NOTA DE FUNDAMENTARE
a proiectului de lege privind protecția informațiilor clasificate

1. Denumirea autorului proiectului
Proiectul de lege privind protecția informațiilor clasificate a fost elaborat de Ministerul Justiției în comun cu Serviciul de Informații și Securitate.
2. Condițiile ce au impus elaborarea proiectului
2.1. Temeiul legal și sursa proiectului
Prezentul proiect are drept scop realizarea acțiunii nr. 1 din Capitolul 31 al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor normative
Cadrul normativ în vigoare este constituit din Legea nr. 245/2008 cu privire la secretul de stat și actele normative subsecvente, inclusiv Hotărârea Guvernului nr. 1176/2010. Pe parcursul aplicării Legii nr. 245/2008, autoritățile responsabile au identificat atât dificultăți, cât și omisiuni care, per ansamblu, diminuează capacitatea statului de a-și proteja informațiile sensibile a căror divulgare neautorizată ar cauza prejudicii de diferite grade securității naționale a Republicii Moldova. Totodată, în procesul de negociere, semnare și implementare a Acordului dintre Republica Moldova și Uniunea Europeană privind procedurile de securitate pentru schimbul și protecția informațiilor clasificate, semnat la Bruxelles la 31 martie 2017, s-au evidențiat discrepanțe majore între normele naționale și cele europene, în special reglementarea fragmentară a securității industriale, a partajării și transmiterii informațiilor clasificate, precum și a protecției informațiilor în sistemele informatice și de comunicații. Aceste deficiențe necesită înlocuirea integrală a cadrului legislativ existent cu o nouă lege, aliniată la terminologia, principiile și standardele minime de securitate consacrate la nivelul Uniunii Europene. Adițional, în contextul integrării Republicii Moldova la Uniunea Europeană, este necesară stabilirea cadrului național de aplicare a Deciziei 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate.

3. Obiectivele urmărite și soluțiile propuse

Obiectivul prezentului proiect constă în alinierea cadrului normativ din domeniul protecției informațiilor clasificate la terminologia, principiile și standardele minime de securitate consacrate la nivelul Uniunii Europene, precum și stabilirea cadrului național de aplicare a Deciziei 2013/488/UE.

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul este structurat în VII capitole și 43 de articole. În continuare, în cadrul prezentului compartiment, vor fi descrise detaliat principalele prevederi ale proiectului, per fiecare capitol, pentru stabilirea sensului exact al normelor juridice propuse.

CAPITOLUL I – DISPOZIȚII GENERALE

Articolul 1 stabilește obiectul legii – cadrul juridic al protecției informațiilor clasificate – și domeniul de aplicare: entitățile care dețin sau gestionează informații clasificate și persoanele fizice care, în exercitarea atribuțiilor, accesează asemenea informații. Legea se aplică și informațiilor clasificate primite de la state străine sau organizații internaționale, în condițiile tratatelor internaționale ori ale acordurilor de securitate încheiate conform legii. Potrivit art. 1 alin. (4), capitolele III–VI se vor aplica în mod corespunzător și informațiilor UE clasificate, în corespundere cu Decizia 2013/488/UE. Această dispoziție va intra în vigoare la data aderării Republicii Moldova la Uniunea Europeană, moment de la care Decizia va deveni aplicabilă Republicii Moldova în calitate de stat membru.

Articolul 2 definește 15 noțiuni principale, preluate, în esență, din apendicele A la Decizia 2013/488/UE. Noțiunea centrală a proiectului de lege este cea de „informații clasificate”, definite drept orice informații sau materiale cărora li s-a atribuit o clasificare de securitate în condițiile prezentei legi, a căror divulgare neautorizată poate cauza prejudicii de diferite grade securității naționale a Republicii Moldova.

Astfel, elementul definitoriu al noțiunii de „informații clasificate” este criteriul material al divulgării neautorizate susceptibile să cauzeze prejudicii securității naționale. Noțiunea de „securitate națională” are semnificația prevăzută la art. 3 pct. 8 din Legea nr. 249/2025 privind securitatea națională a Republicii Moldova, și anume totalitatea acțiunilor și măsurilor întreprinse pentru a asigura existența, stabilitatea și dezvoltarea durabilă a Republicii Moldova prin protejarea suveranității, independenței și unității statului, a integrității teritoriale a țării, a valorilor și

intereselor naționale, precum și a drepturilor și libertăților fundamentale de amenințările și pericolele, interne sau externe, de orice natură.

