R O M Â N I A
SERVICIUL ROMÂN DE INFORMAŢII

PROTECŢIA INFORMAŢIILOR CLASIFICATE

- ghid practic -

C U P R I N S

CAPITOLUL I
Informația clasificată. Informația nedestinată publicității și informația de interes public. Liberul acces la informații versus „necesitatea de a cunoaște” 2

CAPITOLUL II
Protecția personalului 12

CAPITOLUL III
Pregătirea specifică a persoanelelor care au acces la informații clasificate 25

CAPITOLUL IV
Regulile generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, transportul, transmiterea și distrugerea informațiilor clasificate 34

CAPITOLUL V
Protecția fizică..... 38

CAPITOLUL VI
Securitatea industrială 40

CAPITOLUL VII
Securitatea informațiilor clasificate în format electronic 57

CAPITOLUL VIII
Controlul măsurilor privitoare la protecția informațiilor clasificate 68

C A P I T O L U L I

INFORMAȚIA CLASIFICATĂ. INFORMAȚIA NEDESTINATĂ PUBLICITĂȚII ŞI INFORMAȚIA DE INTERES PUBLIC. LIBERUL ACCES LA INFORMAȚII VERSUS "NECESITATEA DE A CUNOAŞTE"

Potrivit Declarației Universale a Drepturilor Omului, *orice persoană are dreptul la libertatea opiniei și expresiei; acest drept include libertatea de a susține opinii fără nici o interferență și de a căuta, primi și răspândi informații și idei prin orice mijloace, indiferent de frontiere.*

Pornind de la conceptul global mai sus prezentat, Legea fundamentală a României consfințește, prin enunțul prevăzut la art. 31 alin. (1), principiul potrivit căruia *dreptul persoanei de a avea acces la orice informație de interes public nu poate fi îngrădit.*

În spiritul acestui principiu, autoritățile statului, potrivit competențelor ce le revin, sunt obligate să asigure informarea corectă a cetățenilor asupra activităților publice și a problemelor de interes personal ale acestora fără a se aduce, însă, atingere vieții intime, familiale și private, valori ocrotite, în egală măsură, de art. 26 din Legea fundamentală.

Prevăzând posibilitatea în care exercitarea dreptului la liberă informare ar putea să implice și unele acțiuni mai puțin legitime, ce ar putea să aibă ca efect vătămarea unor valori universal recunoscute și protejate, legiuitorul a stabilit, prin alineatul (3) al aceluiași articol, o excepție de la regula consacrată de alineatul (1).

Astfel, potrivit Constituției, *dreptul la informație nu trebuie să prejudicieze măsurile de protecție a tinerilor sau securitatea națională.*

În continuarea acestor prevederi, Legea fundamentală, prin articolul 53, reglementează posibilitatea și condițiile generice în care poate avea loc restrângerea unor drepturi sau libertăți constituționale, enumerând, limitativ, *motivele* pentru care exercițiul unui drept poate fi îngrădit: apărarea *siguranței naționale*, a ordinii, a sănătății ori moralei publice, a drepturilor cetățenilor, desfășurarea instrucției penale etc.

În mod justificat, în România, atât legiuitorul cât și societatea civilă au fost preocupați, pentru început, de elaborarea unui act normativ referitor la exercitarea dreptului constituțional al persoanei referitor la liberul acces la informațiile de interes public.

Astfel, a fost adoptată ***Legea nr. 544/2001 privind liberul acces la informațiile de interes public*** care definește, într-o manieră generală, informația de interes public, ca fiind orice informație care privește activitățile sau rezultă din activitățile unei autorități sau instituții publice, indiferent de suportul ori de forma sau modul de exprimare.

În scopul facilitării cunoașterii de către public a informațiilor mai sus definite, actul normativ stabilește, pentru autorități și instituții publice, dezmembrăminte sau structuri aflate sub autoritatea acestora, regii autonome, companii naționale etc., obligația de a comunica, *din oficiu*, anumite categorii de informații, stabilite prin art. 5 alin. (1) din lege. În acest sens, potrivit legii, entităților respective le revine sarcina de a publica și actualiza buletine informative cuprinzând categorii de informații care pot fi accesate de public sau de a prezenta publicității rapoarte periodice referitoare la activitatea pe care o desfășoară.

În plus față de informațiile care se comunică din oficiu publicului, orice persoană are dreptul să solicite și să obțină de la autorități și instituții publice informații de interes public, acestea fiind obligate să asigure accesul la datele solicitate în scris sau verbal.

Cu toate acestea, prevederile aceleiași legi limitează aria liberului acces la informație, instituind șapte excepții, dintre *care primele două vizează domeniul informațiilor clasificate*, astfel:

- informațiile din domeniul apărării nationale, siguranței și ordinii publice, dacă fac parte din categoriile informațiilor clasificate, potrivit legii;
- informațiile privind deliberările autorităților, precum și cele care privesc interesele economice și politice ale României, dacă fac parte din categoria informațiilor clasificate, potrivit legii;
- informațiile privind activitățile comerciale sau financiare, dacă publicitatea acestora aduce atingere principiului concurenței loiale, potrivit legii;
- informațiile cu privire la datele personale, potrivit legii;
- informațiile privind procedura în timpul anchetei penale sau disciplinare, dacă se periclitează rezultatul anchetei, se dezvăluie surse confidențiale ori se pun în pericol viața, integritatea corporală, sănătatea unei persoane, în urma anchetei efectuate sau în curs de desfășurare;
- informațiile privind procedurile judiciare, dacă publicitatea acestora aduce atingere asigurării unui proces echitabil ori interesului legitim al oricăreia dintre părțile implicate în proces;
- informațiile a căror publicare prejudiciază masurile de protecție a tinerilor.

În scopul eliminării oricărui dubiu referitor la posibilitatea ascunderii unor abuzuri ale organelor de stat prin clasificarea unor informații, Legea nr. 544/2001 prevede fără echivoc, la art. 13, faptul că nu pot fi incluse în categoria informațiilor clasificate și că, prin urmare, sunt informații de interes public, toate informațiile care favorizează sau ascund încălcarea legii de către o autoritate sau o instituție publică.

În ce privește informațiile care, deși nu sunt clasificate, nu pot fi puse la dispoziția publicului, trebuie menționat că, atât legislația în vigoare cât și practica unor autorități și instituții publice, au stabilit excepții referitoare la liberul acces la informații de interes public.

În continuare, vă vom prezenta, concret, câteva dintre aceste situații, identificate în diferite domenii de activitate.

1. ***În domeniul circumscris activității magistraților***, trebuie menționat că nu sunt supuse publicității discuțiile purtate între membrii completelor de judecată în procedura de deliberare, ci doar rezultatul lor, materializat în hotărârea judecătorească. De asemenea, nu se aduc la cunoștința publicului:

- informațiile referitoare la condamnarea unor minori;
- informațiile referitoare la identitatea martorilor sau alte date despre aceștia, dacă prin divulgarea lor s-ar pune în pericol viața, sănătatea sau integritatea corporală a acestora;
- informațiile rezultate din exercitarea prerogativelor instanțelor de judecată, care ar aduce atingere dreptului la intimitate al persoanei.

În acest context, subliniem că atât datele cu caracter personal puse la dispoziția Serviciului Român de Informații în vederea derulării procedurilor prealabile acordării avizului necesar eliberării certificatelor sau autorizațiilor de acces cât și

datele obținute ca urmare a derulării procedurii de vetting sunt protejate, în egală măsură, sub aspectul regulilor de securitate impuse de nivelul de secretizare atribuit acestora, cât și în respect pentru dreptul la intimitate al persoanei, drept garantat de Constituția României.

2. ***În materia elaborării proiectelor de acte normative,*** reglementările în vigoare interzic personalului autorităților publice inițiatoare și avizatoare furnizarea în afara instituțiilor respective a unor date sau informații cu privire la respectivele proiecte de acte normative, pe întreg parcursul procedurii de elaborare.

3. ***Ajungând la domeniul statisticii oficiale***, potrivit art. 19 din Ordonanța Guvernului nr. 9/1992 privind organizarea acestei activități, datele și informațiile statistice reprezintă un bun național, accesibil Parlamentului, Președintelui României, Guvernului, instituțiilor administrației publice centrale și locale, partidelor politice, sindicatelor, organizațiilor patronale, organizațiilor neguvernamentale, mijloacelor de informare în masă etc., cu respectarea principiului confidențialității datelor.

Cu toate acestea, serviciilor de statistică oficială și personalului statistic le revine obligația de a adopta și asigura, pe parcursul întregii perioade a cercetării statistice, de la înregistrare până la publicare, măsuri de asigurare a confidențialității datelor care se referă la subiecți statistici individuali - persoane fizice sau juridice - obținute direct prin cercetări statistice sau indirect, din surse administrative ori din alte surse.

4. ***Legea nr. 677/2001*** stabilește măsuri și proceduri referitoare la gestionarea datelor cu caracter personal, în vederea garantării și protejării drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, în raport cu acest tip de date.

În acest sens, interzice prelucrarea, fără acordul persoanei vizate, a datelor cu caracter personal legate de origine rasială sau etnică, de convingeri politice, religioase, filozofice, de apartenenţă sindicală etc.

În aplicarea acestei legi a fost emis Ordinul Avocatului Poporului nr. 75/2002 privind stabilirea unor măsuri şi proceduri specifice care să asigure un nivel satisfăcător de protecţie a drepturilor persoanelor ale căror date cu caracter personal fac obiectul prelucrărilor.

Măsurile şi procedurile au ca scop asigurarea unui nivel corespunzător de protecţie a datelor, de către membrii entităţilor de drept public sau privat), prin stabilirea modalităţilor de exercitare a drepturilor şi obligaţiilor care le revin în domeniul protecţiei persoanelor.

Potrivit Ordinului, nivelul de protecţie şi de securitate adecvat al prelucrărilor de date cu caracter personal reprezintă nivelul de securitate proporţional riscului pe care îl comportă lucrarea faţă de datele cu caracter personal în cauză, faţă de drepturile şi libertăţile persoanelor şi conform cerinţelor minime de securitate stabilite de autoritatea de supraveghere competentă.

5. La 14 mai a.c. a fost adoptată ***Legea privind arhivarea documentelor în formă electronică*** (nr. 135) prin care se stabileşte regimul juridic aplicabil gestionării documentelor în formă electronică sau care urmează a fi arhivate într-o arhivă digitală. De asemenea, sunt reglementate reguli referitoare la constituirea arhivelor de acest tip şi, în egală măsură, sancţiuni de natură contravenţională sau penală care devin aplicabile în cazul divulgării, accesării, copierii, modificării ori distrugerii neautorizate a arhivelor.

