



Rolul funcționarului de securitate pe componenta de protecție a personalului

Potrivit Standardelor naționale de protecție a informațiilor clasificate în România, măsurile de protecție a personalului au drept scop:

- a) să prevină accesul persoanelor neautorizate la informații secrete de stat;
- b) să garanteze că informațiile secrete de stat sunt distribuite deținătorilor de certificate de securitate/autorizații de acces, cu respectarea principiului necesității de a cunoaște;
- c) să permită identificarea persoanelor care, prin acțiunile sau inacțiunile lor, pot pune în pericol securitatea informațiilor secrete de stat și să prevină accesul acestora la astfel de informații.

Protecția personalului se realizează prin: selecționarea, verificarea, avizarea și autorizarea accesului la informații secrete de stat, revalidarea, controlul și instruirea personalului, retragerea certificatului de securitate sau autorizației de acces.

Coroborat cu cele menționate mai sus, în aceleași *Standarde*, regăsim următoarele atribuții ale funcționarului / structurii de securitate:

- asigurarea implementării normelor interne privind securitatea personalului;
- inițierea procesului de verificare de securitate în vederea avizării pentru acces la informații secrete de stat, cu aprobarea șefului instituției;
- punerea la dispoziția persoanei, pentru care se solicită eliberarea certificatului de securitate, a formularelor tip corespunzătoare nivelului de acces solicitat;
- acordarea asistenței în vederea completării formularelor de verificare, cu respectarea termenului de transmitere a solicitării;
- acordarea sprijinului necesar instituțiilor cu atribuții în efectuarea verificărilor asupra personalului ce urmează să aibă acces la informații secrete de stat;
- actualizarea evidenței persoanelor din cadrul instituției care au acces la informații secrete de stat, păstrarea documentelor de acces, luarea măsurilor necesare pentru revalidarea/retragerea certificatelor de securitate/autorizațiilor de acces;
- reanalizarea periodică și actualizarea normelor interne de implementare a reglementărilor privind protecția informațiilor secrete de stat.

Conducătorii autorităților, instituțiilor publice, agenților economici cu capital integral sau parțial de stat și ai celorlalte persoane juridice de drept public sau privat aprobă *Listele funcțiilor care presupun accesul la informații secrete de stat*. În aplicarea principiului "*necesității de a cunoaște*" este necesară evaluarea atribuțiilor specifice fiecărei funcții din statul de organizare, pentru a stabili dacă necesită acces la informații secrete de stat și nivelul de secretizare aferent.

La dimensionarea listei funcțiilor care presupun acces la informații secrete de stat trebuie avute în vedere următoarele aspecte:

- includerea tuturor funcțiilor care presupun acces efectiv la informații secrete de stat, chiar dacă unele dintre acestea sunt vacante
- realizarea concordanței între nivelul de acces solicitat și nivelul de secretizare a informațiilor.

Șeful structurii de securitate și/sau funcționarul de securitate trebuie să dețină certificat de securitate corespunzător celui mai înalt nivel de clasificare a informațiilor secrete de stat gestionate de instituție;

Lista funcțiilor se actualizează ori de câte ori este necesar și se comunică autorității desemnate de securitate competente.

Pot ocupa funcții care presupun acces la informații secrete de stat doar persoanele care au autorizație sau sunt în curs de verificare la Autoritatea Desemnată de Securitate. În situația angajaților care au fost avizați negativ pentru acces la informații secrete de stat sau pentru care nu au fost înaintate formularele de securitate către ADS (deoarece au refuzat sau au întârziat, în mod nejustificat, completarea acestora), aceștia nu mai pot ocupa poziția prevăzută în "*Lista funcțiilor care presupun acces la informații secrete de stat*".

Potrivit legislației în vigoare, fiecare persoană care urmează să aibă acces la informații secrete de stat este verificată, în baza acceptului prealabil, fiind relevante atât trăsăturile de caracter, cât și situațiile sau împrejurările din care pot rezulta riscuri și vulnerabilități de securitate.

Verificarea/avizarea (revalidarea) este derulată de către autoritățile desemnate de securitate cu atribuții în acest sens: Serviciul Român de Informații, Ministerul Apărării Naționale, Serviciul de Informații Externe, Ministerul Afacerilor Interne, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale.