Noțiunea de „entitate publică" cuprinde patru categorii (autorități publice, instituții publice, întreprinderi de stat sau municipale, societăți comerciale cu capital integral sau majoritar public), iar „entitatea industrială sau de altă natură" acoperă orice persoană fizică sau juridică furnizoare de bunuri, lucrări sau servicii, inclusiv din sectorul privat. Definițiile noțiunilor de „emitent" și „deținător" consacră principiul controlului emitentului și, respectiv, principiul necesității de a cunoaște, transversale întregii legi.

CAPITOLUL II – CLASIFICAREA INFORMAȚIILOR

Articolul 3 permite clasificarea numai a informațiilor a căror divulgare neautorizată poate cauza un prejudiciu real și identificabil securității naționale și care se încadrează în una dintre categoriile expres enumerate, grupate în patru domenii: apărarea națională; capacitatea de apărare și mobilizare a statului; relațiile externe; securitatea statului și asigurarea ordinii de drept.

Elementul esențial al procesului de clasificare este prevăzut la art. 3 alin. (2), care instituie expres testul interesului public: informațiile se clasifică numai dacă prejudiciul potențial pentru securitatea națională prevalează în raport cu interesul public în accesarea informației. Norma transformă clasificarea dintr-o prerogativă discreționară într-o decizie supusă unui criteriu material verificabil.

Articolul 4 enumeră categoriile de informații care nu pot fi clasificate (încălcările drepturilor omului, starea mediului, accidentele și catastrofele, starea sănătății populației, faptele de încălcare a legii de către entitățile publice și persoanele cu funcții de răspundere etc.) – garanție de transparență care împiedică utilizarea clasificării pentru ascunderea ilegalităților.

Articolul 5 stabilește cele patru niveluri de clasificare – „Strict secret", „Secret", „Confidențial" și „Restricționat" – definite prin gravitatea prejudiciului pe care divulgarea neautorizată îl poate cauza securității naționale, în deplină corespondență cu nivelurile TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL și RESTREINT UE/EU RESTRICTED prevăzute la art. 2 alin. (2) din Decizie. Sistemul marcajelor de clasificare și al marcajelor suplimentare asigură identificarea și gestionarea corespunzătoare a informațiilor.

Articolul 6 consacră principiul controlului emitentului: informațiile nu pot fi supuse reducerii nivelului de clasificare sau declasificate și niciun marcaj nu poate fi modificat ori eliminat fără acordul prealabil scris al emitentului. Articolul reglementează Nomenclatorul informațiilor clasificate, aprobat de Guvern în scopul

promovării unei politici de stat unice, și nomenclatoarele departamentale, elaborate de entitățile publice în baza și în limitele Nomenclatorului, aprobate după coordonarea cu Serviciul de Informații și Securitate și supuse reevaluării periodice, cel puțin o dată la 5 ani.

Articolul 7 limitează durata maximă a clasificării la 25, 15, 10 și, respectiv, 5 ani, în funcție de nivel, cu posibilitatea prelungirii motivate, care nu poate depăși jumătate din durata inițială. Prin derogare, informațiile privind persoanele care colaborează sau au colaborat confidențial cu organele care desfășoară activitate contrainformativă, informativă externă sau specială de investigații se clasifică pe durată nedeterminată – protecție justificată de riscul permanent la care sunt expuse aceste persoane.

Articolul 8 reglementează declasificarea (la expirarea termenului, la schimbarea circumstanțelor, la modificarea art. 3 sau 4 ori în temeiul unei decizii care constată clasificarea neîntemeiată), inclusiv competența Serviciului de a decide declasificarea informațiilor clasificate neîntemeiat și regimul special al fondurilor arhivistice. Articolul 9, la rândul său, instituie dreptul oricărei persoane fizice sau juridice de a contesta clasificarea în conformitate cu Codul administrativ nr. 116/2018, asigurând controlul judiciar al deciziei de clasificare.