Revenind la practica asigurării unui regim de protecţie a informaţiilor neclasificate, din prisma limitării accesului

publicului la acestea, menționăm că aceasta se regăsește atât la nivelul structurilor administrative ale Uniunii Europene cât și în cadrul Organizației Tratatului Atlanticului de Nord, ambele organizații stabilind categorii de informații care, deși nu sunt clasificate, au un caracter sensibil și sunt destinate doar personalului autorizat (LIMITÉ, pentru UE și UNCLASSIFIED, pentru NATO).

În legătură cu dezbaterile pe marginea liberului acces la informațiile publice, este de remarcat că, în anul 1996, un grup de experți de diferite naționalități a redactat un set de principii referitoare la securitatea națională, accesul la informații și libertatea de exprimare, cunoscute îndeobște ca "***Principiile de la Johanesburg***".

În esență, acestea urmăresc instituirea unei protecții substanțiale pentru accesul la informație și libertatea de exprimare, concomitent cu limitarea posibilităților autorităților de a restrânge exercitarea acestora, pe diferite considerente legate de interese de securitate.

Două dintre aceste principii, relevante în context, ar fi:

Principiul 12:
"Un stat nu poate refuza categoric accesul la toate informațiile privind securitatea națională și trebuie să stabilească prin lege categorii limitate și particulare de informații care trebuie ținute secrete pentru a proteja interese legitime de securitate națională."

Principiul 13:
"În toate legile și deciziile privind dreptul de a obține informații, va prima interesul public în cunoașterea informațiilor."

Principiile de la Johanesburg nu constituie norme obligatorii, însă, oficiali ai Organizației Națiunilor Unite, ai Curții Europene a Drepturilor Omului, precum și ai altor organisme jurisdicționale internaționale, se raportează tot mai frecvent la acestea, considerând oportună transformarea lor în standarde.

În Europa, din punctul de vedere al tradiției reglementării dreptului de acces la informații publice, Suedia este unul dintre primele state care a introdus în Constituția sa, încă din 1766, prevederi dedicate accesului la informații publice.

Totodată, Suedia este prima țară din lume al cărei parlament a adoptat o lege a accesului la informația de interes public (*Legea libertății presei*, 1766), care prevedea că documentele oficiale trebuie *"la cerere, puse la dispoziția oricărei persoane"*, fără perceperea vreunei taxe.

Deciziile autorităților de a refuza accesul la documente oficiale pot fi atacate la tribunalele administrative generale și, în ultimă instanță, la Curtea Supremă Administrativă.

În România, după intrarea în vigoare a Legii nr. 544, având ca suport esențial atât principiile fundamentale definite de Constituție, cât și nevoia de compatibilizare a legislației naționale de securitate cu standardele euro-atlantice și cu exigențele general valabile în toate statele cu tradiție democratică în materia securității, Parlamentul României a adoptat *Legea privind protecția informațiilor clasificate (nr. 182/2002)* prin care au fost a înlocuite vechile reglementări referitoare la apărarea secretului, utilizate încă din anii '70.

Prin intrarea în vigoare a legii sus-menționate au fost instituite limitele dreptului persoanei la informații, prin definirea *informațiilor clasificate* și stabilirea *condițiilor speciale* în care acestea pot fi accesate.

Respectând principiul de bază potrivit căruia atunci când o informație trebuie clasificată, acesteia i se va atribui un nivel de secretizare ce va evidenția importanța relativă în sistemul național de securitate, actul normativ reglementează o ierarhie a ceea ce este cunoscut deja sub numele de *informații clasificate*, stabilind după cum cunoașteți deja, două clase și patru niveluri de importanță a informațiilor.

În „lexiconul" Organizației Tratatului Atlanticului de Nord, *clasificare* înseamnă *etichetări crescătoare ale documentelor sau informațiilor, de la cel mai jos nivel, unde se situează informațiile deschise (open) sau neclasificate (unclassified), la cele confidențiale, urcând spre informații secrete și strict secrete (top secret).*

Inițial, la nivelul Organizației s-a pornit de la idea că informațiile care, prin compromitere, *pot costa vieți umane* sunt marcate *"secret"*, în timp ce informațiile a căror compromitere *costă pierderea multor vieți umane* sunt definite *strict secrete (top secret)*.

În alte țări, evoluția problematicii din domeniile specializate precum și a ierarhiilor și considerentelor de clasificare a informațiilor a avut ca efect, pe lângă atribuirea unor niveluri de secretizare care să reflecte importanța informațiilor în raport cu interesele de securitate, și stabilirea de criterii noi în sensul împărțirii informațiilor clasificate, după domeniile sau interesele de securitate avute în vedere, și în strânsă legătură cu *principiul necesității de a cunoaște*.

Spre exemplu, structura neierarhizată a informațiilor secrete, utilizată în sistemele altor state, conține categorii de *informații clasificate compartimentate*, stabilite astfel în scopul identificării anumitor domenii de activitate în care sunt utilizate (CRIPTA - criptare, SECOM - securitatea comunicației, COMSEC - comunicații secrete ș.a.) sau *informații clasificate cu obiecții* care

privesc îndeosebi naționalitatea potențialilor cititori (ex: în SUA informațiile pot fi marcate cu diverse tipuri de *disclaimer* cum ar fi NOFOR - *nu sunt accesibile străinilor*; în Marea Britanie unele categorii de informații poartă marcajul UK EYES ONLY - *se pot vedea numai de către cetățeni englezi*).

Spre deosebire de accesarea informațiilor de interes public, care pot fi cunoscute de către cetățeni în virtutea drepturilor stabilite prin Constituție, cu respectarea condițiilor impuse de dispozițiile Legii nr. 544/2001, accesul la informațiile clasificate nu este posibil fără îndeplinirea, cumulativă, a două condiții esențiale, stabilite prin lege, respectiv existența necesității de a cunoaște și a certificatului de securitate / autorizației de acces, emisă în condițiile legii.

În ce privește *principiul necesității de a cunoaște*, legea română definește această sintagmă ca fiind *principiul conform căruia accesul la informații clasificate se acordă, în mod individual, numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să lucreze cu astfel de informații sau să aibă acces la acestea.*

În încheierea acestui prim capitol introductiv, față de cele de mai sus se poate afirma că, în timp ce pentru cunoașterea informațiilor de interes public, temeiul accesării acestora este reprezentat de drepturile constituționale ale cetățeanului, exercitate în scopul satisfacerii unor interese de natură personală, accesul la informațiile clasificate, în condițiile legii, este permis doar din necesitatea exercitării corecte a prerogativelor și atribuțiilor profesionale ale persoanei / autorizate în acest sens.

C A P I T O L U L II

PROTECȚIA PERSONALULUI

Potrivit *Standardelor naționale de protecție a informațiilor clasificate în România, aprobate prin HG nr. 585/2002*, cu modificările şi completările ulterioare, protecția personalului se realizează prin: selecționarea, verificarea, avizarea (revalidarea) şi autorizarea accesului utilizatorilor informațiilor clasificate, neacordarea avizului de securitate, retragerea certificatului de securitate sau autorizației de acces, activități de instruire.

Selecționarea persoanelor care urmează să ocupe funcții ce presupun accesul la informații clasificate se derulează integral şi exclusiv în cadrul fiecărei instituții deținătoare de informații clasificate.

Conform *Standardelor naționale*, conducătorii autorităților, instituțiilor publice, agenților economici cu capital integral sau parțial de stat şi celorlalte persoane juridice de drept public sau privat aprobă *Listele funcțiilor care presupun accesul la informații clasificate* (este necesară evaluarea atribuțiilor specifice fiecărei funcții din statul de organizare al instituției, pentru a stabili dacă necesită acces la informații clasificate şi nivelul de secretizare aferent).

La dimensionarea listei funcțiilor care presupun acces la informații clasificate se au în vedere:

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

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

Procedura de *verificare* se efectuează de autoritățile desemnate de securitate și are drept scop identificarea **vulnerabilităților de securitate -** caracteristici de personalitate sau circumstanțe care: a) pun în pericol securitatea informațiilor clasificate, b) pot fi exploatate pentru a se influența persoana să se implice în acte de diseminare neautorizată de informații clasificate și **amenințărilor de securitate -** persoane care sprijină obiectivele unor entități (ex - structuri informative, grupuri de interese) de a avea acces neautorizat la informații clasificate, pentru a se preveni apariția **riscului de securitate –** accesul la informații clasificate va avea drept consecință compromiterea sau/și diseminarea acestora către persoane neautorizate.

Verificarea în vederea avizării pentru acces la informații secrete de stat se efectuează de către:

a) *Serviciul Român de Informații,* pentru:

- personalul propriu;
- personalul autorităților și instituțiilor publice din zona de competență, potrivit legii;
- personalul agenților economici cu capital integral sau parțial de stat și al persoanelor juridice de drept public sau privat, altele decât cele din competența Ministerului Apărării, Serviciului de Informații Externe, Ministerului Administrației și Internelor, Ministerului Justiției,

Serviciului de Protecție și Pază și Serviciului de Telecomunicații Speciale.

b) *Ministerul Apărării,* pentru personalul militar și civil propriu, inclusiv personalul militar care își desfășoară activitatea în străinătate.

c) *Ministerul Administrației și Internelor,* pentru:

- personalul propriu și al persoanelor juridice a căror activitate o coordonează;
- personalul Oficiului Central de Stat pentru Probleme Speciale, Administrației Naționale a Rezervelor de Stat și al altor persoane juridice stabilite prin lege.

d) *Serviciul de Informații Externe,* pentru:

- personalul militar sau civil propriu;
- personalul român al reprezentanțelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internaționale și altor reprezentanțe ale statului român în străinătate;
- cetățenii români aflați în străinătate în cadrul unor contracte, stagii de perfecționare, programe de cercetare sau în calitate de angajați ai unor firme.

e) *Ministerul Justiției, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale*, pentru personalul propriu și al persoanelor juridice a căror activitate o coordonează.

Întrucât verificările se efectuează pe baza datelor completate în formularele de securitate, respectiv în unele situații e necesar să se realizeze și interviul de securitate, următoarele aspecte sunt relevante în ceea ce privește emiterea unui aviz de securitate: refuzul de a completa rubrici din formularul de securitate, omisiunile voluntare, ascunderea și falsificarea unor aspecte, refuzul clarifica situații relevante în cadrul interviului de securitate - *consecința negativă constă în*

faptul că verificarea de securitate nu se realizează în condiții de suficiență a datelor.

