

L E G E

privind protecția informațiilor clasificate

Parlamentul adoptă prezenta lege organică.

Prezenta lege asigură aplicarea Deciziei 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate, publicată în Jurnalul Oficial al Uniunii Europene L 274/1 din 15 octombrie 2013, CELEX: 32013D0488, astfel cum a fost modificată ultima dată prin Decizia (UE) 2025/1540 a Consiliului din 18 iulie 2025, prin stabilirea cadrului național de aplicare a prevederilor 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 actul Uniunii Europene, cuprinzând desemnarea autorităților competente, procedurile administrative, sancțiunile și mecanismele de control.

Capitolul I

DISPOZIȚII GENERALE

Articolul 1. Obiectul și domeniul de aplicare

(1) Prezenta lege stabilește cadrul juridic cu privire la protecția informațiilor clasificate.

(2) Prezenta lege se aplică entităților care dețin sau gestionează informații clasificate, precum și persoanelor fizice care, în exercitarea atribuțiilor lor, accesează informații clasificate.

(3) Prezenta lege se aplică și informațiilor clasificate primite de Republica Moldova de la state străine sau organizații internaționale, în condițiile tratatelor internaționale la care Republica Moldova este parte sau ale acordurilor de securitate încheiate în conformitate cu prezenta lege.

(4) Capitolele III–VI se aplică în mod corespunzător și informațiilor UE clasificate, în corespundere cu Decizia 2013/488/UE a Consiliului.

Articolul 2. Noțiuni

În sensul prezentei legi, următoarele noțiuni semnifică:

informații clasificate – 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;

material – orice document, suport de date sau obiect de tip mașină sau echipament, fabricat sau în proces de fabricație;

document – orice informație înregistrată, indiferent de forma sau caracteristicile sale fizice;

clasificare – încadrarea informațiilor în unul dintre nivelurile de clasificare;

reducerea nivelului de clasificare – atribuirea unui nivel de clasificare inferior;

declasificare – eliminarea clasificării de securitate;

gestionarea informațiilor clasificate – toate acțiunile posibile la care informațiile clasificate pot fi supuse pe parcursul ciclului lor de viață. Aceasta cuprinde crearea, prelucrarea, transportul, reducerea nivelului de clasificare, declasificarea și distrugerea. În relație cu sistemele informatice și de comunicații, aceasta cuprinde, de asemenea, colectarea, afișarea, transmiterea și stocarea;

sistem informatic și de comunicații – orice sistem care permite gestionarea informațiilor în format electronic, care cuprinde toate resursele necesare funcționării sale, inclusiv infrastructura, organizarea, personalul și resursele informaționale;

entitate publică – autoritate publică; instituție publică; întreprindere de stat sau întreprindere municipală; societate comercială cu capital integral sau majoritar de stat.

entitate industrială sau de altă natură – orice persoană fizică sau juridică care furnizează bunuri, execută lucrări sau prestează servicii;

emitent – entitatea publică, statul sau organizația internațională sub a cărei autoritate au fost create și/sau introduse în Republica Moldova informațiile clasificate;

deținător – o persoană fizică autorizată corespunzător, căreia i s-a stabilit necesitatea de a cunoaște, care se află în posesia unei informații clasificate și, în consecință, răspunde de protecția acesteia;

contractant – o persoană fizică sau juridică care are capacitatea juridică de a încheia contracte;

contract clasificat – un contract încheiat de o entitate publică cu un contractant pentru furnizarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la informații clasificate sau crearea acestora;

subcontract clasificat – un contract încheiat de un contractant al entității publice cu un alt contractant (subcontractantul) pentru furnizarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la informații clasificate sau crearea acestora.

Capitolul II

CLASIFICAREA INFORMAȚIILOR

Articolul 3. Categoriile informațiilor clasificate

(1) Pot fi clasificate, în condițiile prezentei legi, numai informațiile a căror divulgare neautorizată poate cauza un prejudiciu real și identificabil securității naționale a Republicii Moldova și care se încadrează în una dintre următoarele categorii:

a) în domeniul apărării naționale:

1) conținutul planurilor strategice și operative, al documentelor ce țin de conducerea operațiunilor de luptă privind pregătirea și derularea operațiunilor, desfășurarea strategică, operativă și de mobilizare a trupelor, alți indicatori importanți ce caracterizează organizarea, efectivul, dislocarea, pregătirea de luptă și de mobilizare, armamentul și asigurarea tehnico-materială a Forțelor Armate ale Republicii Moldova;

2) direcțiile de dezvoltare a unor tipuri de armament, de tehnică militară și specială, cantitatea și caracteristicile lor tehnico-tactice, organizarea și tehnologiile de producere, lucrările științifice teoretice și experimentale legate de crearea modelelor noi de armament, tehnică militară și specială sau modernizarea acestora, alte lucrări planificate sau efectuate în interesele apărării naționale;

3) forțele și mijloacele protecției civile, capacitățile de care dispun localitățile și unele obiective separate pentru protecția, evacuarea și dispersarea populației, asigurarea activităților sociale vitale ale populației și a activității de producere a persoanelor juridice în perioada de război, de asediu sau de urgență, precum și în cazul situațiilor excepționale;

4) dislocarea, destinația, gradul de pregătire și de securitate a obiectivelor cu regim special, proiectarea, construirea și exploatarea acestora, repartizarea terenului, subsolului și acvatoriului pentru asemenea obiective;

5) datele și caracteristicile geodezice, gravimetrice, cartografice și hidrometeorologice care prezintă importanță pentru apărarea statului;

b) în domeniul capacității de apărare și mobilizare a statului:

1) planurile și potențialul de mobilizare a economiei naționale, rezervele și volumul livrărilor de materiale strategice, datele generalizate despre nomenclatura și nivelul stocurilor, volumul livrărilor, alocării, depunerii și împrăștiării acestora;

2) informațiile din Nomenclatorul bunurilor materiale din rezervele de stat și Nomenclatorul bunurilor materiale din rezervele de mobilizare;

3) informațiile generalizate privind disponibilul și circulația bunurilor materiale din rezervele de stat;

4) informațiile generalizate privind disponibilul, amplasarea și circulația bunurilor materiale din rezervele de mobilizare;

5) utilizarea transporturilor, comunicațiilor, a potențialului altor ramuri și obiective ale infrastructurii naționale în scopul asigurării capacității de apărare și a securității statului;

6) planurile, conținutul, volumul, finanțarea și îndeplinirea comenzilor de stat pentru asigurarea securității statului și a necesităților sale de apărare;

7) planurile, volumul și alte caracteristici importante privind extragerea, producerea și realizarea unor tipuri strategice de materie primă și produse;

8) operațiunile ce țin de confecționarea semnelor bănești și a titlurilor de valoare emise de stat, păstrarea și protecția lor contra falsificării, emiterea, schimbul și retragerea lor din circulație;

9) lucrările științifice teoretice, experimentale de construcții și proiectare, în baza cărora pot fi create tehnologii avansate, tipuri noi de producție, produse și procese tehnologice, care prezintă importanță pentru securitatea națională sau o influențează esențial;

c) în domeniul relațiilor externe:

1) activitatea de politică externă, relațiile economice externe ale Republicii Moldova, a căror divulgare prematură poate cauza prejudicii securității naționale;

2) colaborarea militară, tehnico-științifică și de altă natură a Republicii Moldova cu statele străine și organizațiile internaționale, dacă divulgarea acestor informații poate cauza prejudicii securității naționale;

3) activitatea externă a statului în domeniile financiar, creditar și valutar, dacă divulgarea acestor informații poate cauza prejudicii securității naționale;

d) în domeniul securității statului și asigurării ordinii de drept:

1) efectivul, forțele, conținutul, planurile, organizarea, finanțarea și asigurarea tehnico-materială, formele, tactica, metodele, mijloacele și rezultatele activității contrainformative și activității informative externe;

2) efectivul, forțele, conținutul, planurile, organizarea, finanțarea și asigurarea tehnico-materială, formele, tactica, metodele și mijloacele activității speciale de investigații și a testării integrității profesionale, cu excepția rezultatelor măsurilor speciale de investigații și a datelor din raportul privind rezultatele evaluării integrității instituționale;

3) persoanele care colaborează sau au colaborat confidențial cu organele care desfășoară activitate contrainformativă, activitate informativă externă sau activitate specială de investigații;

4) forțele, mijloacele și metodele de asigurare a protecției de stat părții vătămate, martorilor și altor persoane care acordă ajutor în procesul penal;

5) paza frontierei de stat a Republicii Moldova;

6) planurile, organizarea, finanțarea, efectivul, forțele, mijloacele și metodele de asigurare a securității persoanelor beneficiare de protecție de stat, precum și paza sediilor de lucru și a reședințelor acestora;

7) sistemele de telecomunicații guvernamentale și alte tipuri de rețele de telecomunicații electronice care asigură necesitățile autorităților publice, apărării naționale, securității statului și menținerii ordinii publice;

8) organizarea, conținutul, starea și planurile de dezvoltare a protecției criptografice și tehnice a informațiilor clasificate, conținutul și rezultatele cercetărilor științifice în domeniul criptografiei referitor la protecția informațiilor clasificate;

9) sistemele și mijloacele de protecție criptografică a informațiilor clasificate, proiectarea, producerea, tehnologiile de producere și utilizarea acestora;

10) cifrurile de stat, elaborarea, crearea, tehnologiile de producere și utilizarea acestora;

11) organizarea regimului de protecție a informațiilor clasificate în cadrul entităților publice și al altor entități, planurile și măsurile în domeniul protecției informațiilor clasificate;

12) alte metode, forme și mijloace de protecție a informațiilor clasificate.