CAPITOLUL III – SECURITATEA INFORMAȚIILOR CLASIFICATE

Capitolul III constituie nucleul proiectului și este structurat în cinci secțiuni, corespunzătoare celor patru componente ale securității (securitatea personalului, securitatea fizică, securitatea sistemelor informatice și de comunicații, managementul informațiilor), precedate de dispoziții generale.

Secțiunea 1 (art. 10–12) stabilește responsabilitatea deținătorului pentru protecția informației, obligația protejării informațiilor primite de la alte state sau organizații internaționale la nivel echivalent, precum și procesul de gestionare a riscului de securitate, întemeiat pe conceptul apărării în profunzime și pe principiul proporționalității măsurilor cu nivelul de clasificare, forma și volumul informațiilor și evaluarea amenințării. Entitățile elaborează, coordonează cu Serviciul și aplică Programul de prevenire a scurgerii informațiilor clasificate și Planul de urgență. Articolul 12 definește încălcarea securității și compromiterea informațiilor clasificate, instituie obligația raportării imediate către Serviciu a oricărei încălcări sau suspiciuni de încălcare, reglementează măsurile obligatorii în caz de compromitere cunoscută sau prezumată (informarea emitentului, investigarea de către persoane neimplicate, evaluarea prejudiciilor, prevenirea repetării, notificarea

Serviciului și, după caz, a autorității ierarhic superioare) și stabilește răspunderea disciplinară, contravențională sau penală a persoanelor responsabile.

Secțiunea a 2-a (art. 13–33) reglementează regimul juridic al securității personalului. Elementul structurant este distincția, consacrată la art. 13 alin. (2), dintre avizul de securitate a personalului (actul Serviciului care confirmă rezultatul verificării de securitate și care nu conferă, prin el însuși, dreptul de acces) și autorizația de acces la informații clasificate (actul conducătorului entității prin care accesul se acordă efectiv, cu respectarea principiului necesității de a cunoaște).

Articolul 14 condiționează accesul de împlinirea vârstei de 18 ani și de parcurgerea a trei etape: stabilirea necesității de a cunoaște; instruirea și confirmarea scrisă a responsabilităților; pentru nivelul „Confidențial" sau superior – acordarea prealabilă a avizului de securitate a personalului și autorizarea accesului ori autorizarea în alt mod, prin natura funcțiilor deținute. Articolul 15 obligă entitățile publice să aprobe, după coordonarea cu Serviciul, listele funcțiilor care necesită acces, cerința fiind stipulată în fișa postului.

Articolele 16–20 reglementează avizul de securitate a personalului. Evaluarea și emiterea avizului revin Serviciului. Avizul se acordă cetățenilor Republicii Moldova, accesul cetățenilor străini și al apatrizilor fiind reglementat distinct (art. 23 alin. (7) și (8)).

Verificarea de securitate se desfășoară pe baza chestionarului de securitate, în termen de până la 60 de zile lucrătoare pentru nivelul „Confidențial” și până la 90 de zile lucrătoare pentru nivelurile „Secret” și „Strict secret”, cu posibilitatea prelungirii rezonabile, de cel mult 6 luni, în cazul apariției unor riscuri ce necesită verificări suplimentare. Refuzul eliberării avizului se comunică entității printr-o concluzie executorie, care nu exclude o solicitare repetată după înlăturarea împrejurărilor, dar nu mai devreme de 12 luni. Sunt reglementate exhaustiv temeiurile de suspendare a verificării (inclusiv dependența aprecierii de soluționarea definitivă a unei cauze penale în care subiectul are calitatea de bănuit, învinuit sau inculpat – soluție care protejează prezumția de nevinovăție, evitând un refuz întemeiat pe o acuzație nesoluționată) și de încetare a acesteia.