În acest caz, persoanei i se va preciza necesitatea unei cooperări pentru furnizarea datelor și / sau clarificarea aspectelor rezultate din verificări, respectiv că un refuz respectiv devine o bază legitimă pentru returnarea formularelor de securitate/sistarea verificărilor de securitate.

COMPLETAREA FORMULARELOR DE SECURITATE

În vederea asigurării operativității în ceea ce privește emiterea avizului de securitate, facem următoarele recomandări în ceea ce privește completarea formularelor tip:

RECOMANDĂRI GENERALE

- Rezervați timp suficient pentru citirea cu atenție a rubricilor/întrebărilor!
- Asigurați-vă că ați completat toate rubricile, respectiv ați răspuns la toate întrebările (și, unde era cazul, ați precizat detaliile)!
- Asigurați-vă că ați semnat Declarația (nu modificați conținutul)!

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

- La întrebări bifați răspunsurile de tip DA/NU (anulați celălalt răspuns)!

Exemplu

1. – unde sunt prevăzute casete

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

DA	
NU	X

2. – unde nu sunt prevăzute casete, consemnați dvs. DA/NU.

Ați consumat sau consumați substanțe care creează dependență sau droguri?

Dacă răspunsul este afirmativ, detaliați: ***NU***

S-ar putea invoca faptul că dacă nu s-a răspuns cu DA, atunci răspunsul implicit este NU, dar s-a constatat că au fost persoane care au fost implicate în astfel de contexte și au motivat lipsa răspunsului DA prin faptul că "a fost o singură dată, în adolescență" (nn. deși întrebarea nu face diferențieri), dar că apreciază că nu au mințit, pentru că nu au consemnat NU, respectiv "nu au știut dacă să consemneze sau nu".

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

Dacă ați bifat NU, dar totuși există o situație "sensibilă" în legătură cu care nu sunteți sigur că se încadrează la cerințe, este recomandabil să o consemnați și să detaliați (este de preferat să existe mențiuni suplimentare decât să se interpreteze ca o omisiune deliberată a unor date). Dacă ați bifat DA, pe lângă situația certă care se încadrează la cerințe, menționați și situația sensibilă.

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.

- Detaliați denumirile! (ex: Direcția Generală de Export, nu DGE)
- Încercați să completați cu majuscule, pentru a se evita ca scrisul să fie ilizibil!
- Evitați să faceți mențiuni în formularul tip - cum ar fi faptul că datele solicitate se regăsesc în alte documente - și să nu completați rubricile; cel mult, faceți copii după respectivele documente, pe care le puteți anexa la formularele tip, iar la rubrici menționați "conform copiilor anexate".
- Dacă este nevoie să detaliați în scris anumite situații, puteți anexa respectivele file la formularele tip (precizați numele/prenumele pe fiecare filă și semnați).

- Dacă apreciați că este necesar, pentru clarificarea anumitor situații, puteți anexa la formularele tip și copii după documente (precizați numele/prenumele pe fiecare filă și semnați).

Vă recomandăm să păstrați datele referitoare la rude (și alte date pentru care demersurile de obținere sunt dificile), întrucât în cadrul procedurii de revalidare se va solicita ***recompletarea integrală*** *a formularelor tip.*

RECOMANDĂRI SPECIFICE
(**completarea unor rubrici din formulare**)

Datele de identitate – conform buletinului/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 buletinului/cărții de identitate
Domiciliul flotant – precizați și domiciliul unde locuiți efectiv (chiar dacă nu sunteți înregistrat cu acesta în evidențele oficiale)

Notă *– dacă apreciați, puteți preciza perioadele pentru fiecare adresă, respectiv, în cazul închirierii, proprietarii locuințelor (pentru identificarea conformității adresei cu evidențele oficiale)*

Situația familială – consemnați și persoana cu care aveți o relație apropiată și care poate fi inclusă în categoria "partener de viață" (chiar dacă nu locuiți împreună)
Locurile de muncă – menționați toate locurile de muncă pe care le-ați avut (cu titulatura completă și corectă), respectiv precizați, în cazul în care nu există continuitate între perioadele de angajare, care este motivul (șomaj, studii în străinătate etc)
Funcția – conform cu *Lista funcțiilor care necesită acces la informații secrete de stat,* emisă de către instituție (consultați funcționarul de securitate)
Referințe – evitați să consemnați rude (să fie persoane cu care ați păstrat o legătură constantă în ultimii cinci ani)
Sunteți interesat, dvs. sau partenerul de viață în colaborarea cu anumite societăți comerciale înregistrate în țară?
Menționați firmele la care dvs. sau partenerul de viață: a) sunteți înregistra cenzor, membru în Consiliul de administrație etc și/sau b) aveți calitatea de contracte de colaborare, se prestează o activitate voluntară etc.

Aveți relații, dvs. sau partenerul de viață cu firme înregistrate în stră
Dacă ați renunțat recent la calitatea de administrator, asociat etc, consemnați societățile și faceți precizarea respectivă (după caz, anexați și copii după documente care demonstrează acest lucru).

Referitor la formularele tip, **dacă** se apreciază că ar fi inoportun ca funcționarul de securitate să cunoască involuntar unele date, se poate proceda astfel:

1. Se pun la dispoziția solicitantului formularele tip (în funcție de nivelul de acces) și i se aduc la cunoștință recomandările sus-menționate (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 datele și solicită ca în prezența sa funcționarul de securitate să le înregistreze; acest demers presupune că funcționarul are acces numai la prima pagină a formularului de securitate – solicitantul introduce formularele într-un plic pe care îl sigilează (se scriu datele de identitate pe plic).

La completarea formularelor de securitate, este posibil ca solicitantul să nu menționeze unele răspunsuri pentru că nu a înțeles cerințele / întrebarea, a fost superficial/neatent sau nu i s-au prezentat instrucțiunile specifice – de aceea, funcționarul de securitate trebuie să explice necesitatea completării datelor și a furnizării de date suplimentare în cazul unor eventuale neclarități (respectiv să creeze condițiile pentru a completa respectivele date).

Principalele *criterii de evaluare a compatibilității* în acordarea avizului pentru eliberarea certificatului de securitate sau autorizației de acces *vizează* atât *trăsăturile de caracter*, cât și *situațiile sau împrejurările din care pot rezulta amenințări și vulnerabilități de securitate*.

Sunt relevante și se iau în considerare la acordarea avizului de securitate *caracterul, conduita profesională sau socială, concepțiile și mediul de viață al soțului / soției sau concubinului / concubinei persoanei solicitante*.

Decizia privind avizarea eliberării certificatului de securitate sau autorizațiilor de acces se ia pe baza tuturor informațiilor disponibile și are în vedere:

- loialitatea indiscutabilă a persoanei;
- caracterul, obiceiurile, relațiile și discreția persoanei, care să ofere garanții asupra corectitudinii în gestionarea informațiilor secrete de stat, oportunității accesului neînsoțit în compartimente, obiective, zone și locuri de securitate în care se află informații secrete de stat și respectării reglementărilor privind protecția informațiilor secrete de stat din domeniul său de activitate.

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

- 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;
- 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;

- 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;
- dacă este sau a fost un susținător al vreunei organizații prevăzute la punctul anterior, 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*:

- 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;
- are antecedente penale sau a fost sancționat contravențional pentru fapte care indică tendințe infracționale;
- are dificultăți financiare serioase sau există o discordanță semnificativă între nivelul său de trai și veniturile declarate;
- consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau alte substanțe interzise prin lege, care produc dependență;
- are sau a avut comportamente imorale sau deviații de comportament care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni;
- a demonstrat lipsă de loialitate, necinste, incorectitudine sau indiscreție;

- a încălcat reglementările privind protecția informațiilor clasificate;
- 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;
- 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.

Accesul la informații secrete de stat este permis numai persoanelor care dețin certificat de securitate sau autorizație de acces de nivel corespunzător nivelului de secretizare al informațiilor necesare îndeplinirii atribuțiilor de serviciu, în condițiile respectării principiului *"necesității de a cunoaște"(* accesul se acordă în mod individual numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să aibă acces la acestea; astfel, accesul la diferite categorii de informații nu va fi permis numai pe baza funcției, poziției sau a deținerii autorizației de acces).

Dacă, ulterior solicitării avizului la ORNISS, 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, prin ORNISS, sistarea verificărilor.

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.

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

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

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 clasificate.

În situația în care se solicită revalidarea, nu se eliberează un nou certificat de securitate/autorizație de acces în următoarele situații:

- dacă se constată neconcordanțe între datele declarate în formularele tip și cele reale;
- dacă, pe parcursul perioadei de valabilitate a certificatului de securitate/autorizației de acces s-au evidențiat riscuri de securitate;
- în cazul în care ORNISS solicită acest lucru, în mod expres.

Persoanelor cărora li se eliberează certificate de securitate sau autorizații de acces li se asigură *instruirea* cu privire la protecția informațiilor clasificate, înaintea începerii activității și ori de câte ori este nevoie.

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

Organizarea și coordonarea activității de pregătire a structurilor / funcționarilor de securitate sunt asigurate de ORNISS și de autoritățile desemnate de securitate. Planificarea și organizarea activității de pregătire a personalului care în exercitarea atribuțiilor de serviciu lucrează cu informații clasificate se realizează de către funcționarul de securitate.

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

Studiu de caz

În anul 2004, POPESCU POP, funcționar de stat, a fost avizat pentru acces la informații clasificate, nivel "strict secret".

În anul 2005, au rezultat informații că persoana în cauză, sub pretextul că avea lucrări profesionale urgente de realizat, pleca la domiciliu cu laptop-ul pe care redacta la serviciu documente cu caracter clasificat, respectiv îl conecta la locul de muncă la Internet, motivând că era necesar în interes de serviciu.