În vederea eliberării *certificatului de securitate sau autorizației de acces*, conducătorul unității solicită, în scris, ORNISS, efectuarea ***verificărilor de securitate*** asupra persoanei care urmează să aibă acces la informații secrete de stat. Solicitarea este însoțită de formularele tip prevăzute de *Standardele naționale*, completate de persoana în cauză, potrivit nivelului de secretizare a informațiilor, introduse în plic separat, sigilat. Plicul în care sunt introduse formularele se deschide numai de persoana autorizată, din cadrul autorității desemnate de securitate.

] Singura excepție de la această procedură, statuată prin modificările aduse art. 7 din Legea nr. 182 privind protecția informațiilor secrete de stat, stabilește că accesul la informațiile secrete de stat este garantat, sub condiția validării alegerii sau numirii și a depunerii jurământului, pentru președintele României, Primul - ministru, membrii Guvernului, deputații și senatorii, judecătorii și procurorii, precum și magistrații asistenți ai Înaltei Curți de Casație și Justiție, care, în exercitarea atribuțiilor specifice, sunt îndreptățiți să aibă acces la informații secrete de stat fără realizarea verificării de securitate. Pentru aceste categorii de persoane, accesul la informații secrete de stat se acordă în baza unor proceduri interne ale instituțiilor din care fac parte, avizate de Oficiul Registrului Național al Informațiilor Secrete de Stat, după ce au luat cunoștință de responsabilitățile ce le revin privind protecția informațiilor secrete de stat și au semnat angajamentul scris de păstrare a secretului prevăzut la art. 36 alin. (3) din Legea nr. 182/2002.

În cazul în care o persoană deține certificat de securitate/autorizație de acces la informații naționale clasificate, acesteia i se poate elibera și certificat de securitate pentru

acces la informații NATO clasificate valabil pentru același nivel de secretizare sau pentru un nivel inferior.

Dacă informațiile NATO clasificate la care se solicită acces sunt de nivel superior celui pentru care persoana în cauză deține certificat de securitate/autorizație de acces se vor efectua verificările necesare, potrivit standardelor în vigoare.

Valabilitatea certificatului/autorizației eliberate în condițiile menționate anterior încetează la expirarea termenului de valabilitate al certificatului/autorizației inițiale.

De reținut:

Seleționarea persoanelor care urmează să ocupe funcții ce presupun accesul la informații secrete de stat se derulează integral și exclusiv în cadrul fiecărei instituții deținătoare de astfel de informații, demers derulat prin raportare la criteriile de incompatibilitate stabilite de art. 159 și 160 din HG 585/2002 (în măsura în care la nivelul instituției angajatoare sunt disponibile unele date referitoare la persoanele vizate).

Următoarele situații imputabile atât solicitantului, cât și soțului/soției sau concubinului/concubinei acestuia reprezintă elemente de incompatibilitate pentru acces la informații secrete de stat:

a) dacă a comis sau a intenționat să comită, a fost complice, a complotat sau a instigat la comiterea de acte de spionaj, terorism, trădare ori alte infracțiuni contra siguranței statului;

b) dacă a încercat, a susținut, a participat, a cooperat sau a sprijinit acțiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie sau de a fi membre ale unor organizații ori puteri străine inamice ordinii de drept din țara noastră;

c) dacă este sau a fost membru al unei organizații care a încercat, încearcă sau susține răsturnarea ordinii constituționale prin mijloace violente, subversive sau alte forme ilegale;

d) dacă este sau a fost un susținător al vreunei organizații prevăzute la lit. c, este sau a fost în relații apropiate cu membrii unor astfel de organizații într-o formă de natură să ridice suspiciuni temeinice cu privire la încrederea și loialitatea persoanei.