Articolul 18 stabilește criteriile verificării: Serviciul efectuează o evaluare generală a loialității, onestității și încrederii inspirate de persoană, pe baza criteriilor enumerate la alin. (2) – aliniate la pct. 7 din anexa I la Decizie și completate cu elemente specifice contextului național de securitate (separatismul, diversiunea, sprijinirea activităților ostile ale unor state străine). Pentru nivelurile „Secret” și „Strict secret” se verifică suplimentar situația financiară, parcursul educațional, situația profesională, serviciul militar și se realizează interviuri, în corespundere cu pct. 8 din anexa I. Conduita și împrejurările de viață ale soțului/soției ori ale concubinului/concubinei pot fi luate în considerare numai în măsura relevanței

pentru criteriile de securitate, soluție care limitează ingerința în viața privată a terților la strictul necesar.

Articolul 19 dimensionează perioadele de acoperire ale verificării inițiale – cel puțin ultimii 5, 7 și, respectiv, 10 ani, în funcție de nivel, sau perioada de la împlinirea vârstei de 18 ani – în corespundere cu pct. 10–12 din anexa I, și stabilește o valabilitate unică a avizului de 5 ani pentru toate nivelurile.

Articolul 20 reglementează revalidarea în două forme: reverificarea cu eliberarea unui nou aviz (la expirarea valabilității ori la necesitatea unui nivel superior) și reverificarea fără aviz nou, în scopul menținerii sau retragerii avizului existent, declanșată de indicii clare sau suspiciuni rezonabile privind riscuri de securitate. Verificările de revalidare acoperă doar perioada scursă de la verificarea anterioară. Cererea se depune cu cel puțin 3 luni înainte de expirare, iar dacă verificarea nu se finalizează la termen, Serviciul poate prelungi valabilitatea avizului existent cu cel mult 6 luni, după care persoanei i se încredințează atribuții fără acces.

Articolele 21–26 reglementează autorizația de acces. Entitatea publică pune la dispoziție chestionarul de securitate (al cărui model se aprobă de Guvern), îl clasifică, după completare, la nivelul „Restricționat”, solicită acordul scris al persoanei pentru efectuarea verificării și înaintează Serviciului solicitarea motivată. Decizia de autorizare se adoptă de conducătorul entității în termen de 10 zile de la recepționarea avizului, prin emiterea autorizației până la un nivel specificat și o dată precisă, care nu poate depăși valabilitatea avizului. În cazul refuzului avizului, entitatea comunică persoanei esența motivelor, în măsura în care comunicarea nu aduce atingere securității naționale, iar persoana poate solicita Serviciului reexaminarea concluziei și poate contesta refuzul în instanța de contencios administrativ. Pentru nivelul „Restricționat”, autorizația se acordă fără aviz, pe baza verificării interne care include cel puțin verificarea cazierului judiciar. Element de noutate, art. 22 alin. (7)–(9) încredințează autorizarea accesului avocaților, notarilor și executorilor judecătorești organelor de autoadministrare ale profesiilor respective (Consiliul Uniunii Avocaților, Consiliul Camerei Notariale, Consiliul Uniunii Naționale a Executorilor Judecătorești), în conformitate cu legea și cu regulamentele proprii, coordonate cu Serviciul – soluție care conciliază cerințele de securitate cu autonomia profesiilor juridice liberale.

Articolul 23 reglementează certificarea avizului ca instrument de portabilitate la angajare, transfer și detașare, inclusiv internațională, precum și accesul cetățenilor străini și al apatrizilor (în temeiul tratatelor, pe bază de reciprocitate și certificare valabilă; în lipsa acestora – cu titlu de excepție, prin dispoziția scrisă a Prim-ministrului, cu avizul prealabil al Serviciului). Articolul 26 instituie evidența distribuită: Serviciul ține evidența avizelor, iar fiecare entitate – evidența autorizațiilor pe care le emite.

Articolele 24 și 25 reglementează suspendarea și încetarea accesului, cu enumerarea exhaustivă a temeiurilor, interdicția accesului pe durata suspendării, comunicarea esenței motivelor la încetare și dreptul de contestare potrivit Codului administrativ. Persoana căreia accesul i-a încetat ca urmare a încălcărilor poate obține un nou aviz după expirarea termenelor de reabilitare diferențiate: 7 ani (infracțiune), 4 ani (contravenție), 2 ani (încălcare disciplinară) – termene care asigură proporționalitatea consecinței cu gravitatea faptei.