În acest context, s-a efectuat un control la începerea programului de lucru la punctul de acces în sediul instituției, constatându-se că POPESCU POP avea asupra sa laptop-ul, respectiv că pe acesta se aflau documente clasificate; de altfel, prin auditarea informatică a rezultat și că acesta fusese contectat la rețeaua Internet. De asemenea, a rezultat că în normele interne ale instituției referitoare la protecția informațiilor clasificate, era stipulat explicit că ***este interzis să fie scoase din sediu calculatoare pe care se gestionau informații clasificate, respectiv ca acestea să fie conectat la Internet.***

Astfel, avându-se în vedere că la art. 236 din Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin HG nr. 585/2002 se precizează că "modalitățile și măsurile de protecție a informațiilor clasificate care se prezintă în format electronic sunt similare celor pe suport hârtie", întrucât nu s-au respectat cerințele ***art. 121*** *– "informațiile secrete de stat se păstrează în containere speciale, astfel…container clasa B, autorizate la nivel național pentru păstrarea informațiilor strict secrete și secrete în zone de securitate clasa I sau clasa a II-a" și* ***art. 81*** *– "documentele și materialele ce conțin informații clasificate se transportă, pe teritoriul României, prin intermediul unității specializate a SRI, potrivit normelor stabilite prin hotărâre a Guvernului", respectiv nu s-au respectat normele interne ale instituției, situația s-a raportat la elementul de incompatibilitate de la art. 160 lit. g) din Standarde - a încălcat reglementările privind protecția informațiilor clasificate, și* ***s-a retras avizul de securitate****.*

C A P I T O L U L III

PREGĂTIREA SPECIFICĂ A PERSOANELOR CARE AU ACCES LA INFORMAȚII CLASIFICATE

În aplicarea cadrului normativ general în domeniul protecției informațiilor clasificate și a normelor interne elaborate la nivelul unităților care gestionează astfel de informații, segmentul cel mai vulnerabil în funcționarea sistemului de protecție se dovedește a fi *componenta umană*.

În aceste condiții, *protecția personalului* - definită de Legea nr. 182 din 12.04.2002 privind protecția informațiilor clasificate, ca reprezentând "*ansamblul verificărilor și măsurilor destinate persoanelor cu atribuții de serviciu în legătură cu informațiile clasificate, spre a preveni și înlătura riscurile de securitate pentru protecția informațiilor clasificate*" (art.15 lit.j) - dobândește o dimensiune aparte, conferită de incertitudinea și imprevizibilitatea factorului uman.

Prin urmare, în managementul resurselor umane, este necesar să se aibă în vedere:

- *"ecuația personală" unică a individului* (temperament, trăsături de caracter, inteligență, aptitudini, adaptabilitate etc.);
- *motivația personală în exercitarea atribuțiilor profesionale*;
- *necesitatea formării continue*;
- *standardele de competență*.

Protecția personalului se realizează prin parcurgerea unui ansamblu de etape ce reprezintă, în esență, tot atâtea măsuri de protecție a informațiilor clasificate: selecționarea, verificarea, avizarea și autorizarea accesului la informațiile secrete de stat, revalidarea, controlul și *instruirea personalului*, retragerea certificatului de securitate sau autorizației de acces.

Așa cum am menționat și anterior, accesul la informații clasificate este permis numai persoanelor care dețin certificat de securitate/autorizație de acces de nivel corespunzător, cu respectarea principiului "*necesității de a cunoaște*" *și doar în urma unei pregătiri prealabile*.

Ca măsură specifică de securitate, *formarea personalului* se subsumează scopurilor măsurilor protecție a personalului:

- să prevină accesul persoanelor neautorizate la informații secrete de stat;
- să garanteze că informațiile secrete de stat sunt distribuite deținătorilor de certificate de securitate / autorizații de acces, cu respectarea principiului "*necesității de a cunoaște*";
- 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.

Mai mult, ea constituie singura măsură de protecție care vizează optimizarea funcționării sistemului de protecție a personalului, la nivelul de bază, cel al individului care accesează informațiile clasificate.

În îndeplinirea atribuțiilor generale ce îi revin potrivit *Standardele* aprobate prin H.G. nr. 585/2002, structura sau funcționarul de securitate, *planifică și organizează* activități de pregătire specifică a persoanelor cu acces la informații clasificate.

Funcționarul de securitate ori, după caz, membrii structurii de securitate desemnați cu atribuții pe linia pregătirii personalului care accesează informații secrete de stat, vor avea stipulate aceste atribuții în *fișa postului*. Exercitarea, atribuțiilor legale în domeniul pregătirii personalului care accesează informații clasificate, implică și capacitatea de a oferi *consiliere*, în acest domeniu, conducătorului unității.

Standardele naționale fixează finalitățile de ordin strategic - *scopurile* - organizării activităților de pregătire specifică a persoanelor care au acces la informații clasificate. Acestea sunt ***prevenirea, contracararea și eliminarea riscurilor și amenințărilor la adresa informațiilor clasificate***.

De asemenea, precizează *obiectivele generale* ale pregătirii personalului în domeniul protecției informațiilor clasificate sunt:

- însușirea corectă a standardelor de securitate;
- însușirea corectă a modului de implementare eficientă a măsurilor de protecție a informațiilor clasificate.

Din punct de vedere conceptual, termenul „*însușire*" presupune două aspecte complementare, cel *informativ* și cel *formativ*. Abordarea celor două aspecte în *pregătirea personalului în domeniul protecției informațiilor clasificate* trebuie realizată etapizat:

- *formarea inițială* – înaintea numirii în funcție și acordării accesului la informații clasificate;
- *formarea continuă* – periodic, la intervale prestabilite și ori de câte ori este nevoie, astfel încât informațiile clasificate să fie protejate în mod corespunzător.

Etapa de *pregătire inițială* a personalului implică – în primă fază – însușirea unui set de cunoștințe teoretice de bază privind protecția informațiilor clasificate și reprezintă o condiție necesară acordării accesului la astfel de informații.

Astfel, potrivit *Standardelor*, la sfârşitul activității de pregătire inițială, cursanții trebuie să facă dovada următoarelor:

achiziții cognitive

- cunoaşterea reglementărilor privind protecția informațiilor clasificate;
- cunoaşterea procedurilor interne de aplicare a măsurilor de securitate specifice.

Acestea vor fi detaliate şi particularizate în funcție de achizițiile preconizate şi de domeniul specific de activitate, astfel încât să acopere toate componentele sistemului de protecție a informațiilor clasificate.

În continuare, pe parcursul *pregătirii continue*, trebuie avută în vedere articularea laturii informative cu cea formativă. În acest sens, pot fi punctate o serie de achiziții necesare culturii organizaționale de securitate şi lucrului în domenii ce presupun acces la informații clasificate:

atitudini

- respectarea legislației şi a normelor interne în materia informațiilor clasificate;
- respectarea deontologiei profesionale şi a partenerilor socio-profesionali;
- responsabilitatea față de valorile care necesită protecție (informațiile clasificate);

deprinderi

- atenția distributivă orientată spre sesizarea circumstanțelor, elementelor ori fenomenelor care constituie ori pot degenera în factori de insecuritate;
- autocontrolul reacțiilor în condiții de stres ori situații-limită.

competențe

- aplicarea unor modele acționale prestabilite (proceduri de urgență, informarea funcționarului / șefului structurii de securitate, sesizarea autorității desemnate de securitate);
- evaluarea situațiilor-problemă (delimitarea problemei, identificarea elementului problematic, analiza implicațiilor, pertinența modului de acțiune, obiectivitatea aprecierilor);
- identificarea de soluții la probleme atipice și asumarea deciziei rapide în situații-limită.

Transmiterea valorilor de securitate în materia protecției informațiilor clasificate, face obiectul unui demers anticipativ, prin *programele de pregătire a personalului*. Responsabilitatea elaborării acestora revine structurii / funcționarului de securitate, care le supune aprobării conducătorului unității.

Acestea vor conține *tematici de pregătire*, pe baza cărora structura de securitate organizează *activitățile de pregătire*.

Având în vedere că activitatea de formare implică specializare atât în domeniul protecției informațiilor clasificate, cât și în domeniul științelor educației, instituțiile care se confruntă cu necesități de formare a personalului sunt puse în situația de a opta pentru una dintre următoarele variante:

- specializarea personalului prin participarea la cursuri și stagii de formare, organizate de către autorități ori instituții acreditate pentru activități de formare în domeniul protecției informațiilor clasificate;
- formarea unor formatori interni specializați în domeniul protecției informațiilor clasificate;
- angajarea de formatori acreditați, pentru necesitățile de formare cărora instituția nu le poate face față prin resurse proprii;

- pregătirea individuală la locul de muncă, sub îndrumarea unor experți proprii în domeniu, abilitați și pentru activități de formare;
- autoinstruire și autodezvoltare asistată a capacităților profesionale la locul de muncă.

Pregătirea inițială și continuă a personalului se realizează prin diferite *tehnici de formare*, alese funcție de tipul obiectivelor urmărite:

- pentru însușirea legislației, a normelor și procedurilor interne se utilizează *tehnici cu dominantă informativă* – lecții, informări, prelegeri, simpozioane;
- pentru formarea atitudinilor, deprinderilor și competențelor privind lucrul cu informații clasificate, *tehnici cu dominantă formativă* - schimb de experiență, seminarii, ședințe cu caracter aplicativ.

Evaluarea rezultatelor activităților de instruire se realizează prin *verificări finale*, însoțite de *certificarea nivelului de cunoștințe*. Acestea pot fi precedate de *verificări parțiale*, pe domenii sau etape de pregătire.

În pregătirea personalului se aplică *principiul diferențierii* în funcție de nivelul de secretizare a informațiilor la care persoana este autorizată ori certificată să aibă acces.

Mai mult, tematicile de pregătire inițială și continuă trebuie *individualizate* în acord cu atribuțiile profesionale. Astfel, conținuturile și tehnicile de formare trebuie adaptate necesităților de pregătire a:

- *experților* din cadrul structurilor de securitate;
- *formatorilor* în domeniul protecției informațiilor clasificate;
- altor categorii de *personal* cu acces la informații clasificate.

Participarea la fiecare activitate de pregătire se consemnează în *fișa individuală de pregătire* care se păstrează de structura/funcționarul de securitate. După fiecare astfel de activitate de pregătire, 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.

Feed-back-ul realizat pe perioada activităților de instruire permite formatorului și, implicit, funcționarului/structurii de securitate *identificarea riscurilor și vulnerablităților* existente în sistemul de protecție a informațiilor clasificate, datorate unei pregătiri necorespunzătoare a personalului care accesează astfel de informații.

Prin informarea conducătorului unității și propunerea de măsuri în consecință, pot fi eliminate premisele producerii unor incidente de securitate.