(2) Informațiile sunt clasificate numai dacă prejudiciul care poate fi cauzat securității naționale prin divulgarea informației prevalează în raport cu interesul public în accesarea acesteia.

Articolul 4. Informațiile care nu pot fi clasificate

Nu pot fi clasificate informațiile privind:

- a) încălcările drepturilor și libertăților omului;
- b) starea mediului înconjurător, calitatea produselor alimentare și a obiectelor de uz casnic;
- c) accidentele, catastrofele, fenomenele naturale periculoase și alte evenimente care pot afecta ordinea și securitatea publică;
- d) starea sănătății populației, nivelul ei de trai, inclusiv alimentația, asistența medicală și asigurarea socială, indicatorii socio-demografici;
- e) faptele de încălcare a legii de către entitățile publice și persoanele cu funcții de răspundere din cadrul acestora;
- f) starea reală de lucruri în domeniile învățământului, culturii, comerțului, agriculturii și ordinii de drept.

Articolul 5. Clasificările de securitate

(1) Informațiile prevăzute la art. 3 sunt clasificate la unul dintre următoarele niveluri:

a) „Strict secret” – pentru informațiile și materialele a căror divulgare neautorizată poate cauza prejudicii deosebit de grave securității naționale a Republicii Moldova;

b) „Secret” – pentru informațiile și materialele a căror divulgare neautorizată poate cauza prejudicii grave securității naționale a Republicii Moldova;

c) „Confidențial” – pentru informațiile și materialele a căror divulgare neautorizată poate cauza prejudicii securității naționale a Republicii Moldova;

d) „Restricționat” – pentru informațiile și materialele a căror divulgare neautorizată poate fi în defavoarea securității naționale a Republicii Moldova;

(2) Informațiile clasificate sunt marcate cu un marcaj de clasificare, în conformitate cu alin. (1). Acestea pot avea marcaje suplimentare care indică domeniul de activitate la care se referă, identifică emitentul, limitează distribuirea, restrâng utilizarea sau precizează dacă pot fi comunicate.

Articolul 6. Gestionarea clasificărilor

(1) Emitenții trebuie să asigure că informațiile clasificate sunt clasificate corespunzător, identificate în mod clar ca informații clasificate și că nivelul de clasificare al acestora este menținut doar atât timp cât este necesar.

(2) Un volum total de informații clasificate poate justifica un nivel de protecție corespunzător unei clasificări superioare celei a elementelor sale individuale.

(3) Informațiile clasificate nu sunt supuse reducerii nivelului de clasificare sau declasificate și niciun marcaj menționat la art. 5 alin. (2) nu este modificat sau eliminat fără acordul prealabil scris al emitentului.

(4) În scopul promovării unei politici de stat unice în domeniul clasificării informațiilor, Guvernul aprobă Nomenclatorul informațiilor clasificate, în care sunt incluse și entitățile publice cu împuterniciri de dispoziție asupra acestor informații.

(5) În baza și în limitele Nomenclatorului informațiilor clasificate și în scopul concretizării și sistematizării informațiilor în domeniile lor de activitate, entitățile publice elaborează nomenclatoare departamentale de informații care urmează a fi clasificate.

(6) Nomenclatoarele departamentale de informații care urmează a fi clasificate conțin informațiile asupra cărora au împuterniciri de dispoziție entitățile publice în cauză, în acestea stabilindu-se nivelurile și termenele de clasificare a informațiilor.

(7) Nomenclatoarele departamentale de informații care urmează a fi clasificate se aprobă de către conducătorii entităților publice, după coordonarea cu Serviciul de Informații și Securitate al Republicii Moldova (în continuare – *Serviciu*), și nu sunt date publicității. Un exemplar al nomenclatoarelor

departamentale de informații care urmează a fi secretizate se transmite pentru înregistrare Serviciului de Informații și Securitate.

(8) Conducătorii entităților publice sunt obligați să reevalueze periodic, cel puțin o dată la 5 ani, conținutul nomenclatoarelor departamentale de informații care urmează a fi clasificate în vederea stabilirii necesității clasificării informațiilor, corespunderea nivelurilor de clasificare, precum și necesitatea menținerii termenelor de clasificare stabiliți anterior.

Articolul 7. Termenele de clasificare a informațiilor

(1) Durata maximă a clasificării este:

- a) 25 de ani pentru informațiile clasificate „Strict secret”;
- b) 15 ani pentru informațiile clasificate „Secret”;
- c) 10 ani pentru informațiile clasificate „Confidențial”;
- d) 5 ani pentru informațiile clasificate „Restricționat”.

(2) Durata clasificării curge de la data la care a fost aplicat marcajul de clasificare.

(3) Emitentul poate prelungi durata clasificării înainte de expirarea acesteia dacă circumstanțele care au justificat clasificarea inițială persistă și prelungirea este necesară pentru protecția securității naționale. Prelungirea se decide motivat și nu poate depăși jumătate din durata inițială.

(4) Prin derogare de la alin. (1), informațiile privind persoanele care colaborează sau au colaborat confidențial cu organele care desfășoară activitate contrainformativă, activitate informativă externă sau activitate specială de investigații se clasifică pe durată nedeterminată.

Articolul 8. Declassificarea

(1) Informațiile sunt declassificate în următoarele cazuri:

- a) expirarea termenului de clasificare a informațiilor;
- b) schimbarea circumstanțelor obiective, ca urmare a căreia protecția ulterioară a anumitor informații atribuite la informații clasificate nu mai este justificată;
- c) modificarea categoriilor de informații prevăzute la art. 3 sau 4;
- d) existența unei decizii care constată drept neîntemeiată clasificarea informațiilor.

(2) Declassificarea informațiilor se efectuează de emitenți sau cu acordul scris al emitenților.

(3) Serviciul poate emite decizii cu privire la declassificarea informațiilor care au fost clasificate neîntemeiat de entitățile publice.

(4) Conducătorii arhivelor de stat sunt împuterniciți să declassifice informațiile care se păstrează în fondurile închise ale arhivelor, cu condiția că organizația întemeietoare a fondului sau succesorul ei de drept le delegă astfel de împuterniciri. În caz de lichidare a organizației întemeietoare a fondului și de lipsă a succesorului ei de drept, chestiunea declassificării este examinată de Serviciu.

Articolul 9. Contestarea clasificării

Orice persoană fizică sau juridică poate contesta clasificarea informațiilor în conformitate cu prevederile Codului administrativ nr. 116/2018.

Capitolul III SECURITATEA INFORMAȚIILOR CLASIFICATE

Secțiunea 1 Dispoziții generale

Articolul 10. Protecția informațiilor clasificate

(1) Deținătorul oricărei informații clasificate este responsabil de protecția acesteia, în conformitate cu prezenta lege și alte acte normative.

(2) Entitățile publice și entitățile industriale sau de altă natură asigură protecția informațiilor clasificate recepționate de la alte state sau organizațiile internaționale, în conformitate cu marcajul de clasificare echivalent și cu cerințele aplicabile informațiilor clasificate de nivel echivalent, potrivit acordurilor internaționale.

Articolul 11. Procesul de gestionare a riscului de securitate

(1) Riscul la adresa informațiilor clasificate este gestionat ca un proces care urmărește determinarea riscurilor de securitate cunoscute, definirea măsurilor de securitate destinate reducerii acestor riscuri la un nivel acceptabil, în conformitate cu principiile și standardele minime stabilite de prezenta lege și de alte acte normative, precum și aplicarea acestor măsuri în conformitate cu conceptul apărării în profunzime. Eficacitatea măsurilor este evaluată permanent.

(2) Măsurile de securitate pentru protecția informațiilor clasificate pe durata ciclului de viață al acestora sunt proporționale, în special, cu clasificarea de securitate, cu forma și volumul informațiilor sau al materialelor, cu amplasarea și construcția obiectivelor care adăpostesc informații clasificate, precum și cu evaluarea locală a amenințării reprezentate de activități rău-intenționate și/sau infracționale, inclusiv spionaj, diversiune și terorism. Fiecare entitate publică și entitate industrială sau de altă natură care deține sau gestionează informații

clasificate stabilește și aplică aceste măsuri în conformitate cu rezultatul evaluării riscurilor, în condițiile stabilite de prezenta lege și de actele normative.

(3) Măsurile de prevenire și de recuperare destinate minimizării impactului erorilor sau al incidentelor majore survenite în gestionarea și păstrarea informațiilor clasificate se integrează în Programul de prevenire a scurgerii informațiilor clasificate, întocmit în modul stabilit de Guvern.

(4) Procedurile de protecție și, după caz, de evacuare a informațiilor clasificate în situații de urgență, destinate împiedicării accesului neautorizat, divulgării neautorizate sau pierderii integrității ori a disponibilității acestora, se stabilesc în Planul de urgență, întocmit potrivit actelor normative.

(5) Entitățile prevăzute la alin. (2) sunt obligate să elaboreze documentele prevăzute la alin. (3) și (4), să le coordoneze cu Serviciul și să asigure aplicarea acestora.

Articolul 12. Încălări ale securității și compromiterea informațiilor clasificate

(1) O încălcare a securității are loc în urma unei acțiuni sau inacțiuni a unei persoane care contravine normelor de securitate stabilite de legislația privind protecția informațiilor clasificate.

(2) Compromiterea informațiilor clasificate are loc atunci când, în urma unei încălcări a securității, acestea au fost divulgate, integral sau parțial, unor persoane neautorizate.

(3) Orice încălcare sau suspiciune de încălcare a securității este raportată imediat Serviciului.