Articolul 27 reglementează excepțiile de la obligația deținerii avizului pentru un șir de demnitari care au acces prin natura funcției, de la data numirii sau alegerii, fără aviz și fără autorizație de acces. Această excepție este încadrată în trei garanții:

a) accesul se exercită numai în măsura în care este strict necesar exercitării atribuțiilor prevăzute expres de lege (principiul necesității de a cunoaște rămâne pe deplin aplicabil);
b) accesul se acordă după semnarea obligației scrise de nedivulgare și instruirea de către Serviciu, cu confirmare scrisă;
c) accesul poate fi suspendat sau poate înceta în condițiile generale ale legii.

Persoanele care dețin și cetățenia altui stat urmează ordinea generală, după efectuarea verificării de securitate.

Articolul 28 reglementează educația și conștientizarea în materie de securitate: instruirea inițială și periodică, confirmările scrise, obligația de a raporta imediat structurii de securitate orice abordare sau activitate suspectă ori neobișnuită, precum și informarea persoanelor la încetarea atribuțiilor cu privire la obligațiile care le revin în continuare.

Articolele 29–31 reglementează împrejurările excepționale: autorizațiile temporare (valabile cel mult 3 luni, fără acces la „Strict secret”, condiționate de verificări preliminare fără informații adverse și de consultarea Serviciului); numirea provizorie și accesul unic la nivelul imediat superior (nerepetitiv, cu justificare scrisă și consemnare); accesul de urgență în împrejurări absolut excepționale, în special pentru salvarea de vieți (pentru „Strict secret” – limitat la deținătorii accesului „Secret”). Fiecare recurgere la aceste proceduri se notifică imediat Serviciului, care primește și un raport anual de ansamblu.

Articolul 32 impune avizarea persoanelor cu acces potențial (curieri, gardieni, escorte), iar articolul 33 condiționează participarea la ședințele clasificate de confirmarea avizului, cu mecanismul dovezii transmise entității organizatoare și informarea acesteia în cazul retragerii avizului.

Secțiunea a 3-a (art. 34) stabilește cadrul securității fizice: obiectivele măsurilor (împiedicarea accesului disimulat sau forțat, descurajarea, detectarea, separarea personalului pe baza necesității de a cunoaște), stabilirea lor pe baza

managementului riscului, instituirea zonelor securizate pentru nivelul „Confidențial” și superior și utilizarea exclusivă a echipamentelor aprobate, modul de asigurare fiind stabilit de Guvern.

Secțiunea a 4-a (art. 35) reglementează protecția informațiilor în sistemele informatice și de comunicații pe baza conceptului de asigurare a informațiilor (confidențialitate, integritate, disponibilitate, nerepudiere, autenticitate), acreditarea obligatorie a sistemelor de către Serviciu, protecția împotriva emisiilor electromagnetice neintenționate și utilizarea produselor criptografice aprobate de Serviciu.

Secțiunea a 5-a (art. 36) reglementează managementul informațiilor pe durata ciclului de viață: sistemele de registre (registre speciale pentru „Strict secret”), inspecțiile periodice ale Serviciului și regulile de transmitere între incinte, cu prioritatea mijloacelor electronice protejate criptografic.

CAPITOLUL IV – SECURITATEA INDUSTRIALĂ

Capitolul IV extinde protecția asupra sectorului privat, reglementând măsurile aplicabile contractanților și subcontractanților în cursul negocierilor precontractuale și pe toată durata contractelor clasificate. Contractele clasificate nu pot implica accesul la informații „Strict secret”. Contractanții și subcontractanții care necesită acces, în obiectivele lor, la informații „Confidențial” sau „Secret” trebuie să dețină aviz de securitate industrială la nivelul de clasificare necesar, iar personalul acestora obține avize de securitate a personalului în condițiile capitolului III. Serviciul aprobă orientări privind securitatea industrială (avizul de securitate industrială, anexa de securitate, vizitele, transmiterea și transportul informațiilor), iar modul de asigurare a securității industriale se stabilește de Guvern.

CAPITOLUL V – PARTAJAREA ȘI TRANSMITEREA INFORMAȚIILOR CLASIFICATE

Partajarea internă a informațiilor clasificate este condiționată de autorizarea entității destinatare pentru nivelul corespunzător și de asigurarea protecției.