Domeniul culturii de securitate clasificate este în plină dezvoltare. Din acest motiv, și în domeniul particular al protecției informațiilor clasificate, conceperea programelor și tematicilor de pregătire va trebui abordată într-o manieră prospectivă și să răspundă unor exigențe pedagogice:

- obiectivele să fie stabilite corect în relație cu necesitățile de formare ale momentului și cu direcțiile de evoluție a problematicii în materia securității informațiilor clasificate;
- conținutul științific să fie dimensionat astfel încât să acopere integral și echilibrat obiectivele proiectate și, de asemenea, să permită actualizarea facilă;
- strategia de formare să fie concepută în manieră interactivă și flexibilă, adaptată corect obiectivelor, conținutului curricular și resurselor umane implicate;

- realizarea unui raport optim între dimensiunea informativă (transmiterea de cunoștințe) și cea formativă (cultivarea de atitudini, deprinderi și competențe);
- diferențierea formării inițiale și continue, în relație cu natura atribuțiilor profesionale și cu dinamica necesităților de pregătire în domeniul protecției informațiilor clasificate;
- formarea continuă a formatorilor în acord cu evoluțiile legislației în materia informațiilor clasificate și în domeniul științelor educației;
- dezvoltarea și întreținerea motivației principalilor actori (formatorii și cursanții) pentru problematica abordată;
- alocarea și gestionarea corectă a resurselor materiale, financiare, de timp și umane;
- evaluarea periodică (semestrială, anuală etc) a programului în vederea actualizării și optimizării.

La nivelul sistemului național de protecție a informațiilor clasificate, în conformitate cu atribuțiile legale privind coordonarea generală a activității și exercitarea controlului asupra măsurilor privitoare la protecția informațiilor clasificate, în sfera sa de competență, Serviciul Român de Informații *organizează și coordonează activitatea de pregătire a structurilor de securitate*, prin *programe permanente de pregătire*. De asemenea, desfășoară activități de pregătire a personalului cu atribuții pe linia protecției informațiilor clasificate, vehiculate în cadrul activităților industriale.

Importanța pregătirii personalului care accesează informații clasificate este evidențiată de obligația ce revine autorităților desemnate de securitate – printre care și SRI –

privind exercitarea controlul asupra modului de realizare a acestei activități.

Instruirea corespunzătoare a personalului reprezintă una dintre condițiile eliminării riscurilor și evitării producerii evenimentelor de securitate.

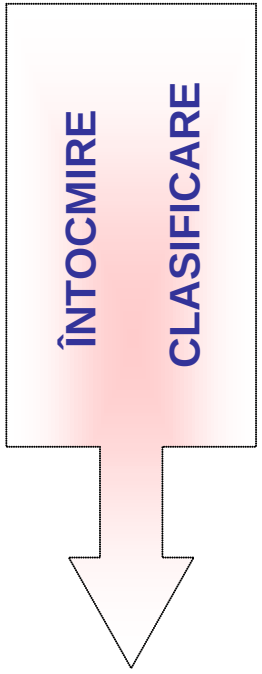
Avându-se în vedere daunele pe care pregătirea deficitară a personalului le poate provoca securității naționale prin compromiterea informațiilor secrete de stat, *Standardele naționale* stabilesc sancțiuni pentru faptele de natură contravențională privind neîndeplinirea obligațiilor și nerespectarea normelor în domeniul pregătirii personalului care accesează informații secrete de stat.

C A P I T O L U L IV

REGULILE GENERALE PRIVIND EVIDENȚA, ÎNTOCMIREA, PĂSTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA ŞI DISTRUGEREA INFORMAȚIILOR CLASIFICATE

Activitățile de ***evidență, întocmire, păstrare, procesare, manipulare şi multiplicare*** a documentelor clasificate, se realizează în cadrul ***compartimentelor speciale***, subordonate conducătorului unității ce gestionează de astfel de informații.

Corespunzător prevederilor Capitolului III din *Standardele naționale de protecție a informațiilor clasificate,* aprobate prin HG nr. 585/2002, ***diagrama de proces*** aferentă activităților circumscrise gestionării documentelor clasificate este următoarea:

DATE DE INTRARE	DIAGRAMA DE FLUX	DATE DE IEŞIRE
Încadrarea informației create intern, în clase şi niveluri de secretizare		**INFORMAȚII ÎNCADRATE ÎN CLASE ŞI NIVELURI DE SECRETIZARE** ▪ Informațiile ***se clasifică*** secrete de stat sau secrete de serviciu în raport cu importanţa pe care o au pentru securitatea naţională şi consecinţele pe care le-ar putea produce dezvăluirea sau diseminarea lor neautorizată. Includerea informațiilor în clase şi niveluri de secretizare se realizează prin consultarea ghidului de încadrare corectă şi uniformă a informațiilor în clase şi niveluri de secretizare, a listelor cu informații secrete de stat sau a listelor cu informații secrete de serviciu. Emitenţii informațiilor secrete de stat au obligaţia de a evalua periodic necesitatea menţinerii lor în nivelurile de secretizare şi de a prezenta propuneri în consecinţă împuterniciţilor şi funcţionarilor superiori abilitați prin lege să atribuie niveluri de secretizare. ▪ Informațiile *secrete de stat* se ***declasifică*** prin hotărâre a Guvernului, la solicitarea motivată a emitentului, în situațiile în care termenul de clasificare stabilit a expirat sau dezvăluirea informațiilor nu mai poate prejudicia siguranţa naţională, apărarea ţării, ordinea publică ori interesele deţinătorilor sau atunci când clasa şi nivelul de secretizare au fost atribuite de o persoană neîmputernicită prin lege. Informațiile *secrete de serviciu* se declasifică prin scoaterea lor de pe listele stabilite şi aprobate de către unităţile emitente.

2)***Înregistrarea*** documentelor:

- *elaborate intern* şi *clasificate*
- *primite de la emitenţi externi*

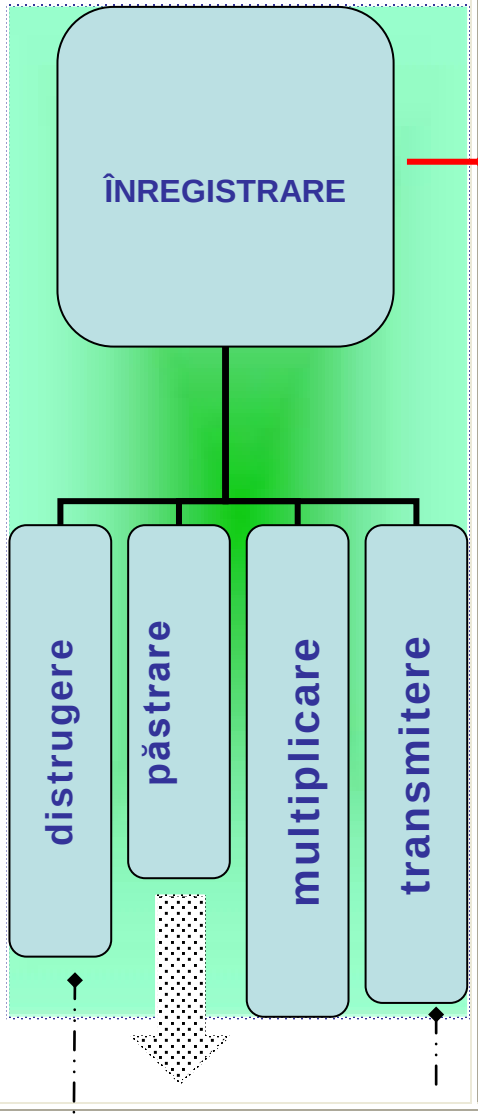
3) Pentru ***documentele înregistrate*** se poate avea în vedere:

a. păstrare

b. *multiplicare* în vederea păstrării / transmiterii

c. transmitere

d. distrugere



◆ **DOCUMENTE LUATE ÎN EVIDENŢĂ**

Înregistrarea documentelor clasificate în registrele de evidenţă se face succesiv, pe parcursul unui an calendaristic; numărul alocat se înscrie pe exemplarele materialelor care conţin informaţii clasificate şi pe anexe.

◆ **DOCUMENTE DESTINATE VALORIFICĂRII ÎN ACTIVITATEA SPECIFICĂ**

◆ **DOCUMENTE MULTIPLICATE**

Multiplicarea informaţiilor clasificate se realizează exclusiv de către persoane autorizate, în baza aprobării conducătorului unităţii deţinătoare, cu avizul structurii / funcţionarului de securitate.

Evidenţierea operaţiunii de multiplicare se face prin marcare pe original (în partea dreaptă jos a ultimei pagini), şi pe copiile rezultate (sub numărul de înregistrare al documentului).

◆ **DOCUMENTE DESTINATE TRANSMITERII**

Transmiterea informaţiilor clasificate se realizează cu aprobarea emitentului şi cu respectarea principiului *"necesităţii de a cunoaşte"*.

Către destinatar extern: numai dacă reprezentantul destinatarului este autorizat corespunzător pentru accesul la informaţii clasificate

◆ **DOCUMENTE DESTINATE DISTRUGERII**

Distrugerea documentelor clasificate se realizează de emitenţi, în funcţie de clasa / nivelul de secretizare.

Documentele, ciornele sau materialele acumulate ori create în procesul de elaborare a informaţiei clasificate se distrug pe bază de proces-verbal. În situaţia în care se păstrează, acestea vor fi datate, marcate cu clasa sau nivelul de secretizare cel mai înalt al informaţiilor conţinute, arhivate şi protejate corespunzător clasei sau nivelului de secretizare al documentului final.

Distrugerea se menţionează în registrul de evidenţă, prin consemnarea numărului de înregistrare al procesului-verbal de distrugere.

4) ***Pregătirea arhivării*** documentelor	ARHIVARE	**DOCUMENTE ARHIVATE** În conformitate cu prevederile *Legii nr. 16 / 1996 a Arhivelor Naționale*	***Inventarierea anuală a documentelor***
5) ***Operațiuni de descărcare a evidenței*** pentru documentele: ▪ transmise ▪ distruse ▪ destinate arhivării	OPERAȚIUNI DESCĂRCARE EVIDENȚĂ	**DOCUMENTE DE EVIDENȚĂ** (registre de evidență pe clase și niveluri de securitate, registre de listare, condici etc.)	
6) ***Pregătirea transportului*** documentelor	TRANSPORT	**CORESPONDENȚĂ CLASIFICATĂ** ***Transportul***, ***pe teritoriul României***, a documentelor și materialele ce conțin informații clasificate se realizează de unitatea specializată a Serviciului Român de Informații, potrivit normelor stabilite prin *HG nr. 1349/2003*. Conducătorii unităților deținătoare de informații clasificate au obligația să desemneze cel puțin un delegat împuternicit pentru transportul și executarea operațiunilor de predare-primire a corespondenței clasificate, între acestea și unitatea specializată a Serviciului Român de Informații. ***Transportul în străinătate*** al documentelor și materialelor care conțin informații clasificate se realizează prin valiza diplomatică, de către curieri diplomatici selecționați și pregătiți de Serviciul de Informații Externe.	