(4) În cazul în care se cunoaște sau există motive întemeiate să se presupună că informațiile clasificate au fost compromise, entitatea ia toate măsurile corespunzătoare pentru:

- a) a informa emitentul;
- b) a asigura investigarea cazului de persoane care nu sunt implicate în mod direct în încălcarea securității, în vederea stabilirii faptelor;
- c) a evalua eventualele prejudicii aduse securității naționale;
- d) a lua măsurile adecvate pentru a împiedica repetarea situației;
- e) a notifica Serviciul și, după caz, autoritatea publică ierarhic superioară cu privire la măsurile întreprinse.

(5) Orice persoană responsabilă de încălcarea normelor de securitate prevăzute de legislația privind protecția informațiilor clasificate sau de compromiterea ori pierderea informațiilor clasificate este pasibilă de răspundere disciplinară, contravențională sau penală.

Secțiunea a 2-a

Securitatea personalului

Subsecțiunea 1

Dispoziții generale

Articolul 13. Securitatea personalului

(1) Securitatea personalului constă în aplicarea unor măsuri care să garanteze că accesul la informații clasificate este acordat numai persoanelor care:

- a) au necesitatea de a cunoaște;
- b) dețin, în cazurile prevăzute de prezenta lege, un aviz de securitate a personalului de nivel corespunzător și o autorizație de acces la informații clasificate;
- c) au fost instruite cu privire la responsabilitățile care le revin.

(2) Avizul de securitate a personalului confirmă rezultatul verificării de securitate și nu conferă, prin el însuși, dreptul de acces la informații clasificate. Accesul se acordă numai în temeiul autorizației de acces la informații clasificate, emisă în condițiile prezentei legi, cu respectarea principiului necesității de a cunoaște.

Subsecțiunea a 2-a

Acordarea accesului la informații clasificate

Articolul 14. Condițiile de acordare a accesului la informații clasificate

Accesul la informații clasificate se acordă persoanei care a împlinit vârsta de 18 ani, numai după parcurgerea următoarelor etape:

- a) a fost stabilită necesitatea de a cunoaște a persoanei, în virtutea funcției sau în legătură cu studiile ori cu locul desfășurării activității legate de informațiile clasificate;
- b) persoana a fost instruită cu privire la normele și procedurile de securitate pentru protecția informațiilor clasificate și a confirmat în scris că a luat cunoștință de responsabilitățile care îi revin în ceea ce privește protecția acestor informații;
- c) în cazul informațiilor clasificate la nivelul „Confidențial” sau la un nivel superior, persoanei i s-a acordat, înainte de a i se permite accesul, un aviz de securitate a personalului de nivel corespunzător și i-a fost autorizat accesul pentru nivelul relevant ori persoana a fost autorizată în alt mod, prin natura funcțiilor deținute, în conformitate cu actele normative.

Articolul 15. Lista funcțiilor care necesită acces la informații clasificate

(1) Fiecare entitate publică aprobă, după coordonare cu Serviciul, lista funcțiilor care necesită acces la informații clasificate. Cerința de a lucra cu informații clasificate se stabilește în fișa postului.

(2) Pot ocupa funcții care necesită acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior doar persoanele care dețin un aviz de securitate a personalului valabil, corespunzător nivelului de acces.

Subsecțiunea a 3-a
Avizul de securitate a personalului

Articolul 16. Avizul de securitate a personalului

(1) Evaluarea și emiterea avizului de securitate a personalului se efectuează de către Serviciu, în conformitate cu prezenta lege și cu alte acte normative, pentru a stabili dacă o persoană poate avea acces la informații clasificate, ținându-se seama de loialitatea și onestitatea acesteia și de încrederea pe care o inspiră.

(2) Avizul de securitate a personalului se acordă cetățenilor Republicii Moldova. Accesul cetățenilor străini și al apatrizilor la informații clasificate se acordă în condițiile art. 23 alin. (6) și (7).

(3) Persoanele ale căror atribuții de serviciu necesită accesul la informații clasificate de nivelul „Confidențial” sau superior ori gestionarea acestora obțin avizul de securitate a personalului pentru nivelul corespunzător înainte de a li se acorda acces la respectivele informații.

(4) Serviciului, la solicitarea entităților publice, îi revine responsabilitatea de a asigura că toate persoanele cărora trebuie să li se acorde acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior sunt supuse verificării de securitate.

(5) La solicitarea autorităților naționale de securitate ale statelor cu care Republica Moldova a încheiat acorduri în domeniul protecției reciproce a informațiilor clasificate sau a organizațiilor internaționale, Serviciul efectuează verificări de securitate în privința cetățenilor Republicii Moldova și a cetățenilor străini cu reședința în Republica Moldova care solicită acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior în statele sau în organizațiile respective, în conformitate cu standardele naționale de verificare.

(6) Pentru persoanele care au avut sau au reședința pe teritoriul unui alt stat, Serviciul solicită asistența autorității competente din statul de reședință, în conformitate cu tratatele internaționale la care Republica Moldova este parte.

Articolul 17. Verificarea de securitate

(1) Efectuarea verificării de securitate necesită completarea și semnarea, de către candidatul la funcția care implică acces la informații clasificate ori de către titularul acesteia, a chestionarului de securitate.

(2) În funcție de nivelul de clasificare a informațiilor pentru care se solicită avizul de securitate a personalului, termenele verificării de securitate sunt:

a) pentru acces la informații de nivelul „Secret” și „Strict secret” – până la 90 de zile lucrătoare;

b) pentru acces la informații de nivelul „Confidențial” – până la 60 de zile lucrătoare.

(3) Dacă în cursul verificării de securitate, pentru orice nivel, apar informații care evidențiază riscuri de securitate și care necesită verificări suplimentare, termenul de verificare poate fi prelungit cu o perioadă determinată în mod rezonabil, care nu poate depăși 6 luni.

(4) După evaluarea pozitivă a rezultatelor verificării de securitate, Serviciul eliberează avizul de securitate a personalului de nivel corespunzător și îl remite entității publice inițiatoare.

(5) În cazul în care informațiile acumulate în cadrul verificării de securitate denotă prezența unuia dintre temeiurile prevăzute la art. 18, Serviciul refuză eliberarea avizului de securitate a personalului și notifică entitatea inițiatoare printr-o concluzie privind imposibilitatea emiterii avizului de securitate a personalului, care cuprinde temeiul și esența motivelor refuzului.

(6) Concluzia Serviciului, emisă în condițiile alin. (5), este executorie pentru persoanele cu funcții de răspundere din cadrul entității publice, însă nu exclude înaintarea unei solicitări repetate în cazul înlăturării împrejurărilor care au făcut imposibilă acordarea avizului de securitate a personalului, dar nu mai devreme de 12 luni de la data emiterii concluziei respective.

(7) Verificarea de securitate poate fi suspendată, în funcție de relevanța pentru evaluarea de securitate, în următoarele cazuri:

a) subiectul verificării suferă de o boală care necesită un tratament cu o durată mai mare de 30 de zile și care face imposibilă efectuarea eficientă a verificării;

b) subiectul verificării pleacă în străinătate pentru o perioadă mai mare de 30 de zile;

c) aprecierea persoanei sub aspectul loialității, onestității și încrederii depinde de soluționarea prealabilă a unei chestiuni de către o altă autoritate publică, inclusiv de soluționarea definitivă a unei cauze penale în care subiectul verificării are calitatea de bănuț, învinuit sau inculpat;

d) desfășurarea efectivă a verificării de securitate nu este posibilă din alte motive care nu depind de Serviciu.

(8) Verificarea de securitate se reia dacă au dispărut motivele care au justificat suspendarea.

(9) Serviciul notifică entitatea publică despre suspendarea sau reluarea verificării de securitate.

(10) Verificarea de securitate încetează în următoarele cazuri:

- a) decesul subiectului verificării;
- b) subiectul verificării refuză funcția pentru care a fost inițiată verificarea;
- c) entitatea publică își retrace intenția de a numi persoana verificată în funcția care necesită acces la informații clasificate sau de a-i încredința lucrări ce implică accesul la informații clasificate.

(11) Serviciul este abilitat să solicite și să primească informații de la entitățile publice și de la entitățile industriale sau de altă natură, în vederea efectuării verificării de securitate și a eliberării avizului de securitate a personalului. Entitățile publice și entitățile industriale sau de altă natură sunt obligate să furnizeze informațiile solicitate de Serviciu în termen de cel mult 15 zile lucrătoare.

Articolul 18. Criteriile verificării de securitate

(1) Loialitatea, onestitatea și încrederea inspirată de o persoană, în scopul avizării de securitate pentru accesul la informații clasificate la nivelul „Confidențial” sau la un nivel superior, se stabilesc prin intermediul verificării de securitate.

