regulament sunt formulate ca obligații ale statelor membre („Member States shall ensure”) și nu sunt însoțite de un mecanism european de amenzi aplicabile acestor organisme. Proiectul le transpune prin măsuri organizatorice și normative adoptate de Guvern, inclusiv cele prevăzute la art. 55 alin. (3) și art. 56 alin. (4), precum și printr-un termen de conformare de 24 de luni, potrivit art. 80 alin. (5). În cazul autorităților publice, aplicarea unei amenzi care urmează a fi vărsată la bugetul de stat, conform art. 77 alin. (2), nu ar produce, în sine, efectul de conformare urmărit, întrucât ar conduce, în esență, la transferarea unor mijloace financiare în interiorul sectorului public.

			Pentru această categorie, respectarea obligațiilor se asigură mai adecvat prin mecanismele de control administrativ, control ierarhic, responsabilitate managerială și celelalte forme de răspundere prevăzute de cadrul normativ aplicabil. Din acest motiv, amenzile aplicabile autorităților publice au fost prevăzute numai în măsura în care acestea acționează în calitate de furnizori de portofele sau prestatori de servicii de încredere, potrivit art. 79 alin. (3). În ceea ce privește emitenții de atestate electronice ale atributelor, aceștia nu constituie o categorie distinctă de subiecți. Emiterea și validarea atestatelor reprezintă servicii de încredere, potrivit noțiunii de „serviciu de încredere” de la art. 3 lit. g) și h). Prin urmare, entitățile private care prestează asemenea servicii se califică drept prestatori de servicii de încredere, calificați sau necalificați, și sunt supuse integral supravegherii și regimului sancționator prevăzut la art. 64 și 77–79, inclusiv în ceea ce privește obligațiile de la art. 57 și 58. În afara acestui regim rămân exclusiv organismele publice prevăzute la art. 56, cărora li se aplică argumentele expuse mai sus. Excluderea anumitor categorii din sfera amenzilor nu creează o lacună în competențele de supraveghere. Procedura de constatare a încălcărilor poate fi inițiată atât în urma unei plângeri depuse de orice persoană afectată, cât și din oficiu, potrivit art. 72 alin. (1). Totodată, toate persoanele juridice de drept public sau privat și persoanele fizice au obligația de a se supune activităților de investigare, conform art. 74 alin. (6). Prin urmare, faptul că aplica-

			rea amenzilor este rezervată anumitor categorii de entități nu limitează competența generală de supraveghere și investigare a organismului competent. În această logică, diferența dintre sfera subiecților supuși supravegherii și sfera subiecților cărora li se pot aplica amenzi este una deliberată. Nu orice entitate asupra căreia organismul de supraveghere poate exercita competențe de investigare trebuie, în mod necesar, să fie și subiect al sancțiunilor pecuniare. Prin urmare, soluția propusă nu trebuie interpretată ca o excludere definitivă a posibilității instituirii unor sancțiuni pecuniare pentru alte categorii de entități, ci ca o opțiune legislativă proporțională cu cadrul european, natura obligațiilor și mecanismele de conformare aplicabile fiecărei categorii. Necesitatea unor sancțiuni specifice pentru alte categorii poate fi reevaluată ulterior, inclusiv în lumina practicii de supraveghere, a evoluției pieței și în cadrul procesului de convergență prevăzut la pct. 1.
	4	4. Lacune suplimentare confirmate Articolul 65 (punct unic de contact). Proiectul de lege nu prevede publicarea numelui și adresei organismului de supraveghere în calitatea sa de punct unic de contact, așa cum prevede articolul 46 litera c alineatul (3) din Regulament. Aceasta este o lacună îngustă, dar confirmată (evaluată independent ca „Nealiniată”) și ușor de eliminat. Articolele 70/71/17 (răspundere). Relația dintre regula generală privind răspunderea (art. 70), regula răspunderii specifice transfrontaliere (art. 71) și regula răspunderii serviciilor de încredere (art. 17) este neclară - în special, care regim guvernează tranzacțiile pur naționale .	Punctul unic de contact este desemnat chiar prin lege: art. 65, coroborat cu art. 64 alin. (1), îl desemnează pe Serviciul de Informații și Securitate. Prin publicarea legii în Monitorul Oficial, desemnarea devine publică, iar denumirea și adresa instituției sunt publice. Notificarea Comisiei Europene și publicarea listei de către Comisie (art. 46c alin. (3) și (4)) sunt obligații ale statelor membre. În tabel, ele sunt marcate ca prevederi care vor deveni aplicabile la data aderării.

Ministru **Claudiu-Iulius-Gavril NĂSUI**