C A P I T O L U L V

PROTECȚIA FIZICĂ

Măsurile de protecție fizică - gratii la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru supraveghere, control, acces, patrule de securitate, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării - se dimensionează în raport cu:

- nivelul de secretizare a informațiilor, volumul și localizarea acestora,
- tipul containerelor în care sunt depozitate informațiile;
- caracteristicile clădirii și zonei de amplasare.

Spațiile unde sunt manipulate sau stocate informațiilor clasificate se organizează și administrează ca ***zone de securitate*** *(**clasa I** și **clasa a II - a**)* constituite în perimetre clar delimitate și protejate, în care accesul este controlat prin sisteme de recunoaștere individuală.

În *zonele de securitate clasa I* se gestionează informații secrete de stat, nivel *"strict secret de importanță deosebită"* și *"strict secret"*, iar în *zonele de securitate clasa II - a*, informații secrete de stat, nivel *"secret"*. În jurul zonelor de securitate poate fi stabilită o *zonă administrativă*, cu perimetru vizibil delimitat, în interiorul căreia să existe posibilitatea de control al personalului și al vehiculelor.

Unitățile deținătoare de informații secrete de stat stabilesc *reguli cu privire la circulația și ordinea interioară în zonele de securitate* și un *sistem propriu de control al vizitatorilor*, astfel încât accesul să fie permis exclusiv posesorilor de certificate de securitate și autorizații de acces, cu respectarea principiului *"necesității de a cunoaște"*.

Informațiile clasificate se păstrează în *containere speciale* (***clasa A***-pentru păstrarea informațiilor *"strict secrete de importanță deosebită"* și ***clasa B*** - pentru păstrarea informațiilor *"strict secrete"* și *"secrete"*), ale căror cerințe de securitate și standarde constructive sunt stabilite de ORNISS.

Cheile containerelor și încăperilor de securitate nu se scot din zonele de securitate în care se află documentele clasificate, iar combinațiile încuietorilor containerelor de securitate sunt cunoscute numai de persoanele abilitate. Pentru cazuri de urgență, un rând de chei suplimentare (o evidență scrisă a fiecărei combinații) se păstrează în plicuri mate sigilate, într-un compartiment stabilit de conducerea instituției, sub control corespunzător. Evidența fiecărei combinații se păstrează în plic separat. Cheilor și plicurilor trebuie să li se asigure același nivel de protecție ca și informațiilor clasificate la care permit accesul.

Copiatoarele și dispozitivele telefax se instalează în încăperi special destinate și se folosesc numai de către persoanele autorizate, potrivit nivelului de secretizare al informațiilor la care au acces.

Echipamentele de comunicații și dotările din birouri, în principal cele electrice și electronice, se verifică de specialiști ai autorităților desemnate de securitate competente, înainte de a fi folosite în zonele în care se lucrează ori se discută despre informații clasificate *strict secret* sau *strict secret de importanță deosebită*, pentru a preveni transmiterea sau interceptarea, în afara cadrului legal, a oricăror informații inteligibile.

Pentru zonele menționate se organizează o evidență a tipului și numerelor de inventar ale echipamentului și a mobilierului mutat în/din interiorul încăperilor.

C A P I T O L U L VI

SECURITATEA INDUSTRIALĂ

În domeniul securității industriale, Serviciul Român de Informații are ca atribuții principale verificarea și avizarea persoanelor juridice care participă la negocierea sau derularea de contracte clasificate secret de stat, precum și avizarea Programelor de prevenire a scurgerii de informații clasificate întocmite de autorități și instituții publice, agenți economici cu capital integral sau parțial de stat și celelalte persoane juridice de drept public sau privat. Importanța acestor activități este deosebită, deoarece marea majoritate a contractelor încheiate până în prezent sunt realizate cu autoritățile și instituțiile din domeniul apărării și siguranței naționale.

Activitățile circumscrise asigurării protecției informațiilor clasificate în domeniul industrial se desfășoară pe două coordonate principale:

1. Acordarea avizului necesar eliberării autorizației sau certificatului de securitate industrială

Toate persoanele juridice de drept public sau privat care desfășoară ori solicită să deruleze activități contractuale ce presupun accesul la informații clasificate secret de stat trebuie să se conformeze prevederilor capitolului VII - Securitate industrială din Standardele aprobate prin HG nr. 585/2002.

Persoanele juridice care intenționează să participe la negocierea unui contract clasificat trebuie să dețină autorizație de securitate industrială eliberată de Oficiul Registrului Național al Informațiilor Secrete de Stat, în baza avizului de securitate acordat de Serviciul Român de Informații. După adjudecarea contractului clasificat, contractantul este obligat să solicite la Oficiul Registrului Național al Informațiilor Secrete de Stat eliberarea certificatului de securitate industrială.

Pentru eliberarea autorizației de securitate industrială necesară participării la procedura de atribuire/negocierea contractelor clasificate și a certificatului de securitate industrială pentru derularea unui contract în care se gestionează informații clasificate secret de stat, societatea comercială se va adresa, în scris, Oficiului Registrului Național al Informațiilor Secrete de Stat, căruia, conform procedurii, îi va trimite chestionarul de securitate(având toate rubricile completate), în plic sigilat. Adresa trebuie însoțită de un document care să ateste participarea la negocierea sau derularea contractului clasificat, iar în cazul derulării unui contract clasificat, va fi prezentată și anexa de securitate. ORNISS va trimite la SRI o adresă, însoțită de plicul sigilat și, anexa de securitate, prin care va solicita declanșarea procedurii de verificare a societății comerciale.

Inițierea verificărilor privind eliberarea autorizației / certificatului de securitate industrială în vederea negocierii / derulării contractelor clasificate se realizează de Oficiului pentru Supravegherea Secretelor de Stat. Solicitarea ORNISS va însoți plicul închis care conține chestionarele de securitate stabilite potrivit Anexelor 25, 26 și 27 la Standarde.

Termenele de verificare, în funcție de nivelul de secretizare al informațiilor clasificate la care se solicită acces, sunt cele prevăzute Standardele aprobate prin în HG nr. 585/2002, respectiv:

- 60 de zile lucrătoare pentru verificarea de nivel I – autorizație de securitate;
- 90 de zile lucrătoare pentru verificarea de nivel II – certificat de securitate de nivel *secret*;
- 120 de zile lucrătoare pentru verificarea de nivel III – certificat de securitate de nivel *strict secret*;
- 180 de zile lucrătoare pentru verificarea de nivel IV – certificat de securitate de nivel *strict secret de importanță deosebită*.

Potrivit art. 225 din *Standarde*, în cadrul verificării de securitate se derulează următoarele activități:

Pentru verificările de securitate de nivel I:

- verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială;
- verificarea modului de aplicare a prevederilor programului de prevenire a scurgerii de informații clasificate;
- evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director și structura de securitate - ori executivă implicată în negocierea contractului clasificat;
- verificarea datelor minime referitoare la bonitatea și stabilitatea economică a obiectivului industrial - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare.

Pentru verificarea de securitate de nivel II:

- verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială;
- evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori,

persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat;

- verificarea unor date minime referitoare la bonitatea şi stabilitatea economică a obiectivului industrial - domeniu şi obiect de activitate, statut juridic, acționari, garanții bancare;
- verificarea modului de implementare şi de aplicare a normelor şi măsurilor de securitate fizică, de securitate a personalului şi a documentelor, prevăzute pentru nivelul secret.

Pentru verificarea de securitate de nivel III:

- verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială;
- evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat, precum şi a celor desemnate să participe la activitățile de negociere a acestuia;
- verificarea datelor referitoare la bonitatea şi stabilitatea economică a agentului economic - domeniu şi obiect de activitate, statut juridic, acționari, garanții bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
- verificarea existenței autorizării sistemului informatic şi de comunicații propriu, pentru nivelul strict secret;
- verificarea modului de implementare şi de aplicare a normelor şi măsurilor de securitate fizică, de securitate a personalului şi a documentelor, prevăzute pentru nivelul strict secret;

- discuţii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajaţii, în vederea clarificării datelor rezultate din chestionar, după caz.

Pentru verificarea de securitate de nivel IV:

- verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială;
- evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat;
- verificarea informaţiilor detaliate referitoare la bonitatea şi stabilitatea economică a agentului economic - domeniu şi obiect de activitate, statut juridic, acţionari, garanţii bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
- verificarea existenţei autorizării sistemului informatic şi de comunicaţii propriu, pentru nivel strict secret de importanţă deosebită;
- verificarea modului de implementare şi de aplicare a normelor şi măsurilor de securitate fizică, de securitate a personalului şi a documentelor, prevăzute pentru nivelul strict secret de importanţă deosebită;
- discuţii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajaţii, în vederea clarificării datelor rezultate din chestionar, după caz.

Oportunitatea acordării avizului pentru eliberarea autorizaţiei sau a certificatului de securitate industrială se evaluează pe baza tuturor datelor şi informaţiilor obţinute, în raport cu criteriile de incompatibilitate stipulate de art. 218 din Standardele naţionale de protecţie a informaţiilor clasificate în România aprobate prin HG nr. 585/2002.

În eventualitatea în care constată că societatea comercială nu întrunește condițiile de securitate necesare, Autoritatea Desemnată de Securitate competentă acordă aviz negativ, iar ORNISS nu eliberează autorizația/certificatul de securitate industrială și informează despre acest lucru agentul economic solicitant și Serviciul Român de Informații.

Procedura de verificare de securitate, pentru eliberarea unei noi autorizații de securitate industrială sau a unui nou certificat de securitate industrială se realizează pe baza unor noi chestionare de securitate industrială cu respectarea prevederilor legale.

Retragerea autorizației sau a certificatului de securitate industrială se realizează conform prevederilor art. 235 din *Standardele naționale de protecție a informațiilor clasificate în România* aprobate prin HG nr. 585/2002:

a) la solicitarea obiectivului industrial;

b) la propunerea motivată a autorității desemnate de securitate competente;

c) la expirarea termenului de valabilitate;

d) la încetarea contractului;

e) la schimbarea nivelului de certificarea acordat inițial.

Aspecte rezultate din practica acordării avizelor de securitate industrială

Cu toate că se constată o creștere a interesului pentru autorizarea negocierii/derulării contractelor clasificate ce presupun accesarea de informații secrete de stat, au fost înregistrate situații în care unele societăți comerciale au solicitat eliberarea *autorizațiilor de securitate industrială ulterior participării la licitațiile organizate de instituțiile de stat sau, mai mult, după adjudecarea ori chiar derularea contractului clasificat secret de stat*.