Transmiterea către alte state sau către organizații internaționale se realizează în temeiul tratatelor internaționale care garantează protecția la standarde cel puțin la fel de stricte ca cele naționale. În lipsa tratatelor, transmiterea are loc în modul stabilit de Guvern. Entitățile desemnează registre care servesc drept puncte principale de intrare și de ieșire pentru informațiile partajate sau schimbate – mecanism care asigură trasabilitatea circuitului.

CAPITOLUL VI – ORGANIZAREA ȘI CONTROLUL SISTEMULUI DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE

Articolul 39 desemnează Serviciul de Informații și Securitate în calitate de autoritate națională de securitate, responsabilă de punerea în aplicare a legii, stabilește responsabilitatea conducătorilor entităților publice pentru aplicarea legislației la nivelul entităților, obligația entităților publice și industriale de a adopta, după coordonarea cu Serviciul, norme interne de aplicare, precum și competența Serviciului de a emite îndrumări metodologice.

Articolul 40 detaliază atribuțiile Serviciului (coordonarea normelor interne; vizitele de evaluare și controlul măsurilor de securitate; elaborarea proiectelor de acte normative; consultanța; cooperarea cu autoritățile naționale de securitate ale altor state și cu structurile de securitate ale organizațiilor internaționale; efectuarea verificărilor de securitate a personalului și ale entităților industriale; eliberarea avizelor de securitate a personalului și a avizelor de securitate industrială; acreditarea sistemelor; certificarea și expertiza mijloacelor criptografice și tehnice; crearea și administrarea sistemelor guvernamentale de comunicații; constatarea încălcărilor; curieratul diplomatic) și atribuțiile conducătorului entității publice (aprobarea normelor interne și a nomenclatoarelor departamentale; organizarea structurilor de securitate; acordarea autorizațiilor de acces; dispunerea investigațiilor și a inspecțiilor; notificarea Serviciului). Atribuțiile privind măsurile de securitate pentru protecția informațiilor UE clasificate și funcțiile de asigurare a informațiilor prevăzute de Decizia 2013/488/UE (art. 40 alin. (1) lit. o) și p)) intră în vigoare la data aderării Republicii Moldova la Uniunea Europeană, iar atribuțiile privind informațiile clasificate NATO (lit. q) și r)) se exercită de la intrarea în vigoare a legii, în temeiul cadrului de cooperare existent cu Alianța.

Articolul 41 instituie sistemul de control pe trei niveluri: controlul permanent exercitat de conducătorii entităților prin structurile sau funcționarii de securitate; controlul Serviciului asupra entităților publice și industriale, cu prerogative de acces în incinte și la documente, registre și sisteme, în măsura necesară verificării respectării legislației, concluziile controlului fiind obligatorii pentru persoanele cu funcții de răspundere; controlul parlamentar asupra executării legislației, exercitat prin comisia permanentă de profil și prin subcomisia specializată de control asupra activității Serviciului, în condițiile Regulamentului Parlamentului – mecanism care asigură supravegherea democratică a întregului sistem.

CAPITOLUL VII – DISPOZIȚII FINALE ȘI TRANZIOTRII

Legea intră în vigoare la 1 ianuarie 2028, cu excepția art. 1 alin. (4) și art. 40 alin. (1) lit. o) și p), care intră în vigoare la data aderării Republicii Moldova la Uniunea Europeană.

La data intrării în vigoare se abrogă Legea nr. 245/2008 cu privire la secretul de stat. Dispozițiile tranzitorii asigură continuitatea protecției: informațiile atribuite la secret de stat se echivalează cu nivelurile de clasificare ale noii legi, autorizațiile de acces emise în temeiul Legii nr. 245/2008 își păstrează valabilitatea, iar cauzele aflate pe rol se soluționează potrivit legii în vigoare la data apariției raportului juridic litigios.

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

În vederea atingerii obiectivului trasat, opțiuni alternative nu au fost identificate.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul nu implică crearea unor instituții noi și nu produce impacturi structurale asupra sistemului administrației publice: rolul de autoritate națională de securitate revine Serviciului de Informații și Securitate, care exercită deja funcții în domeniu în temeiul cadrului actual.