(2) Serviciul efectuează o evaluare generală în baza verificării de securitate. Principalele criterii utilizate în acest scop includ stabilirea faptului dacă persoana:

a) a comis sau a intenționat să comită, a fost complice, a ajutat ori a instigat o altă persoană să comită acte de spionaj, terorism, diversiune, separatism, trădare de Patrie sau rebeliune armată;

b) este sau a fost asociată cu persoane care au comis ori care sunt suspectate, pe baza unor motive întemeiate, că au comis faptele prevăzute la lit. a) ori cu reprezentanți ai unor organizații ale altor state, inclusiv ai serviciilor speciale, sau ai unor structuri separatiste, care pot amenința securitatea Republicii Moldova, cu excepția cazurilor în care asemenea asocieri au fost autorizate pentru îndeplinirea unor atribuții oficiale;

c) este sau a fost membră a unei organizații care urmărește, prin mijloace violente, subversive ori prin alte mijloace ilegale, răsturnarea sau subminarea ordinii constituționale, violarea integrității teritoriale a Republicii Moldova ori înlăturarea prin asemenea mijloace a autorităților legal constituite;

d) sprijinirii de către acesta a activității unui stat străin, a unei organizații străine sau a reprezentanților acestora, precum și a unor cetățeni străini sau apatrizi ce cauzează prejudicii intereselor și/sau securității Republicii Moldova sau în cazul

participării cetățeanului la activitatea unor partide sau asociații obștești a căror activitate este suspendată, limitată sau interzisă în modul stabilit de lege;

e) este sau a fost susținătoare a unei organizații prevăzute la lit. c) ori se află sau s-a aflat recent în relații apropiate cu membri ai unei asemenea organizații;

f) descoperirii, în urma măsurilor de verificare, a altor acțiuni ale acestuia care prezintă pericol pentru securitatea națională a Republicii Moldova.

g) a ascuns, a denaturat sau a falsificat în mod deliberat informații relevante, în special referitoare la securitate, ori a mințit cu bună știință la completarea chestionarului de securitate sau în timpul interviului de securitate;

h) a fost condamnată, printr-o hotărâre judecătorească definitivă, pentru o infracțiune contra păcii și securității omenirii, infracțiune de război, infracțiune contra securității publice și a ordinii publice, infracțiune contra autorităților publice și a securității de stat, infracțiune contra bunei desfășurări a activității în sfera publică, infracțiune contra justiției ori pentru o altă infracțiune săvârșită cu intenție care o face incompatibilă cu accesul la informații clasificate;

i) capacitatea sa de exercițiu a fost limitată prin hotărâre judecătorească;

j) are un istoric de dependență de alcool ori de consum de substanțe stupefiante, psihotrope și/sau de alte substanțe cu efecte similare care produc dependență;

k) manifestă sau a manifestat comportamente care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni;

l) prin fapte sau limbaj, a demonstrat lipsă de onestitate ori de loialitate sau incapacitatea de a inspira încredere;

m) a încălcat în mod grav sau repetat normele de protecție a informațiilor clasificate;

n) poate fi expusă la presiuni, de exemplu în virtutea deținerii uneia sau mai multor cetățenii ale altor state ori prin intermediul unor rude sau asociați apropiați vulnerabili față de servicii speciale străine, grupări teroriste ori alte organizații sau persoane ale căror interese sunt ostile Republicii Moldova;

o) suferă sau a suferit de o afecțiune fizică sau psihică ce îi poate afecta discernământul ori capacitatea de a proteja informațiile clasificate, confirmată printr-o investigație medicală efectuată cu acordul persoanei;

p) a încercat ori a reușit să desfășoare o activitate neautorizată legată de sistemele informatice și de comunicații.

(3) Suplimentar criteriilor indicate la alin. (2), pentru acordarea avizului de securitate a personalului pentru nivelul „Secret” sau „Strict secret” se verifică următoarele aspecte:

a) situația financiară – se caută informații privind situația financiară a persoanei, pentru a evalua orice vulnerabilitate la presiuni străine sau naționale cauzate de dificultăți financiare grave ori pentru a descoperi averi nejustificate;

b) educația – se verifică parcursul educațional al persoanei la școlile, universitățile și alte instituții de învățământ frecventate de la împlinirea vârstei de 18 ani ori pentru o perioadă considerată oportună de Serviciu;

c) situația profesională – se verifică situația profesională prezentă și trecută, consultându-se surse precum evidențele privind angajarea în muncă, rapoartele de performanță și de eficiență, precum și angajatorii și autoritățile de supraveghere;

d) serviciul militar – după caz, se verifică serviciul persoanei în cadrul forțelor armate și statutul cu care a fost eliberată din serviciul militar;

e) interviurile – au loc unul sau mai multe interviuri cu persoana în cauză, precum și cu alte persoane care pot oferi o evaluare nepărtinitoare a mediului, activităților, loialității, onestității și gradului de încredere inspirate de persoana evaluată. La solicitarea Serviciului, subiectul verificării furnizează referințe; persoanele indicate ca referințe sunt intervievate, cu excepția cazului în care există motive întemeiate pentru a nu proceda astfel.

(4) În cadrul verificării de securitate pot fi luate în considerare, în măsura în care sunt relevante pentru criteriile prevăzute la alin. (2), conduita și împrejurările de viață ale soțului/soției ori ale concubinului/concubinei subiectului verificării.

Articolul 19. Avizul de securitate a personalului inițial

(1) Avizul de securitate a personalului inițial pentru accesul la informații clasificate „Confidențial” se bazează pe verificarea de securitate care acoperă cel puțin ultimii 5 ani sau perioada cuprinsă între împlinirea vârstei de 18 ani și prezent, în funcție de care dintre aceste perioade este mai scurtă.

(2) Avizul de securitate a personalului inițial pentru accesul la informații clasificate „Secret” se bazează pe verificarea de securitate care acoperă cel puțin ultimii 7 ani sau perioada cuprinsă între împlinirea vârstei de 18 ani și prezent, în funcție de care dintre aceste perioade este mai scurtă.

(3) Avizul de securitate a personalului inițial pentru accesul la informații clasificate „Strict secret” se bazează pe verificarea de securitate care acoperă cel puțin ultimii 10 ani sau perioada cuprinsă între împlinirea vârstei de 18 ani și prezent, în funcție de care dintre aceste perioade este mai scurtă.

(4) Valabilitatea avizului de securitate a personalului pentru accesul la informații clasificate de nivelul „Confidențial” sau superior este de 5 ani de la data emiterii acestuia în condițiile art. 17 alin. (4). În această perioadă, reverificarea poate fi inițiată oricând, în condițiile art. 20 alin. (3).

Articolul 20. Revalidarea avizului de securitate a personalului

(1) Revalidarea avizului de securitate a personalului presupune reverificarea persoanei deținătoare a unui aviz de securitate a personalului care a lucrat neîntrerupt și necesită acces permanent la informații clasificate.

(2) Reverificarea persoanei și eliberarea unui nou aviz de securitate a personalului pot avea loc la solicitarea entității publice în cadrul căreia persoana își desfășoară activitatea, în următoarele cazuri:

a) înainte de expirarea perioadei de valabilitate a avizului de securitate a personalului deținut anterior, în conformitate cu alin. (5);

b) la apariția necesității de autorizare a accesului la informații clasificate de nivel superior.

(3) Reverificarea fără eliberarea unui nou aviz de securitate a personalului se efectuează în scopul menținerii sau al retragerii avizului de securitate a personalului existent și poate avea loc la solicitarea entității publice în cadrul căreia persoana își desfășoară activitatea și/sau la inițiativa Serviciului, dacă pe parcursul perioadei de valabilitate a avizului apar indicii clare sau suspiciuni rezonabile cu privire la existența unor riscuri de securitate.

(4) Verificările de securitate destinate revalidării acoperă doar perioada scursă de la verificarea anterioară. Prevederile art. 17 și 18 se aplică în mod corespunzător.

(5) Cererile de revalidare în temeiul alin. (2) lit. a) se înaintează Serviciului cu cel puțin 3 luni înainte de expirarea termenului de valabilitate a avizului de securitate a personalului.

(6) În cazul în care cererea de revalidare și chestionarul de securitate au fost depuse în termenul prevăzut la alin. (5), iar verificarea de securitate nu a fost finalizată până la expirarea avizului de securitate a personalului, Serviciul poate prelungi valabilitatea avizului existent cu cel mult 6 luni. Dacă la expirarea acestui termen verificarea nu a fost finalizată, persoanei îi sunt încredințate atribuții care nu necesită acces la informații clasificate.

Subsecțiunea a 4-a

Autorizația de acces la informații clasificate

Articolul 21. Acțiunile entității publice aferente autorizării accesului

(1) În vederea autorizării accesului la informații clasificate, entitatea publică:

a) pune la dispoziția candidatului la funcția care implică acces la informații clasificate ori a titularului acesteia chestionarul de securitate, pentru completare. Modelul chestionarului de securitate și instrucțiunea privind completarea acestuia se aprobă de Guvern;

b) după recepționarea chestionarului de securitate completat, verifică corectitudinea întocmirii acestuia și îl clasifică la nivelul „Restrictionat”;

c) solicită acordul scris al candidatului/titularului pentru efectuarea verificării de securitate, în forma standard stabilită de actele normative.

(2) Entitatea publică înaintează Serviciului solicitarea motivată privind inițierea verificării de securitate pentru nivelul de clasificare solicitat, împreună cu actele menționate la alin. (1) lit. b) și c).

(3) În cazul în care entitatea publică intră în posesia unor informații relevante pentru verificarea de securitate referitoare la persoana supusă verificării, aceasta notifică Serviciul, la orice etapă a procesului de verificare.

(4) Entitatea publică notifică imediat Serviciul ori de câte ori intră în posesia unor informații relevante pentru securitate referitoare la o persoană care deține un aviz de securitate a personalului, în vederea aplicării prevederilor art. 20 alin. (3).

Articolul 22. Deciziile privind autorizarea accesului la informații clasificate

(1) Decizia privind autorizarea accesului la informații clasificate se ia de conducătorul entității cu drept de numire în funcție a persoanei, prin emiterea autorizației de acces la informații clasificate până la un nivel specificat și până la o dată precisă, care nu poate depăși termenul de valabilitate a avizului de securitate a personalului. Decizia se adoptă în termen de 10 zile de la recepționarea avizului de securitate a personalului emis în corespundere cu art. 17 alin. (4).