Astfel, pot să apară premisele accesării/diseminării neautorizate a informațiilor secrete de stat ce fac obiectul activităților contractuale datorită faptului că, în cele mai multe situații (*ex.: solicitanții nu aveau personal autorizat pentru accesul la informații clasificate și programul de prevenire a scurgerii de informații clasificate avizat de instituția noastră, sau au transmis chestionare de securitate industrială incomplete sau pentru alt nivel de secretizare decât cel specificat în adresa ORNISS și, mai ales trebuie precizat că funcționarii de securitate nu cunosc prevederile legale aferente obținerii avizului de securitate industrială)*.

În ceea ce privește solicitările privind obținerea certificatelor de securitate *industrială* necesare derulării contractelor clasificate secrete de stat, s-au înregistrat situații în care societățile comerciale nu respectă prevederile stipulate de standarde în vigoare *(ex.: firme care nu dispun de pregătirea și logistica necesară; contractantul cedează unui subcontractant realizarea unei părți a contractului clasificat, fără să înștiințeze contractorul și să se asigure că subcontractantul deține certificat de securitate industrială; anexele de securitate nu prevăd clauze și proceduri de protecție a informațiilor clasificate ce vor fi diseminate pe perioada derulării contractului secret de stat potrivit reglementărilor legale în materie*).

Cu foarte puține excepții, *măsurile INFOSEC* aferente sistemelor informatice și de comunicații pe care sunt vehiculate datele secret de stat, nivel *strict secret* nu asigură integritatea informațiilor clasificate ce fac obiectul contractelor clasificate. *De regulă, activitățile de instalare și întreținere a echipamentelor informatice și de comunicații, precum și instruirea utilizatorilor acestora sunt realizate de firme private sau de persoane fizice neautorizate iar, în foarte multe situații, mediile de stocare a informațiilor clasificate în format electronic sunt gestionate cu nerespectarea reglementărilor în vigoare.*

Vulnerabilitățile pe această componentă se datorează cu precădere necunoașterii de către societățile comerciale solicitante de certificate de securitate industrială, *nivel strict secret* a obligativității deținerii *acreditării INFOSEC* și lipsei de expertiză a persoanelor cu atribuții specifice în cadrul structurilor de securitate proprii, privind implementarea/ operaționalizarea reglementărilor specifice elaborate de ORNISS.

În contextul evaluării bonității și stabilității economice a societăților comerciale care solicită eliberarea autorizației / certificatului de securitate industrială au existat situații în care agenții economici *nu au transmis instituției noastre documente fiscale solicitate întrucât figurau cu datorii mari la bugetul de stat* - aspect ce a fundamentat acordarea avizului negativ(art. 218 (1) lit. b).

2. Avizarea Programelor de prevenire a scurgerii de informații clasificate

Pentru asigurarea măsurilor protective și prevenirea situațiilor de natură a crea condițiile accesării, diseminării, multiplicării și distrugerii neautorizate a informațiilor clasificate emise sau gestionate de autoritățile și instituțiile publice, structurile de securitate constituite la nivelul acestora au obligația să elaboreze și să prezinte spre aprobare, conducătorilor acestora, norme interne de lucru și de ordine interioară, destinate implementării măsurilor de protecție a acestor informații.

Programul de prevenire a scurgerii de informații clasificate constituie componenta de bază destinată implementării complexului de măsuri privind protecția fizică și procedurală a informațiilor clasificate.

Conform prevederilor art. 86 alin. (1) lit. h) din Standarde, conducătorii unităților deținătoare de informații clasificate au obligația de a supune avizării instituțiilor abilitate Programul propriu de prevenire a scurgerii de informații clasificate și să asigure aplicarea acestuia.

Până la momentul elaborării Programului de prevenire a scurgerii de informații clasificate, conducătorii unităților gestionare de informații clasificate trebuie să asigure realizarea următoarelor categorii de activități:

- Să numească, prin ordin intern, persoanele care vor face parte din structura de securitate și să stabilească atribuțiile acestora, în paralel cu constituirea și operaționalizarea compartimentelor speciale pentru gestionarea informațiilor clasificate, în condițiile legii.
- Să stabilească categoriile de informații clasificate gestionate, în vederea inițierii de măsuri pentru constituirea listei cu informații clasificate secrete de stat, pe niveluri de secretizare, în vederea aprobării acesteia prin hotărâre de guvern. Înainte de a supune aprobării hotărârea de guvern respectivă, lista cu informații clasificate va fi transmisă, spre avizare, autorității desemnate de securitate competente. În cazul în care unitatea deținătoare de informații clasificate este în subordinea, sub autoritatea sau în coordonarea unei instituții tutelare, constituirea listei proprii cu informațiile clasificate se va realiza prin raportarea la hotărârea de guvern care se stabilesc categoriile de informații clasificate, corespunzătoare domeniului respectiv de activitate.
- Să stabilească obiectivele, sectoarele și locurile din zona de competență care prezintă importanță deosebită pentru protecția informațiilor secrete de stat și să le comunice Serviciului Român de Informații, pentru a fi

supuse spre aprobare Guvernului. În acest sens, unitățile deținătoare de informații clasificate pot solicita asistență de specialitate Serviciului Român de Informații. În funcție de locurile unde sunt gestionate informații clasificate se stabilesc zonele de securitate clasa I și, respectiv, a II-a, precum și zonele administrative.

- Să aprobe lista funcțiilor ce implică acces la informații clasificate, pe niveluri de secretizare, respectându-se principiul nevoii de a cunoaște.
- Să aprobe listele cu personalul care are sau urmează să aibă acces la informații clasificate și să le comunice la Oficiul Registrului Național al Informațiilor Secrete de Stat și la instituțiile abilitate să coordoneze activitatea și controlul măsurilor privitoare la protecția informațiilor clasificate, potrivit legii. Este obligatoriu ca numărul persoanelor autorizate să acceseze informații clasificate să nu depășească numărul funcțiilor care implică accesul la astfel de informații.

Programul se întocmește de către structura de securitate, potrivit prevederilor Anexei nr. 10 la *"Standardele naționale de protecție a informațiilor clasificate în România"* aprobate prin HG nr. 585/2002, raportate la condițiile generale și specifice ale instituției. Acesta va respecta pe formă prevederile Anexei nr. 10 din *Standardele naționale de protecție a informațiilor clasificate din România*, aprobate prin HG nr. 585/2002, astfel:

- să fie transmis spre avizare în două exemplare;
- clasificarea să fie înscrisă în funcție de nivelul maxim de clasificare a informațiilor pe care acesta le cuprinde;
- paginile să fie marcate și numerotate corect (numărul curent, urmat de numărul total al acestora).

Documentul trebuie să fie structurat pe nouă capitole și să cuprindă elemente referitoare la:

- informații clasificate deținute de unitatea în cauză și baza legală a deținerii lor;
- locurile în care se concentrează informații clasificate;
- componența structurii de securitate;
- lista funcțiilor și lista persoanelor care urmează să aibă acces la informații clasificate;
- măsurile pentru protecția fizică a clădirilor, spațiilor și locurilor unde se lucrează cu informații clasificate;
- modalități de protecție a activităților și a informațiilor clasificate, în funcție de suportul acestora (electronic, audio, video, hârtie etc.);
- măsurile de protecție împotriva observării și ascultării;
- activitățile de control, analiză și evaluare a modului în care se respectă prevederile legale, procedurile de raportare, investigare și evidență a incidentelor de securitate;
- modul de instruire protectivă a persoanelor care au acces la informații clasificate.

Autoritățile și instituțiile publice centrale, precum și agenții economici și societățile comerciale de interes public sau privat, cu sediul în municipiul București sau în județul Ilfov, vor transmite SRI Programul de prevenire a scurgerii de informații clasificate. Unitățile teritoriale din subordinea, coordonarea sau sub autoritatea instituțiilor centrale vor întocmi Programe proprii de prevenire a scurgerii de informații clasificate și le vor trimite spre avizare structurilor teritoriale competente ale Serviciului.

Se verifică conformitatea Programului cu prevederile Anexei nr. 10 la *Standardele* aprobate prin HG nr. 585/2002, urmărindu-se respectarea elementelor de formă și conținut, în raport cu realitățile din teren, capitol cu capitol, astfel:

Capitolul I

Consemnarea bazei legale (Legea nr. 182/2002 privind *protecția informațiilor clasificate*; HG nr. 585/2002 pentru aprobarea *Standardelor naționale de protecție a informațiilor clasificate în România*; HG nr. 781/2002 privind *informațiile secrete de serviciu*; HG. nr. 1349/27.11.2002 privind *colectarea, transportul, distribuirea și protecția, pe teritoriul României, a corespondenței clasificate*). În cadrul capitolului se consemnează baza legală a deținerii informațiilor clasificate, precum și deciziile conducătorului instituției privind constituirea structurii de securitate și aprobarea listei funcțiilor ce implică accesul la informații clasificate.

Capitolul II

Se vor prezenta, pe scurt, aspectele legate de obiectul de activitate al instituției. Totodată, vor fi prezentate obiectivele și principiile care stau la baza măsurilor de prevenire a scurgerii de informații clasificate.

Capitolul III

- prezentarea elementelor generale privind informațiile clasificate gestionate;
- lista informațiilor secrete de stat, pe clase și niveluri de secretizare, aprobată prin Hotărâre de Guvern (după caz, extras din această listă, care poate fi anexat la Program);
- prezentarea locurilor unde se gestionează informații secrete de stat (conform Anexei nr. 10/A);

Capitolul IV

- lista funcțiilor care necesită acces la informații clasificate, pe niveluri de secretizare;
- prezentarea persoanelor din cadrul structurii de securitate, a listei cu persoanele care urmează să aibă acces la informații clasificate și a listei cu persoanele

cărora li se acordă acces temporar la informații clasificate;

Capitolul V

- măsurile de protecție fizică a clădirilor, spațiilor / ocurilor unde se păstrează sau se concentrează datele, informațiile si documentele clasificate ori se desfășoară astfel de activități (conform Anexei nr. 10/B);
- măsurile procedurale de protecție a datelor, informațiilor, documentelor și a activităților clasificate;
- planurile în situații de urgență, în care sunt detaliate activitățile ce trebuie desfășurate în astfel de cazuri;

Capitolul VI

- prezentarea sistemului de protecție a surselor generatoare de informații clasificate (se va urmări să corespundă prevederilor Anexei nr. 10/C);
- vor fi prezentate echipamentele de telecomunicații și birotică prin care vor fi transmise/prelucrate informații clasificate;

Capitolul VII

- măsurile de protecție împotriva observării și ascultării (conform Anexei nr. 10/D);
- în funcție de nivelul informațiilor care vor fi accesate se vor lua măsuri împotriva ascultării și observării pasive;

Capitolul VIII

- planificarea și modul de realizare a controalelor, activităților de analiză și evaluare a respectării reglementărilor legale în domeniul protecției informațiilor clasificate și, respectiv, a soluționării cazurilor de încălcare a acestora;

- modul de soluționare a cazurilor de încălcare a reglementărilor privind protecția informațiilor clasificate (Anexa nr. 10/E la Standarde);

Capitolul IX

- măsurile de instruire și educație protectivă a persoanelor desemnate să îndeplinească atribuții pe linia protecției informațiilor clasificate (Anexa nr. 10/F);
- reguli privind accesul cetățenilor străini, cetățenilor români care au și cetățenia altui stat, precum și apatrizilor, la informațiile clasificate și în locurile în care se desfășoară activități, se expun obiecte sau se execută lucrări din această categorie.