Constituie elemente de incompatibilitate pentru accesul solicitantului la informații secrete de stat oricare din următoarele situații:

a) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informații cu relevanță în planul siguranței naționale ori a mințit în completarea formularelor tip sau în cursul interviului de securitate;

b) are antecedente penale sau a fost sancționat contravențional pentru fapte care indică tendințe infracționale;

c) are dificultăți financiare serioase sau există o discordanță semnificativă între nivelul său de trai și veniturile declarate;

d) consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau de alte substanțe interzise prin lege care produc dependență;

e) are sau a avut comportamente imorale sau deviații de comportament care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni;

f) a demonstrat lipsă de loialitate, necinste, incorectitudine sau indiscreție;

g) a încălcat reglementările privind protecția informațiilor secrete de stat;

h) suferă sau a suferit de boli fizice sau psihice care îi pot cauza deficiențe de discernământ confirmate prin investigație medicală efectuată cu acordul persoanei solicitante;

i) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilități exploatabile de către serviciile de informații ale căror interese sunt ostile României și aliaților săi.

Astfel, **dacă este de notorietate** că o persoană consumă excesiv băuturi alcoolice sau este dependentă de alcool (lit. d), are comportamente imorale sau deviații de comportament care o fac vulnerabilă la șantaj sau presiuni (lit. e), a încălcat reglementările privind protecția informațiilor clasificate (lit. g), suferă de boli fizice sau psihice care îi pot cauza deficiențe de discernământ (lit. h) sau - ceea ce poate fi evident pentru oricine -

există o discordanță între nivelul de trai și veniturile legal obținute (lit. c), apreciem că aceste date pot constitui criteriile de selecționare primară în vederea inițierii procedurii de verificare (completarea formularelor tip), context în care structura de securitate se poate adresa conducerii instituției cu propunerea de excludere a persoanei de pe Lista specifică.

Procedura de vetting are ca punct de pornire datele menționate de solicitant în formularele de verificare.

COMPLETAREA FORMULARELOR DE SECURITATE

În vederea asigurării operativității emiterii avizului de securitate, facem următoarele recomandări cu privire la aspectele de adus la cunoștința solicitanților, în ceea ce privește completarea formularelor tip:

RECOMANDĂRI GENERALE

Asigurați-vă că persoana care urmează să completeze formularele de securitate:

- își rezervă timp suficient pentru citirea cu atenție a rubricilor/întrebărilor;

În urma interviurilor de securitate derulate pentru clarificarea unor neconcordanțe între cele consemnate în formulare și cele rezultate din verificări, cea mai des întâlnită motivare a discrepanțelor a fost cea referitoare la timpul limitat acordat completării formularelor.

- înțelege cum să completează rubricile și să răspundă la toate întrebările;

Un alt argument adus de solicitanți în interviul de securitate este legat de neînțelegerea întrebărilor, spre exemplu, se motivează referitor la capitolul de antecedente și cazier că nu au consemnat unele condamnări penale sau sancțiuni administrative întrucât în prezent nu există înregistrări în cazierul judiciar, intervenind reabilitarea sau prescrierea acestora, însă întrebările se referă la contextul în care persoana a fost vreodată cercetată sau sancționată penal sau administrativ indiferent dacă în prezent are cazierul curat.

- a semnat Declarația și nu îi modifică conținutul;

*Lipsa/insuficiența datelor sau nesemnarea/modificarea Declarației poate avea drept consecință **returnarea** formularelor tip.*

- la întrebările cu variante de răspuns bifează răspunsul dorit și anulează celălalt răspuns.

Exemplu

1. – unde sunt prevăzute casete

Sunteți în relații permanente de natură profesională sau personală cu cetățeni străini?

DA	<input type="checkbox"/>
----	--------------------------

NU	<input checked="" type="checkbox"/>
----	-------------------------------------

Așa nu

DA	<input type="checkbox"/>
----	--------------------------

NU	<input type="checkbox"/>
---------------	--------------------------

2. – unde nu sunt prevăzute casete, se precizează "DA/NU".

Ați consumat sau consumați substanțe care creează dependență sau droguri?

*Dacă răspunsul este negativ, în caseta de detaliere, se consemnează **NU**.*

Chiar dacă răspunsul este "NU", este necesară consemnarea acestuia: s-a constatat că au fost persoane implicate în diverse situații care au motivat lipsa răspunsului DA prin faptul că "a fost o singură dată, în adolescență" (nn. deși întrebarea nu face diferențieri),

dar care apreciază că nu au mințit pentru că au consemnat "NU" (sau au motivat prin faptul că "nu au știut dacă să consemneze sau nu").