(2) În cazul în care Serviciul a refuzat eliberarea avizului de securitate a personalului în condițiile art. 17 alin. (5), entitatea publică comunică persoanei vizate acest fapt, inclusiv temeiul și esența motivelor refuzului, și nu emite autorizația de acces la informații clasificate. Persoana vizată poate solicita Serviciului reexaminarea concluziei și poate contesta refuzul în condițiile alin. (12).

(3) Prin derogare de la alin. (1), autorizația de acces la informații clasificate de nivelul „Restrictionat” se acordă de conducătorul entității cu drept de numire în funcție a persoanei, fără aviz de securitate a personalului, pe baza rezultatului verificării interne care include cel puțin verificarea cazierului judiciar.

(4) Dacă necesitatea accesului la informații clasificate nu este legată de locul de muncă, de serviciu ori de studii, autorizația de acces la informații clasificate poate fi emisă la locul desfășurării activității legate de informațiile clasificate, de către conducătorul entității beneficiare a lucrărilor legate de informațiile clasificate ori de către conducătorul entității unde se desfășoară activitatea respectivă, în condiții generale.

(5) Personalul contractanților și al subcontractanților obține autorizația de acces la informații clasificate conform prevederilor de securitate din contractul

clasificat, cu respectarea cerințelor stabilite de prezenta lege și de alte acte normative.

(6) Despre orice angajare într-o funcție care implică acces la informații clasificate și despre emiterea autorizației de acces la informații clasificate până la un nivel specificat și până la o anumită dată, entitatea publică informează Serviciul în termen de 10 zile lucrătoare. Despre suspendarea accesului la informații clasificate sau despre retragerea autorizației de acces la informații clasificate, entitatea publică informează Serviciul și persoana vizată în termen de 3 zile lucrătoare, persoana vizată având dreptul să solicite să fie audiată de entitatea publică.

(7) Consiliul Uniunii Avocaților autorizează accesul avocaților la informații clasificate în conformitate cu prezenta lege și cu propriul regulament, care se coordonează cu Serviciul.

(8) Consiliul Camerei Notariale autorizează accesul notarilor la informații clasificate în conformitate cu prezenta lege și cu propriul regulament, care se coordonează cu Serviciul.

(9) Consiliul Uniunii Naționale a Executorilor Judecătorești autorizează accesul executorilor judecătorești la informații clasificate în conformitate cu prezenta lege și cu propriul regulament, care se coordonează cu Serviciul.

(10) În cadrul procedurilor administrative privind avizarea de securitate și autorizarea accesului la informații clasificate, actele administrative, acțiunile sau inacțiunile entităților publice și ale Serviciului pot fi contestate în conformitate cu prevederile Codului administrativ al Republicii Moldova nr. 116/2018.

Articolul 23. Certificarea avizului de securitate a personalului

(1) În cazul intenției de angajare sau de transfer în cadrul altei entități publice ori al detașării în cadrul altei entități publice, inclusiv în alte state, misiuni sau organizații internaționale, într-o funcție care necesită acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior, persoana solicită Serviciului eliberarea certificării avizului de securitate a personalului, cu condiția ca atât avizul, cât și certificarea să rămână valabile pentru o perioadă suficientă desfășurării procedurilor de angajare sau de transfer.

(2) Serviciul eliberează certificarea, care indică nivelul de acces („Confidențial” sau superior), durata de valabilitate a avizului de securitate a personalului și data expirării certificării.

(3) Entitatea publică în care persoana urmează să se angajeze sau să se transfere acceptă certificarea avizului de securitate a personalului, cu condiția ca atât avizul, cât și certificarea să rămână valabile, și emite, în baza acesteia, o autorizație de acces la informații clasificate de nivel corespunzător. Avizul de securitate a personalului acoperă orice funcție deținută de persoana în cauză în cadrul entității

publice, corespunzător nivelului de acces indicat sau unui nivel inferior. Entitatea publică în care persoana își preia funcția informează Serviciul, în termen de 10 zile, cu privire la angajarea persoanei și la eliberarea autorizației de acces la informații clasificate.

(4) Persoanele detașate în cadrul altor entități publice, într-o funcție care necesită acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior, prezintă entității publice la care sunt detașate, înainte de preluarea funcției, o certificare valabilă a avizului de securitate a personalului, pe baza căreia entitatea publică emite o autorizație de acces la informații clasificate.

(5) Persoanele detașate în cadrul instituțiilor internaționale, într-o funcție care necesită acces la informații clasificate la nivelul „Confidențial” sau la un nivel superior, prezintă instituției internaționale, înainte de preluarea funcției, o certificare valabilă a avizului de securitate a personalului, pe baza căreia instituția internațională emite o autorizație de acces la informații clasificate.

(6) Dacă persoana nu își începe activitatea în termen de 12 luni de la recepționarea avizului de securitate a personalului sau dacă intervine o pauză de 12 luni în exercitarea atribuțiilor sale, entitatea publică notifică Serviciul și solicită confirmarea menținerii valabilității avizului de securitate a personalului.

(7) Accesul cetățenilor străini și al apatrizilor la informații clasificate se acordă în temeiul tratatelor internaționale la care Republica Moldova este parte, în bază de reciprocitate, cu condiția deținerii unei certificări valabile a avizului de securitate a personalului, coordonată în prealabil cu Serviciul, pe baza căreia entitatea publică emite o autorizație de acces la informații clasificate. Entitatea publică informează Serviciul, în termen de 10 zile, cu privire la eliberarea autorizației de acces la informații clasificate, la nivelul de acces și la valabilitatea acesteia.

(8) În lipsa unei certificări valabile a avizului de securitate a personalului și a tratatelor internaționale în materie de protecție reciprocă a informațiilor clasificate la care Republica Moldova este parte, accesul cetățenilor străini și al apatrizilor la informații clasificate se acordă cu titlu de excepție, ținând cont de necesitatea asigurării securității naționale a Republicii Moldova, în temeiul dispoziției scrise a Prim-ministrului, adoptată în baza propunerilor motivate ale entității publice, cu condiția obținerii prealabile de la Serviciu, în condiții generale, a avizului de securitate a personalului pentru fiecare cetățean străin sau apatrid. Entitatea publică emite autorizația de acces la informații clasificate și informează Serviciul, în termen de 10 zile, cu privire la eliberarea acesteia, la nivelul de acces și la valabilitatea ei.

Articolul 24. Suspendarea accesului la informații clasificate

(1) Accesul la informații clasificate poate fi suspendat în următoarele situații:

a) la inițierea reverificării de securitate prevăzute la art. 20 alin. (3), până la adoptarea unei decizii privind menținerea sau retragerea avizului de securitate a personalului, dar nu mai mult decât termenele prevăzute la art. 17 alin. (2) și (3);

b) la dobândirea calității de bănuț, învinuit sau inculpat într-o cauză penală privind o infracțiune contra păcii și securității omenirii, infracțiune de război, infracțiune contra securității publice și a ordinii publice, infracțiune contra autorităților publice și a securității de stat, infracțiune contra bunei desfășurări a activității în sfera publică, infracțiune contra justiției ori pentru o altă infracțiune săvârșită cu intenție care o face incompatibilă cu accesul la informații clasificate, până la soluționarea definitivă a cauzei;

c) la inițierea unei investigații de serviciu în legătură cu încălcarea regulilor de gestionare a informațiilor clasificate, până la finalizarea investigației și adoptarea unei decizii definitive de către entitatea publică, dar nu mai mult de 30 de zile lucrătoare;

d) la suspendarea raporturilor de serviciu ale titularului autorizației de acces la informații clasificate pe o durată de până la 12 luni.

(2) Pe perioada suspendării accesului la informații clasificate, titularului autorizației de acces la informații clasificate i se interzice accesul la orice document clasificat ori sistem informațional clasificat, cu excepția celor care vizează rezultatele reverificării sau ale investigației de serviciu efectuate în privința sa.

(3) Durata suspendării nu prelungește durata valabilității autorizației de acces la informații clasificate.

(4) Decizia entității publice de suspendare a accesului la informații clasificate, emisă în temeiul prezentului articol, poate fi contestată în conformitate cu prevederile Codului administrativ al Republicii Moldova nr. 116/2018.

Articolul 25. Încetarea accesului la informații clasificate

(1) Încetarea accesului la informații clasificate are loc în următoarele situații:

a) la expirarea termenului de valabilitate a avizului de securitate a personalului;

b) la adoptarea unei decizii de retragere a avizului de securitate a personalului;

c) la rămânerea definitivă a unei hotărâri judecătorești de condamnare pentru o infracțiune prevăzută la art. 18 lit. f);

d) la încălcarea gravă sau repetată a regulilor de gestionare a informațiilor clasificate;

e) la pierderea cetățeniei Republicii Moldova;

f) la încetarea raporturilor de serviciu ori a contractului individual de muncă ce implică lucrul cu informații clasificate;

g) la acordarea accesului la informații clasificate de nivel superior, în condițiile art. 20 alin. (2) lit. b);

h) la suspendarea raporturilor de serviciu ale titularului autorizației de acces la informații clasificate pe o durată mai mare de 12 luni.

(2) La adoptarea deciziei de încetare a accesului la informații clasificate, entitatea publică comunică persoanei vizate temeiul, precum și, cel puțin sumar, esența motivelor care au stat la baza deciziei, în măsura în care comunicarea nu aduce atingere securității naționale.

(3) Adoptarea deciziei de încetare a accesului la informații clasificate conduce la retragerea autorizației de acces la informații clasificate.