Pentru entitățile publice care dețin sau gestionează informații clasificate, proiectul clarifică și sistematizează obligațiile existente: organizarea structurilor sau desemnarea funcționarilor de securitate, adoptarea normelor interne coordonate cu Serviciul, elaborarea nomenclatoarelor departamentale, ținerea evidenței autorizațiilor și a instruirilor, instituirea sistemelor de registre. Delimitarea clară a competențelor între Serviciu (verificarea de securitate și emiterea avizelor) și conducătorii entităților (autorizarea accesului) elimină incertitudinile din practica actuală și reduce riscul de aplicare neuniformă.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea prevederilor prezentului proiect de lege nu implică cheltuieli financiare suplimentare.

4.3. Impactul asupra sectorului privat
Nu este aplicabil.
4.4. Impactul social
Nu este aplicabil.
4.4.1. Impactul asupra protecției datelor cu caracter personal
Nu este aplicabil.
4.4.2. Impactul asupra echității și egalității de gen
Nu este aplicabil.
4.5. Impactul asupra mediului
Nu este aplicabil.
4.6. Alte impacturi și informații relevante
Nu este aplicabil.
5. Compatibilitatea proiectului cu legislația UE
5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională
Prezentul proiect stabilește cadrul național de aplicare a Deciziei 2013/488/UE Deciziei 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate. Decizia 2013/488/UE nu este un act supus transpunerii, ci un act al Consiliului care stabilește normele de securitate pentru protecția informațiilor UE clasificate, ale cărui dispoziții rezervă expres actelor cu putere de lege și normelor administrative ale statelor membre reglementarea unor materii esențiale. Prin urmare, proiectul stabilește cadrul național de aplicare cerut de art. 1 alin. (2), art. 7 alin. (4), art. 9 alin. (2), art. 10 alin. (8) și (9), art. 11 alin. (5) și (6), art. 15 alin. (3) și art. 16 alin. (3) din Decizie, cuprinzând desemnarea autorităților competente, procedurile administrative, sancțiunile și mecanismele de control, și preia în dreptul intern principiile de bază și standardele minime de securitate ale Deciziei. În temeiul pct. 15 din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația UE, aprobat prin Hotărârea Guvernului nr. 1171/2018, pentru

proiectele de acte normative cu relevanță UE care nu au ca scop transpunerea directă a legislației UE, dar urmăresc crearea cadrului juridic național necesar pentru implementarea legislației UE, nu este necesară întocmirea tabelului de concordanță.
5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE
Punerea în aplicare a legii presupune adoptarea, până la intrarea acesteia în vigoare, a actelor normative de executare: hotărârile Guvernului privind Nomenclatorul informațiilor clasificate, modelul chestionarului de securitate, securitatea fizică, protecția informațiilor în sistemele informatice și de comunicații, managementul informațiilor clasificate, securitatea industrială și partajarea informațiilor; actele normative departamentale ale Serviciului; regulamentele organelor de autoadministrare ale profesiilor juridice prevăzute la art. 22 alin. (7)–(9).
6. Avizarea și consultarea publică a proiectului
Inițierea elaborării prezentului proiect de lege a fost anunțată la 24 iulie 2025 (link). Propuneri sau recomandări nu au fost recepționate.
7. Modul de încorporare a actului în cadrul normativ existent
Adoptarea proiectului de lege va necesita modificarea cadrului normativ conex în corespundere cu noile prevederi.
8. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ
Punerea în aplicare a legii presupune adoptarea, până la intrarea acesteia în vigoare, a actelor normative de executare: hotărârile Guvernului privind Nomenclatorul informațiilor clasificate, modelul chestionarului de securitate, securitatea fizică, protecția informațiilor în sistemele informatice și de comunicații, managementul informațiilor clasificate, securitatea industrială și partajarea informațiilor; actele normative departamentale ale Serviciului; regulamentele organelor de autoadministrare ale profesiilor juridice prevăzute la art. 22 alin. (7)–(9).

Secretar de stat **Mihai GHEORGHIEȘ**