Totodată, răspunsurile la întrebările din formularele de securitate trebuie consemnate de fiecare dată când se solicită revalidarea avizului pentru acces la informații secrete de stat (au existat situații când, la revalidare, solicitantul nu a menționat date relevante la capitolul *Antecedente și cazier*, motivând că acestea au fost deja consemnate în formularul completat anterior).

Menționăm că în cadrul verificărilor de securitate, absența unui răspuns de tip DA la întrebări unde nu există casete cu răspunsuri determinate este susceptibilă de a fi interpretată ca fiind un răspuns negativ, iar în cazul în care se constată că au existat situații necesar a fi consemnate, se poate lua decizia emiterii unui aviz negativ pe baza elementului de incompatibilitate "a mințit în completarea formularelor tip".

Dacă persoana care completează formularul de securitate se află în situația în care ar bifa "NU", dar totuși există o situație "sensibilă" în legătură cu care nu este sigur că se încadrează la cerințe, se recomandă consemnarea și detalierea acesteia (este de preferat să existe mențiuni suplimentare decât să se interpreteze ca o omisiune deliberată a unor date). Dacă se bifează "DA", pe lângă situația certă care se încadrează la cerințe, se recomandă detalierea și a celei "sensibile".

Un răspuns negativ consemnat "din neatenție" și care nu corespunde realității poate avea drept consecință emiterea unui aviz negativ în baza elementului de incompatibilitate "a mințit în completarea formularelor tip".

Totodată, lipsa unui răspuns/un răspuns pozitiv consemnat "din neatenție" va impune contactarea persoanei/realizarea unui interviu de securitate pentru clarificarea/detalierea situației.

- detaliază denumirile (de exemplu, Direcția Generală de Export și nu DGE)
- completează cu majuscule, pentru a evita situația în care scrisul este ilizibil.

Recomandăm evitarea mențiunilor de tipul "datele solicitate se regăsesc în Declarațiile de Avere și/sau Interese", "conform Declarației de Avere", fără detalierea acestora în formularul de securitate; cel mult, se pot anexa copii ale respectivelor documente, iar la rubricile în cauză se menționează "conform copiilor anexate" (valabil și pentru situațiile în care este necesară detalierea anumitor situații - respectivele file se semnează, datează și se anexează la formularul de securitate).

Întrucât procedura de revalidare presupune re completarea integrală a tuturor rubricilor, este important ca persoana solicitantă să cunoască faptul că datele referitoare la rude (și orice alte date pentru care demersurile de obținere sunt dificile) trebuie păstrate - adesea se apreciază în mod eronat faptul că în contextul revalidării nu mai este necesară completarea datelor de identitate pentru frați/cumnați întrucât au fost consemnate în contextul verificărilor anterioare.

RECOMANDĂRI SPECIFICE (completarea unor rubrici din formularele tip)

Spațiu rezervat instituției solicitante - este necesară completarea funcției persoanei, conform *Listei funcțiilor care presupun acces la informații secrete de stat*. În cazul în care persoana necesită acces la informații secrete de stat în vederea participării la un contract clasificat, este necesară detalierea situației respective la rubrica *motivul solicitării*.

Datele de identitate – conform cărții de identitate (dacă există diferențe față de certificatul de naștere, precizați și datele din acest document, cu mențiunea “conform certificatului de naștere”)

Domiciliul permanent – conform cărții de identitate

Domiciliul flotant – se precizează atât reședința din evidențele oficiale (viza de flotant), cât și reședința efectivă (dacă este cazul, chiar dacă nu sunteți înregistrat cu aceasta în evidențele oficiale)

Notă - se pot preciza și intervalele de timp aferente fiecărei adrese, respectiv, în cazul închirierii, se pot nominaliza proprietarii (pentru stabilirea conformității datelor)

Studii - se vor consemna instituțiile de învățământ, perioada efectuării studiilor și felul acestora (inclusiv în cazul revalidării); se vor evita abrevierile pentru denumirile instituțiilor de învățământ.

Situația familială – se consemnează și persoana care poate fi inclusă în categoria “partener de viață”, în legătură cu care solicitantul apreciază că are o relație apropiată (chiar dacă nu locuiesc împreună); la rubrica *Alte situații*, pot fi consemnate detalii despre tipul relației.