(4) În cazul încetării accesului la informații clasificate și al retragerii autorizației de acces la informații clasificate ca urmare a unor acțiuni sau inacțiuni ce constituie încălcări ale normelor de protecție a informațiilor clasificate, persoana are dreptul să obțină un nou aviz de securitate a personalului și o nouă autorizație de acces la informații clasificate dacă, la momentul solicitării, au expirat următoarele termene:

a) 7 ani de la data rămânerii definitive a actului prin care se constată că fapta persoanei constituie infracțiune în domeniul respectiv;

b) 4 ani de la data rămânerii definitive a actului prin care se constată că fapta persoanei constituie contravenție în domeniul respectiv;

c) 2 ani de la data rămânerii definitive a actului prin care se constată că fapta persoanei constituie o încălcare disciplinară în domeniul respectiv.

(5) Decizia entității publice de încetare a accesului la informații clasificate și de retragere a autorizației de acces la informații clasificate, emisă în temeiul prezentului articol, poate fi contestată în conformitate cu prevederile Codului administrativ al Republicii Moldova nr. 116/2018.

Articolul 26. Evidența avizelor de securitate a personalului și a autorizațiilor de acces

Serviciul ține evidența avizelor de securitate a personalului, iar fiecare entitate publică ține evidența autorizațiilor de acces la informații clasificate pe care le emite. Evidențele respective conțin cel puțin detalii cu privire la nivelul informațiilor clasificate la care este permis accesul persoanei, data acordării avizului de securitate a personalului, după caz, și durata valabilității acestuia.

Articolul 27. Excepțiile de la obligația deținerii avizului de securitate a personalului

(1) Au dreptul de acces la informații clasificate de toate nivelurile de la data numirii sau alegerii lor în funcție, fără obligația obținerii avizului de securitate a personalului și fără autorizare de acces la informații clasificate, următoarele persoane:

- a) Președintele Republicii Moldova;
- b) Președintele Parlamentului;
- c) deputații în Parlament;
- d) membrii Guvernului;
- e) directorul Serviciului de Informații și Securitate;
- f) directorul Serviciului de Protecție și Pază de Stat;
- g) guvernatorul Băncii Naționale a Moldovei;
- h) președintele Curții de Conturi;
- i) președintele Consiliului Superior al Magistraturii;
- j) judecătorii instanțelor judecătorești și ai Curții Constituționale;
- k) președintele Consiliului Superior al Procurorilor;
- l) Procurorul General.

(2) Persoanele prevăzute la alin. (1) au dreptul de acces la informațiile clasificate în măsura în care accesul este strict necesar pentru exercitarea atribuțiilor prevăzute expres de lege.

(3) Accesul persoanelor prevăzute la alin. (1) se acordă după semnarea obligației scrise privind nedivulgarea informațiilor clasificate. Persoanele respective sunt instruite de către Serviciu cu privire la normele și procedurile de securitate pentru protecția informațiilor clasificate și își asumă responsabilitățile cu privire la protecția informațiilor respective, fapt confirmat în scris. Confirmările scrise se păstrează la Serviciu.

(4) Prevederile alin. (1) nu se aplică cetățenilor Republicii Moldova care dețin și cetățenia altui stat. Accesul acestora la informații clasificate se acordă în ordinea generală prevăzută de prezenta lege, după efectuarea verificării de securitate. Solicitarea de efectuare a verificării de securitate se depune de către persoana împuternicită să facă numirea în funcție sau de către Președintele Parlamentului, în cazul deputaților.

(5) Accesul la informații clasificate al titularilor funcțiilor prevăzute la alin. (1) și (4) poate fi suspendat sau poate înceta în condițiile generale stabilite de prezenta lege.

Subsecțiunea a 5-a

Educația și conștientizarea în materie de securitate

Articolul 28. Educația protectivă

(1) Educația protectivă are ca obiectiv instruirea persoanelor care au sau urmează să aibă acces la informații clasificate în vederea aplicării măsurilor referitoare la protecția acestor informații. Entitățile publice țin evidența instruirilor și asigură pregătirea tuturor persoanelor vizate care nu au participat la instruirile organizate.

(2) Toate persoanele cărora li s-a acordat un aviz de securitate a personalului confirmă în scris, prin semnarea fișelor de instruire, faptul că au fost instruite cu privire la protecția informațiilor clasificate și la consecințele compromiterii acestora.

(3) Persoanele autorizate să aibă acces la informații clasificate sunt informate inițial și, ulterior, periodic cu privire la responsabilitățile care le revin și la amenințările la adresa securității informațiilor clasificate și sunt obligate să raporteze imediat structurii de securitate a entității orice abordare sau activitate pe care o consideră suspectă ori neobișnuită.

(4) Persoanele care încetează să exercite atribuții ce necesită acces la informații clasificate sunt informate cu privire la obligațiile care le revin în continuare pentru protecția informațiilor clasificate și confirmă în scris acest fapt.

Subsecțiunea a 6-a

Împrejurări excepționale

Articolul 29. Acordarea autorizațiilor temporare de acces la informații clasificate

(1) Din motive de urgență, în cazuri de interes de serviciu justificate corespunzător printr-o decizie scrisă și în așteptarea finalizării unei verificări de securitate complete, entitatea publică poate acorda angajaților o autorizație temporară de acces la informații clasificate pentru o funcție specifică, după consultarea Serviciului și cu condiția ca rezultatul verificărilor preliminare să ateste că nu se cunosc informații adverse. Autorizațiile temporare sunt valabile cel mult 3 luni și nu permit accesul la informații clasificate „Strict secret”.

(2) Toate persoanele cărora li s-a acordat o autorizație temporară confirmă în scris, prin fișe de instruire, faptul că își înțeleg obligațiile cu privire la protecția informațiilor clasificate, precum și consecințele compromiterii acestora. Entitatea publică ține evidența acestor fișe de instruire.

Articolul 30. Numirea provizorie, accesul unic și accesul de urgență la informații clasificate

(1) În cazul în care o persoană urmează să fie numită într-o funcție care necesită un aviz de securitate a personalului de nivel superior celui deținut, numirea se poate face provizoriu, cu condiția ca:

a) necesitatea vitală de acces la informațiile clasificate de nivel superior să fie justificată, în scris, de către superiorul persoanei în cauză;

b) accesul să fie limitat la anumite informații clasificate, în sprijinul numirii;

c) persoana să dețină un aviz de securitate a personalului valabil de nivel inferior;

d) să fie inițiate demersurile pentru obținerea accesului la nivelul necesar funcției în cauză;

e) persoana să nu fi încălcat în mod grav sau repetat normele de securitate;

f) numirea persoanei să fie aprobată de structura de securitate a entității publice;

g) excepția să fie consemnată, împreună cu descrierea informațiilor la care a fost aprobat accesul.

(2) Procedura prevăzută la alin. (1) se utilizează pentru accesul unic la informații clasificate de nivelul imediat superior celui pentru care persoana deține aviz de securitate a personalului. Nu se recurge în mod repetat la această procedură.

(3) În împrejurări absolut excepționale, precum misiunile în medii ostile sau perioadele de tensiune internațională crescândă, când măsurile de urgență o impun, în special în scopul salvării de vieți, entitățile publice pot acorda, în scris, acces la informații clasificate „Confidențial” sau „Secret” unor persoane care nu dețin avizul de securitate a personalului necesar, cu condiția ca permisiunea să fie absolut necesară și să nu existe suspiciuni întemeiate cu privire la loialitatea, onestitatea și încrederea inspirată de persoana respectivă. Permisiunea se consemnează, cu descrierea informațiilor la care s-a aprobat accesul.

(4) În cazul informațiilor clasificate „Strict secret”, accesul de urgență este limitat la persoanele care beneficiază de acces autorizat la informații clasificate „Secret”.

Articolul 31. Raportarea despre împrejurările excepționale

Entitățile publice notifică imediat Serviciul cu privire la fiecare caz de recurgere la una dintre procedurile prevăzute la art. 29 și 30 și prezintă Serviciului un raport anual de ansamblu privind aplicarea acestora.

Articolul 32. Accesul potențial la informații clasificate

Curierii, gardienii și escortele, ale căror funcții implică un acces potențial la informații clasificate, dețin un aviz de securitate a personalului de nivel corespunzător, sunt informați cu privire la procedurile de securitate și sunt instruiți asupra obligațiilor de protecție a informațiilor care le sunt încredințate.

Articolul 33. Participarea la ședințele clasificate

(1) Fără a aduce atingere art. 27, persoanele desemnate să participe la ședințe în cadrul cărora se discută informații clasificate la nivelul „Confidențial” sau la un nivel superior pot participa numai după ce se confirmă că dețin un aviz de securitate a personalului. Dovada avizului de securitate a personalului este transmisă de entitatea publică care a delegat persoana desemnată către entitatea organizatoare a ședinței clasificate sau, în cazuri excepționale, poate fi prezentată nemijlocit de persoana desemnată. După caz, se poate folosi o listă centralizată de nume, cuprinzând dovada relevantă a avizului de securitate a personalului.

(2) În cazul în care avizul de securitate a personalului este retras persoanei desemnate, entitatea publică informează despre acest fapt entitatea organizatoare.

Secțiunea a 3-a SECURITATEA FIZICĂ

Articolul 34. Securitatea fizică

(1) Securitatea fizică reprezintă aplicarea măsurilor de protecție fizică și tehnică în vederea împiedicării accesului neautorizat la informațiile clasificate.

(2) Măsurile de securitate fizică sunt concepute astfel încât să împiedice accesul disimulat sau forțat al unei persoane neautorizate, să descurajeze, să împiedice și să detecteze acțiunile neautorizate și să permită separarea personalului în ceea ce privește accesul acestuia la informațiile clasificate, pe baza principiului necesității de a cunoaște. Aceste măsuri sunt stabilite pe baza unui proces de management al riscului.