Locurile de muncă – este necesară nominalizarea tuturor locurilor de muncă, inclusiv a celor "neoficiale" (fără contract de muncă), cu perioadele aferente (de evitat abrevierile); dacă este cazul, se poate detalia motivul pentru care nu a existat continuitate - șomaj, studii în străinătate, concediu pentru creșterea copilului etc.

Funcția – conform cu denumirea existentă în *Lista funcțiilor care necesită acces la informații secrete de stat*, emisă de către instituție (de exemplu, dacă solicitantul ocupă funcția de *consilier* nu este necesar să se precizeze *consilier grad I A*).

Referințe – se recomandă evitarea nominalizării unor rude.

Colaborarea cu anumite societăți comerciale - în situația în care persoana care face obiectul verificărilor de securitate a renunțat la calitatea de administrator, asociat etc. se recomandă descrierea situației și nominalizarea societăților comerciale (după caz, se pot anexa copii ale unor documente privind statutul actual al solicitantului în raport cu societatea respectivă).

În situația în care persoana care face obiectul verificărilor de securitate dorește completarea formularelor tip, fără ca funcționarul de securitate să poată avea acces la eventuale "situații sensibile", se poate proceda astfel:

1. Se pun la dispoziția solicitantului formularele (în funcție de nivelul de acces) și i se aduc la cunoștință recomandările sus-menționate (ce se pot xeroxa pentru fiecare persoană).
2. Solicitantul completează **datele de identitate** pe prima pagină a fiecărui formular tip, **funcția** (conform cu *Lista funcțiilor care necesită acces la informații secrete de stat*), și semnează/datează **Declarațiile** din fiecare formular tip.
3. Funcționarul de securitate verifică corectitudinea datelor de pe prima pagină a fiecărui formular tip, a titulaturii funcției și dacă s-au semnat/datat **Declarațiile**; ulterior, contrasemnează **Declarațiile**.
4. Solicitantul completează formularele de securitate și, în prezența sa, funcționarul de securitate le înregistrează; ulterior, solicitantul introduce formularele într-un plic pe care îl sigilează (se scriu datele de identitate pe plic).

Așa da: structura de securitate a unui minister a întocmit o notă explicativă (asumată sub semnătură de către persoana a cărei verificare se solicita) cu privire la

modul adecvat de completare a formularelor, termenele legale de finalizare a verificărilor, posibilitatea contactării de către ADS pentru realizarea unui interviu de securitate.

Așa nu: funcționarul de securitate al unui Parchet a transmis formularele unei persoane care nu a completat decât rubricile privind datele generale și cele referitoare la membrii de familie, respectiv consimțământul pentru efectuarea verificării; chestionarele au fost restituite fără emiterea unui aviz.

În alte situații:

- declarațiile nu au fost semnate de către solicitant/funcționarul de securitate;
- au fost operate modificări în conținutul declarației de către solicitant;
- nu au fost consemnate integral răspunsurile la capitolele "Antecedente și cazier" și "Date de securitate";
- au fost completate eronat anumite rubrici din formularele de securitate;
- nu a fost completată funcția pentru care se solicită avizarea accesului/nu a fost consemnat motivul solicitării;
- au existat neconcordanțe între funcția menționată în formulare și cea din Lista funcțiilor de la nivelul instituției;
- au existat neconcordanțe între nivelul pentru care se solicită avizarea accesului și cel prevăzut în Lista funcțiilor pentru funcția deținută de solicitant.

Așa da: la completarea formularelor, funcționarul de securitate al unei instituții din cadrul administrației centrale a comunicat solicitantului că este posibil să fie contactat pentru realizarea unui interviu de securitate și i-a trasat indicații privind necesitatea ca în cadrul discuțiilor să manifeste responsabilitate, seriozitate și onestitate.

Așa nu: o angajată a unui minister a fost contactată în vederea organizării interviului de securitate, însă aceasta a refuzat să se prezinte la activitate, motivând prin aceea că nu dorește să fie autorizată și nici să aibă acces la informații secrete de stat.