(3) Măsurile de securitate fizică sunt instituite pentru toate spațiile, inclusiv incintele, clădirile, birourile, încăperile și alte zone în care sunt gestionate sau păstrate informații clasificate, inclusiv zonele care adăpostesc sisteme informatice și de comunicații.

(4) Zonele în care sunt păstrate informații clasificate la nivelul „Confidențial” sau la un nivel superior sunt stabilite ca zone securizate, în conformitate cu actele normative.

(5) În vederea protecției informațiilor clasificate la nivelul „Confidențial” sau la un nivel superior se utilizează numai echipamente sau dispozitive aprobate.

(6) Modul de asigurare a securității fizice a informațiilor clasificate este stabilit de Guvern.

Secțiunea a 4-a

SECURITATEA SISTEMELOR INFORMATICE ȘI DE COMUNICAȚII

Articolul 35. Protecția informațiilor clasificate în sisteme informatice și de comunicații

(1) Sistemele informatice și de comunicații gestionează informații clasificate în conformitate cu conceptul de asigurare a informațiilor.

(2) Asigurarea informațiilor în domeniul sistemelor informatice și de comunicații reprezintă certitudinea faptului că aceste sisteme vor proteja informațiile pe care le gestionează și vor funcționa corespunzător, atunci când este necesar, sub controlul utilizatorilor legitimi. Asigurarea informațiilor se bazează pe un proces de management al riscului.

(3) O asigurare a informațiilor eficientă garantează grade adecvate de confidențialitate, integritate, disponibilitate, nerepudiare și autenticitate.

(4) Toate sistemele informatice și de comunicații sunt supuse unui proces de acreditare de către Serviciu. Acreditarea urmărește să garanteze faptul că au fost puse în aplicare toate măsurile de securitate corespunzătoare și că s-a obținut un nivel suficient de protecție a informațiilor clasificate și a sistemelor informatice și de comunicații, în conformitate cu actele normative. Declarația de acreditare stabilește nivelul maxim de clasificare a informațiilor care poate fi gestionat de sistem, precum și termenii și condițiile acreditării respective.

(5) Se pun în aplicare măsuri de securitate în domeniul informațiilor pentru a proteja sistemele informatice și de comunicații care tratează informații clasificate la nivelul „Confidențial” și la un nivel superior împotriva compromiterii acestor informații prin emisii electromagnetice neintenționate. Măsurile de securitate respective sunt proporționale cu riscul de exploatare și nivelul de clasificare a informațiilor.

(6) În cazurile în care protecția informațiilor clasificate este asigurată prin produse criptografice, acestea sunt aprobate de Serviciu.

(7) În cursul transmiterii informațiilor clasificate prin mijloace electronice, se folosesc produse criptografice aprobate. Fără a aduce atingere acestei cerințe, pot fi

aplicate proceduri specifice în situații de urgență sau în cadrul unor configurații tehnice specifice, în conformitate cu actele normative.

(8) Modul de protecție a informațiilor clasificate în sisteme informatice și de comunicații se stabilește de Guvern.

Secțiunea a 5-a

MANAGEMENTUL INFORMAȚIILOR CLASIFICATE

Articolul 36. Managementul informațiilor clasificate

(1) Managementul informațiilor clasificate constă în aplicarea unor măsuri administrative pentru a controla informațiile clasificate pe durata ciclului lor de viață, în vederea completării măsurilor prevăzute la secțiunile 2, 3 și 4, contribuind astfel la descurajarea și detectarea compromiterii sau pierderii deliberate sau accidentale a informațiilor de acest tip. Măsurile respective se referă, în special, la crearea, înregistrarea, copierea, traducerea, reducerea nivelului de clasificare, declasificarea, transportul și distrugerea informațiilor clasificate.

(2) Din motive de securitate, informațiile clasificate sunt înregistrate, la primirea acestora, înainte de a fi distribuite. În acest scop, entitățile înființează sisteme de registre. Informațiile clasificate „Strict secret” sunt înregistrate în registre speciale.

(3) Incintele unde sunt gestionate sau păstrate informații clasificate sunt supuse unor inspecții periodice de către Serviciu.

(4) Informațiile clasificate sunt transmise între incinte situate în afara zonelor protejate fizic după cum urmează:

a) ca regulă generală, informațiile clasificate sunt transmise prin mijloace electronice protejate prin intermediul unor produse criptografice aprobate;

b) în situațiile în care nu se utilizează mijloacele prevăzute la lit. a), informațiile clasificate sunt transportate:

1) pe suport electronic (chei USB, CD-uri, hard diskuri sau alte suporturi electronice) protejat prin intermediul unor produse criptografice aprobate; sau

2) în toate celelalte cazuri, conform indicațiilor primite de la Serviciu, în conformitate cu măsurile de protecție prevăzute de actele normative.

(5) Modul de asigurare a managementului informațiilor clasificate este stabilit de Guvern.

Capitolul IV

SECURITATEA INDUSTRIALĂ

Articolul 37. Securitatea industrială

(1) Securitatea industrială constă în aplicarea de măsuri în vederea asigurării protecției informațiilor clasificate de către contractanți și subcontractanți în cursul negocierilor anterioare încheierii contractelor și pe toată durata contractelor clasificate încheiate de entitățile publice. Astfel de contracte nu implică accesul la informații clasificate „Strict secret”.

(2) Entitățile publice pot încredința prin contract sarcini care implică sau determină accesul la informații clasificate sau gestionarea sau păstrarea acestora de entități industriale sau de altă natură înregistrate în Republica Moldova sau într-un alt stat în condițiile actelor normative.

(3) Atunci când atribuie contracte clasificate entităților industriale sau de altă natură, entitățile publice, în calitate de autoritate contractantă, asigură respectarea standardelor minime privind securitatea industrială stabilite de actele normative și menționate în contract.

(4) Serviciul asigură că atât contractanții, cât și subcontractanții iau toate măsurile necesare pentru protecția informațiilor clasificate în cursul negocierilor premergătoare contractului, precum și pe parcursul executării contractelor clasificate.

(5) Serviciul asigură că atât contractanții, cât și subcontractanții înregistrați în Republica Moldova și care participă la contracte sau subcontracte necesitând accesul, în obiectivele lor, la informații clasificate „Confidențial” sau „Secret”, fie în cursul executării contractelor respective, fie în etapa precontractuală, trebuie să dețină aviz de securitate industrială, la nivelul de clasificare necesar.

(6) Personalului contractantului sau al subcontractantului ale cărui atribuții pot necesita accesul la informații clasificate „Confidențial” sau „Secret” în scopul executării unui contract clasificat i se acordă avize de securitate a personalului de către Serviciu, în conformitate cu prevederile din capitolul III.

(7) Serviciul aprobă orientări privind securitatea industrială, descriind în special cerințe detaliate referitoare la avizul de securitate industrială, anexa de securitate, vizite, transmiterea și transportul informațiilor clasificate.

(8) Modul de asigurare a securității industriale este stabilit de Guvern.

Capitolul V

PARTAJAREA ȘI TRANSMITEREA INFORMAȚIILOR CLASIFICATE

Articolul 38. Partajarea și transmiterea informațiilor clasificate

(1) Entitățile pot partaja informațiile clasificate pe care le dețin cu alte entități din Republica Moldova, dacă entitatea destinatară este autorizată să gestioneze informații clasificate de nivelul corespunzător și asigură protecția acestora în condițiile prezentei legi.

(2) Transmiterea informațiilor clasificate către alte state sau către organizații internaționale se realizează în temeiul tratatelor internaționale, care conțin dispoziții ce garantează că destinatarii protejează informațiile clasificate la standarde cel puțin la fel de stricte ca cele prevăzute de prezenta lege și alte acte normative.

(3) În lipsa tratatelor internaționale prevăzute la alin. (2), informațiile clasificate pot fi transmise altor state sau organizații internaționale în modul stabilit de Guvern.

(4) Entitățile publice și entitățile industriale sau de altă natură desemnează registre care servesc drept puncte principale de intrare și de ieșire pentru informațiile clasificate partajate sau schimbate la nivel național.

(5) Modul de partajare și transmitere a informațiilor clasificate se stabilește de Guvern.

Capitolul VI

ORGANIZAREA ȘI CONTROLUL SISTEMULUI DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE

Articolul 39. Responsabilitatea pentru punerea în aplicare a legii

(1) Serviciul, în calitate de autoritate națională de securitate, întreprinde toate măsurile necesare pentru a asigura punerea în aplicare a prezentei legi și a altor acte normative în domeniul protecției informațiilor clasificate.

(2) Serviciul poate emite îndrumări metodologice în vederea asigurării unei interpretări și aplicări adecvate a legislației privind protecția informațiilor clasificate.

(3) Conducătorii entităților publice întreprind toate măsurile necesare pentru a asigura, în cazul deținerii sau gestionării informațiilor clasificate, aplicarea corespunzătoare a legislației privind protecția informațiilor clasificate.

(4) Entitățile publice și entitățile industriale sau de altă natură, după coordonarea cu Serviciul, adoptă normele interne care stabilesc particularitățile de punere în aplicare a legislației privind protecția informațiilor clasificate.

Articolul 40. Atribuțiile Serviciului și ale entităților publice

(1) Serviciul:

a) coordonează normele interne de protecție a informațiilor clasificate în entitățile publice;

b) efectuează vizite de evaluare a entităților publice și a entităților industriale sau de altă natură, în scopul stabilirii eficienței măsurilor puse în aplicare pentru protecția informațiilor clasificate;

c) realizează controlul măsurilor de securitate destinate protecției informațiilor clasificate din cadrul entităților publice și entităților industriale sau de altă natură;

d) elaborează și prezintă Guvernului spre aprobare proiecte de acte normative în domeniul protecției informațiilor clasificate;

e) oferă consultanță entităților publice și entităților industriale și de altă natură cu privire la natura amenințărilor la adresa securității informațiilor clasificate și la mijloacele de protecție împotriva acestora, precum și cu privire la măsurile organizatorice de protecție;

f) colaborează cu autoritățile naționale de securitate ale altor state și cu structurile de securitate ale organizațiilor internaționale privind protecția informațiilor clasificate;

g) efectuează verificările de securitate a personalului;

h) efectuează verificările de securitate ale entităților industriale sau de altă natură privind capacitatea entităților respective de a proteja informațiile clasificate la care ar urma să aibă acces în baza unor activități contractuale;

i) eliberează avizele de securitate a personalului și avizele de securitate industrială;

j) acreditează sistemele de protecție a informațiilor clasificate;

k) organizează și coordonează certificarea și expertiza mijloacelor de protejare criptografică și tehnică a informațiilor clasificate;

l) creează sisteme guvernamentale de comunicații, asigură funcționarea, securitatea, întreținerea, dezvoltarea și modernizarea acestor sisteme în scopul asigurării unui schimb protejat de informații clasificate;

m) constată cazurile de încălcare a normelor privind protecția informațiilor clasificate;

n) asigură curieratul diplomatic și exercită controlul asupra circuitului informațiilor clasificate și al informațiilor de serviciu între Ministerul Afacerilor Externe și misiunile diplomatice și oficiile consulare ale Republicii Moldova din străinătate;

o) este responsabil cu măsurile de securitate pentru protecția informațiilor UE clasificate, în corespundere cu art. 15 alin. (3) lit. a) și b) din Decizia 2013/488/UE a Consiliului;

p) exercită funcțiile aferente asigurării informațiilor în domeniul sistemelor informatice și de comunicații conform art. 10 alin. (8) și (9) din Decizia 2013/488/UE a Consiliului și în modul stabilit de Guvern;

q) eliberează avizele de securitate pentru accesul la informații clasificate NATO, în modul stabilit de Guvern;

r) asigură evidența, gestionarea și controlul informațiilor clasificate NATO;

s) exercită și alte atribuții prevăzute de actele normative în domeniul protecției informațiilor clasificate.

(2) Conducătorul entității publice este responsabil de protecția informațiilor clasificate în cadrul entității. În această calitate, conducătorul:

a) aprobă și pune în aplicare norme interne de securitate în coordonare cu Serviciul;

b) aprobă nomenclatoarele departamentale de informații care urmează a fi clasificate și listele funcțiilor care necesită acces la informații clasificate;

c) organizează funcționarea structurilor de securitate responsabile de implementarea măsurilor de protecție a informațiilor clasificate;

d) colaborează cu Serviciul cu privire la toate chestiunile de securitate privind protecția informațiilor clasificate relevante pentru activitatea entității publice;

e) acordă autorizația de acces la informații clasificate personalului entității;

f) dispune efectuarea de investigații cu privire la orice compromitere sau pierdere, reală sau prezumată, de informații clasificate deținute sau elaborate de entitatea publică și notifică Serviciul despre astfel de circumstanțe și solicită implicarea Serviciului în procesul de investigație;

g) dispune efectuarea inspecțiilor periodice ale măsurilor de securitate pentru protecția informațiilor clasificate în incinta entității, de către structura de securitate sau funcționarul de securitate;

h) elaborează și aprobă norme interne privind mecanismul de verificare în vederea acordării autorizației de acces la nivelul „Restricționat” pentru personalul din cadrul entității publice;

i) dispune și/sau efectuează, împreună și de comun acord cu Serviciul, evaluări periodice ale măsurilor de securitate pentru protecția informațiilor clasificate din cadrul serviciilor și incintelor aparținând entităților din subordine;

j) notifică Serviciul despre orice indiciu sau suspiciune ce pot genera riscuri de securitate în privința informațiilor clasificate;

k) se asigură că măsurile de securitate sunt coordonate cu Serviciul, inclusiv în ceea ce privește natura amenințărilor la adresa securității informațiilor clasificate și mijloacele de protecție împotriva acestora;

l) solicită Serviciului realizarea măsurilor de verificare în vederea emiterii avizului de securitate a personalului în vederea acordării autorizației de acces de nivelul „Confidențial” și de nivel superior;

m) exercită și alte atribuții prevăzute de actele normative în domeniul protecției informațiilor clasificate.

(4) În îndeplinirea acestor responsabilități, entitățile publice pot recurge la un contractant care să efectueze, sub conducerea și supravegherea acesteia, sarcini legate de asigurarea securității.

Articolul 41. Controlul asigurării protecției informațiilor clasificate

(1) Conducătorii entităților publice, prin structurile de securitate sau funcționarii de securitate, exercită controlul permanent al asigurării protecției informațiilor clasificate deținute de entitățile pe care le conduc.

(2) Serviciul efectuează controlul asigurării protecției informațiilor clasificate în cadrul entităților publice și al entităților industriale sau de altă natură care dețin sau gestionează informații clasificate. În exercitarea controlului, personalul Serviciului are acces, în condițiile legii, în incintele și la documentele, registrele și sistemele informatice și de comunicații ale entității controlate, în măsura necesară verificării respectării legislației privind protecția informațiilor clasificate.

(3) Concluziile întocmite de Serviciu în baza rezultatelor controlului sunt obligatorii pentru persoanele cu funcții de răspundere din cadrul entităților controlate.

(4) Parlamentul exercită controlul asupra executării legislației privind protecția informațiilor clasificate prin comisia permanentă de profil și prin subcomisia specializată de control asupra activității Serviciului, în condițiile Regulamentului Parlamentului.

CAPITOLUL VII DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 42. Dispozițiile finale

(1) Prezenta lege intră în vigoare pe 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.

(2) La data intrării în vigoare a prezentei legi, Legea nr. 245/2008 cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr. 45–46, art. 123) se abrogă.

(3) Până la intrarea în vigoare a prezentei legi:

a) Guvernul:

1) va prezenta Parlamentului propuneri pentru aducerea legislației în vigoare în concordanță cu prezenta lege;

2) va aduce actele sale normative în concordanță cu prezenta lege;

3) va aproba actele normative necesare executării prezentei legi;

b) Serviciul va elabora actele normative departamentale necesare executării prezentei legi;

c) Consiliul Uniunii Avocaților, Consiliul Camerei Notariale și Consiliul Uniunii Naționale a Executorilor Judecătorești vor aproba, în coordonare cu Serviciul, regulamentele prevăzute la art. 22 alin. (7)–(9).

(4) Până la intrarea în vigoare a prezentei legi, entitățile care dețin informații atribuite la secret de stat adoptă norme interne de securitate aliniate la cerințele prezentei legi.

Articolul 43. Dispozițiile tranzitorii

(1) După intrarea în vigoare a prezentei legi:

a) informațiile atribuite la secret de stat în temeiul Legii nr. 245/2008 cu privire la secretul de stat se echivalează cu nivelurile de clasificare prevăzute de prezenta lege și sunt protejate în conformitate cu prevederile prezentei legi;

b) autorizațiile de acces emise în temeiul Legii nr. 245/2008 cu privire la secretul de stat își păstrează termenul de valabilitate și continuă să fie acceptate în conformitate cu prevederile corespunzătoare ale prezentei legi.

(2) Cauzele civile, contravenționale, penale și de contencios administrativ se examinează și se soluționează în conformitate cu prevederile legii în vigoare la data apariției raportului juridic litigios.

PREȘEDINTELE PARLAMENTULUI

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. Adicional, 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 appendicele 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, accidente 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 declassificate 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 ierarhice 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 bănuț, 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 (infrațiune), 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, nerepudiare, 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 destinate 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 transunerii, 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 GHEORGHIȘ

CERERE nr. 03/8720 din 31 iulie 2026
privind înregistrarea de către Cancelaria de Stat
a proiectului de lege privind protecția informațiilor clasificate

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiect de lege privind protecția informațiilor clasificate
2.	Autoritatea care a elaborat proiectul	Ministerul Justiției
3.	Justificarea depunerii cererii	Implementarea legislației UE
4.	Referința la documentul de planificare care prevede elaborarea proiectului	Acțiunea 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.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1) Cancelaria de Stat (Centrul de Armonizare a Legislației); 2) Ministerul Apărării; 3) Ministerul Afacerilor Interne; 4) Ministerul Energiei; 5) Ministerul Mediului; 6) Ministerul Educației și Cercetării; 7) Ministerul Agriculturii și Industriei Alimentare; 8) Ministerul Dezvoltării Economice și Digitalizării; 9) Ministerul Finanțelor; 10) Ministerul Muncii și Protecției Sociale; 11) Ministerul Afacerilor Externe; 12) Ministerul Infrastructurii și Dezvoltării Regionale; 13) Ministerul Sănătății; 14) Ministerul Culturii; 15) Serviciul de Informații și Securitate; 16) Banca Națională a Moldovei; 17) Curtea de Conturi; 18) Consiliul Superior al Magistraturii; 19) Curtea Supremă de Justiție; 20) Consiliul Superior al Procurorilor; 21) Procuratura Generală;
6.	Termenul-limită pentru depunerea avizelor și/sau expertizelor	15 zile lucrătoare
7.	Persoana responsabilă de promovarea proiectului	Victor KALUGHIN Consultant principal, Direcția elaborare acte normative, Ministerul Justiției; Tel.: (022) 20 14 69; Email: victor.kalughin@justice.gov.md

8.	Anexe	1) Proiectul de lege; 2) Nota de fundamentare;
9.	Data și ora depunerii cererii	Conform semnăturii

Secretar de stat

Mihai GHEORGHIȚ