După efectuarea verificărilor, în funcție de propunerea de aviz comunicată de autoritatea desemnată de securitate, ORNISS avizează eliberarea *documentului de autorizare*, aduce la cunoștința conducătorului unității acest fapt, care va dispune eliberarea *certificatului de securitate/autorizației de acces*, după caz.

Certificatul de securitate sau autorizația de acces se emite în două exemplare originale, dintre care unul este păstrat de funcționarul de securitate, iar celălalt se trimite la ORNISS, care notifică ADS-ul care a efectuat verificările de securitate.

La primirea *certificatului de securitate/autorizației de acces*, posesorul acesteia are obligația să semneze angajamentul de confidențialitate.

Valabilitatea *certificatului de securitate sau autorizației de acces* este de până la patru ani, pentru acces la informații secrete de stat, și de trei ani pentru acces la informații NATO clasificate.

În cadrul acestor termene, *revalidarea* poate avea loc la solicitarea unității în care persoana își desfășoară activitatea sau a ORNISS, în oricare din următoarele situații:

- atunci când pentru îndeplinirea sarcinilor de serviciu ale persoanei deținătoare este necesar accesul la informații de nivel superior;
- la expirarea perioadei de valabilitate a certificatului de securitate /autorizației de acces deținute anterior;
- dacă apar modificări în datele de identificare ale persoanei;
- la apariția unor riscuri de securitate din punct de vedere al compatibilității accesului la informații secrete de stat.

Revalidarea avizului privind accesul la informații secrete de stat presupune reverificarea persoanei deținătoare a unui certificat de securitate / autorizație de acces în vederea menținerii sau retragerii acesteia.

Totodată, ORNISS poate solicita *reluarea verificărilor* la sesizarea autorităților competente, în situația în care sunt semnalate incompatibilități privind accesul la informații secrete de stat.

Certificatul de securitate/autorizația de acces își încetează valabilitatea și se *retrage* în următoarele cazuri:

- la solicitarea ORNISS;
- prin decizia conducătorului unității care le-a eliberat;
- la solicitarea autorității desemnate de securitate competente;
- la plecarea din unitate sau la schimbarea locului de muncă al deținătorului în cadrul unității, dacă noul loc de muncă nu presupune lucrul cu astfel de informații;
- la schimbarea nivelului de secretizare a informațiilor necesare îndeplinirii atribuțiilor de serviciu.

În cazuri excepționale, determinate de situații de criză, calamități sau evenimente imprevizibile, conducătorul unității poate acorda *acces temporar* la informații secrete de stat anumitor persoane care nu dețin certificat de securitate sau autorizație de acces, cu condiția asigurării unui sistem corespunzător de evidență.

Persoanele care primesc dreptul de acces temporar la informații secrete de stat semnează angajamentul de confidențialitate și au obligația să se conformeze procedurilor de verificare și avizare, în cel mai scurt timp.

Dacă în perioada în care se află în verificări de securitate, persoana în cauză încetează raporturile de muncă sau este transferată pe o funcție ce nu presupune accesul la informații secrete de stat, se solicită în scris Autorității Desemnate de Securitate, prin ORNISS, sistarea verificărilor.

Așa da: funcționarul de securitate din cadrul unui minister a notificat telefonic DGSI cu privire la situațiile în care urmează să se solicite sistarea verificărilor, anterior transmiterii documentelor la ORNISS și DGSI.

Așa nu: un angajat al unei primării a încetat raporturile de activitate cu instituția în cauză, funcționarul de securitate fiind notificat de DGSI cu privire la necesitatea sistării verificărilor; funcționarul a transmis, după 3 luni, solicitarea de sistare exclusiv la DGSI.

Persoanele cărora li se eliberează certificate de securitate/autorizații de acces vor fi instruite, obligatoriu, cu privire la protecția informațiilor secrete de stat, înaintea începerii activității și ori de câte ori este nevoie.

Planificarea și organizarea activității de pregătire a personalului se realizează de către structura/funcționarul de securitate.

Activitatea de pregătire se efectuează planificat, în scopul prevenirii, contracarării și eliminării riscurilor și amenințărilor la adresa securității informațiilor secrete de stat.

Pregătirea personalului se realizează diferențiat, potrivit nivelului de secretizare a informațiilor la care certificatul de securitate sau autorizația de acces permite accesul și va fi înscrisă în fișa individuală de pregătire, care se păstrează la structura/funcționarul de securitate.

După fiecare instruire, persoana care deține certificat de securitate sau autorizație de acces va semna că a luat act de conținutul reglementărilor privind protecția informațiilor secrete de stat.

Pregătirea personalului urmărește însușirea corectă a standardelor de securitate și a modului de implementare eficientă a măsurilor de protecție a informațiilor secrete de stat.

Pregătirea individuală a persoanelor care dețin certificate de securitate/autorizații de acces se realizează în raport cu atribuțiile profesionale.

Toate persoanele care gestionează informații secrete de stat au obligația să cunoască reglementările privind protecția informațiilor secrete de stat și procedurile interne de aplicare a măsurilor de securitate specifice.

Pregătirea personalului se realizează sub formă de lecții, informări, prelegeri, simpozioane, schimb de experiență, seminarii, ședințe cu caracter aplicativ și se poate finaliza prin verificări sau certificări ale nivelului de cunoștințe.

Activitățile de pregătire vor fi organizate de structura/funcționarul de securitate, conform tematicilor cuprinse în programele aprobate de conducerea unității.

Cu privire la acest aspect, instituția noastră vine în sprijinul structurilor de securitate prin implementarea unui proiect de consolidare a culturii de securitate - awareness, prin care, la solicitarea instituțiilor gestionare de informații secrete de stat, sunt organizate întâlniri, la sediul acestora, adresate unor grupuri țintă - persoane care sunt autorizate pentru accesul la informații secrete de stat, cu prezentarea unor teme aplicative.

Anual, autoritățile desemnate de securitate controlează, potrivit competențelor, modul de realizare a activității de pregătire a personalului care accesează informații secrete de stat.

Accesarea și gestionarea informațiilor din domeniul securității naționale

Persoanele cărora li se prezintă materiale de informare emise de **serviciile sau structurile departamentale de informații** răspund de asigurarea protecției acestora, având obligația de a exercita controlul permanent asupra păstrării și manipulării lor, pentru prevenirea pierderii, alterării, distrugerii, sustragerii sau divulgării datelor la care se referă.

Divulgarea, prin orice mijloace, de date și informații secrete de stat care pot aduce prejudicii intereselor de securitate națională, indiferent de modul în care au fost obținute, este interzisă și atrage, potrivit legii, răspunderea celor vinovați.

Comunicarea informațiilor de interes pentru securitatea națională se aprobă de către conducătorii organelor cu atribuții în domeniu.

Pot primi astfel de informații:

- președintele României, președintele Senatului, președintele Camerei Deputaților, precum și cei ai Comisiilor pentru Apărare și Asigurare a Ordinei Publice și Siguranței Naționale;
- prim - ministrul, miniștrii și șefii departamentelor din ministere, când informațiile privesc probleme ce au legătură cu domeniile de activitate pe care le coordonează sau de care răspund;
- prefecții, primarul general al Capitalei, precum și conducătorii consiliilor județene, respectiv al municipiului București, pentru probleme ce vizează competența organelor respective;
- organele de urmărire penală, când informațiile privesc săvârșirea unei infracțiuni.

Este interzisă punerea la dispoziția altor persoane a materialelor de informare în original, în copie sau în extras.

De asemenea, este interzisă scoaterea materialelor de informare din incinta instituției destinate, multiplicarea acestora, integral sau în parte, precum și aducerea la cunoștința persoanelor neautorizate a datelor pe care le conțin.

Astfel de materiale de informare se păstrează în containere sigilate, iar restituirea se realizează de către beneficiarii lor, care au obligația să închidă personal plicurile și să le remită emitentului, în condiții de maximă siguranță, după consultare.

Pierderea, alterarea, distrugerea, sustragerea ori transmiterea către persoane neautorizate a materialelor de informare, precum și divulgarea conținutului acestora se aduc de îndată la cunoștința emitentului, în vederea prevenirii și contracarării eventualelor consecințe în planul securității naționale și luării măsurilor ce se impun, potrivit legii.

Beneficiarii materialelor de informare au obligația să păstreze secretul asupra conținutului acestora, inclusiv după părăsirea, în orice mod, a funcției pe care o dețin.