Totodată, se verifică dacă la Program este anexat Planul de pază și apărare, întocmit în conformitate cu prevederile art. 120 din *"Standardele naționale de protecție a informațiilor clasificate în România"* aprobate prin HG nr. 585/2002, care trebuie să cuprindă:

- date privind delimitarea și marcarea zonelor de securitate, dispunerea posturilor de pază și măsurile de supraveghere a perimetrului protejat;
- sistemul de control al accesului în zonele de securitate;
- măsurile de avertizare și alarmare pentru situații de urgență;
- planul de evacuare a documentelor și modul de acțiune în caz de urgență;
- procedura de raportare, cercetare și evidență a incidentelor de securitate.

Trebuie precizat faptul că Planul de pază și apărare va fi înregistrat potrivit celui mai înalt nivel de secretizare a informațiilor protejate și va cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

Dacă se constată că modul de elaborare a Programului și a Planului de pază nu respectă prevederile cuprinse în Anexa nr. 10 și, respectiv, în art. 120 din Standarde, se va realiza o discuție cu funcționarul de securitate în vederea clarificării neconformităților de formă și de conținut.

Ulterior, exemplarul nr. 1 al Programului de prevenire a scurgerii de informații clasificate va fi restituit instituției în cauză în vederea reevaluării și completării.

După refacerea acestuia, Programul reevaluat și completat va fi transmis SRI prin Poșta Secretă.

Dacă în urma analizei rezultă că Programul respectă prevederile Anexei nr. 10, se efectuează o evaluare, la sediul instituției solicitante, a pertinenței măsurilor prevăzute în cadrul acestuia.

În urma evaluării, în situația în care rezultă că sunt respectate toate măsurile prevăzute în Program și nu au fost evidențiate neconcordanțe sau situații de natură a crea riscuri sau vulnerabilități în planul protecției informațiilor clasificate, Oficiul pentru Supravegherea Secretelor de Stat sau, după caz secția județeană de informații, va transmite oficial, prin adresă, instituției solicitante, exemplarul nr. 1 al Programului de prevenire a scurgerii de informații clasificate, avizat pozitiv.

În cazul în care sunt semnalate riscuri și vulnerabilități referitoare la protecția informațiilor clasificate ori sunt primite reclamații sau sesizări cu privire la încălcări ale măsurilor instituite prin Programele de prevenire a scurgerii de informații clasificate, Serviciul realizează evaluările necesare și, de la caz la caz, propune revizuirea acestora.

Programul de prevenire a scurgerii de informații clasificate se actualizează anual sau ori de câte ori se impune (când sunt identificate riscuri și vulnerabilități etc.), modificările efectuate aducându-se la cunoștința SRI, prin transmiterea unor documente de completare, în vederea avizării.

Aspecte practice rezultate din activitatea de avizare a programului de prevenire a scurgerii de informații clasificate

Din analiza documentelor primite spre avizare, în unele situații au fost constatate neajunsuri de natură procedurală și aspecte de neconformitate, cum ar fi:

- au fost transmise spre avizare fără adresă de însoțire, întocmite într-un singur exemplar, clasificate greșit, cu pagini sau anexe lipsă, fără a fii marcate și/sau înregistrate;
- baza legală a deținerii documentelor clasificate, fiind menționat numai la cadrul normativ care reglementează protecția informațiilor clasificate;
- omiterea includerii în programul de prevenire a elementelor privind accesul la informații secret de serviciu (*Liste categorii informații, funcții și persoane* întocmirea incompletă a *listelor de funcții care necesită acces la informații clasificate* (în care sunt prezentate numai funcțiile propriu-zise fără a se preciza și numărul de posturi aferente fiecărei funcții) și *listelor de persoane care au sau urmează să aibă acces la informații clasificate* (omiterea unor date de identificare);
- neconcordanță între listele cu funcții și persoane, fiind prezentat un număr mai mare de persoane pentru accesul la informații clasificate decât funcțiile care necesită acces la astfel de informații;
- măsurile de protecție fizică fie erau prezentate lapidar (fiind omise prevederile referitoare la *controlul cheilor și combinațiilor încăperilor și zonelor de securitate* și *planurile de urgență*) fie erau supra/subdimensionate în conformitate cu nivelul maxim de clasificare și volumul informațiilor gestionate;

- nu era prezentat sistemul informatic folosit pentru elaborarea documentelor clasificate sau chiar se făceau precizări cum că instituția nu deține un sistem informatic dedicat pentru astfel de activități;
- diferențe majore între măsurile de protecție fizică stipulate în program și cele existente la sediul solicitantului, în sensul că acestea nu erau implementate în totalitate;
- referitor la modalitatea în care se realizează controlul cheilor s-a constatat că în cel puțin 50% din cazuri condica de predare-primire a cheilor nu era instituită sau nu era completată la zi;
- lipsa marcajului zonelor de securitate sau a însemnelor ce din care să rezulte interzicerea accesului personalului ce nu este autorizat pentru accesul la informații clasificate;
- nu erau aprobate norme proprii în aplicarea H.G. nr. 585/2002;
- stații de lucru conectate la intranet sau la internet, (deși funcționarul de securitate prezenta sistemele informatice ca fiind neconectate la aceste rețele) sau neasigurate corespunzător (accesul nu se efectua prin alocarea unor conturi individuale protejate prin parole sau coduri);
- lipsa documentelor de planificare aprobate de conducerea organizației pentru efectuarea controalelor interne și pregătirii personalului pe componenta protecției informațiilor clasificate;
- necompletarea fișelor de pregătire a personalului cu atribuții pe linia protecției informațiilor clasificate.

C A P I T O L U L VII

SECURITATEA INFORMAȚIILOR CLASIFICATE ÎN FORMAT ELECTRONIC

Informația în format electronic reprezintă texte, date, imagini, sunete, înregistrate pe dispozitive electronice de stocare sau pe suporturi magnetice, optice, electrice ori transmise sub formă de curenți, tensiuni sau câmp electromagnetic, în eter sau în rețele de comunicații. Informație în format electronic întâlnim în sistemele de calcul, în rețelele de transmisii date, în telefonia fixă sau mobilă, în transmisiile radio, etc. ***Informația clasificată în format electronic*** reprezintă orice informație în format electronic de interes pentru securitatea națională, care, datorită nivelurilor de importanță și consecințelor care s-ar produce ca urmare a dezvăluirii și diseminării neautorizate, trebuie să fie protejată.

Nu se poate vorbi despre *informație clasificată în format electronic* decât în strânsă legătură cu sistemele informatice si de comunicație (SIC) care le procesează, stochează sau transmit între diverse componente prin diverse medii de transmitere (fir, aer, mediu de stocare).

Securitatea informației în format electronic – stare de siguranță în care se află informația – se realizează prin măsuri de protecție asupra sistemelor informatice și de comunicații, a căror implementare duce la înlăturarea riscului de securitate *(probabilitatea ca o amenințare la adresa securității unui sistem*

informatic și de comunicații să exploateze o vulnerabilitate a acestuia, efectul fiind compromiterea obiectivelor de securitate, respectiv: confidențialitatea, integritatea, disponibilitatea, autenticitatea și nerepudierea informațiilor clasificate vehiculate prin acel sistem informatic).

Potrivit Standardelor naționale de protecție a informațiilor clasificate în România – securitatea informațiilor clasificate în format electronic acoperă securitatea calculatoarelor, a mediilor de stocare, a comunicațiilor, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele informatice.

Există legislație în domeniu, începând cu Legea nr.182, Standardele de protecție a informațiilor clasificate, Ordinele Directorului ORNISS în care sunt prezentate în amănunt măsurile de protecție ce trebuie luate pentru protecția informației clasificate în format electronic. Sunt măsuri și proceduri care trebuie urmate începând de la achiziție, operaționalizare, acreditare și scoatere din uz a sistemelor informatice.

Totuși, până a ajunge la implementarea în detaliu a tuturor acestor măsuri și proceduri de securitate sunt necesare și posibile demersuri care ne stau la îndemână și a căror implementare duce la scăderea considerabilă a riscului de securitate. O parte din acestea sunt cele valabile și la gestionarea în condiții de securitate a documentelor pe suport de hîrtie, sau sunt facilități ale sistemelor informatice oferite de fabricant (hard sau soft) sau se referă la protecția personalului.

Standardele naționale de protecție a informațiilor clasificate operează cu următoarele componente INFOSEC:

- Securitatea personalului;
- Securitatea fizică;
- Controlul accesului la SIC;

- Securitatea informațiilor clasificate în format electronic;
- Controlul și evidența informațiilor în format electronic;
- Manipularea și controlul mediilor de stocare a informațiilor clasificate în format electronic;
- Declasificarea și distrugerea mediilor de stocare a informațiilor în format electronic.

Dintre aceste componente, ne-am propus să supunem atenției componenta de securitate a informației clasificate în format electronic iar în această perspectivă să discutăm despre securitatea calculatoarelor – a sistemelor informatice, securitatea mediilor de stocare și securitatea comunicațiilor.

În continuare vă supun atenției câteva din aceste măsuri de protecție pentru a căror implementare nu este necesară intervenția cuiva din afară ci poate fi făcută de structura de securitate – administratorii bazelor de date și ai rețelelor de calculatoare.

A. Securitatea calculatoarelor

Securitatea calculatoarelor – COMPUSEC - aplicarea la nivelul fiecărui calculator a facilităților de securitate hardware, firmware și software, pentru a preveni divulgarea, manevrarea, modificarea sau ștergerea neautorizată a informațiilor clasificate ori invalidarea neautorizată a unor funcții

Mecanismele de securitate hardware, firmware și software pot contribui individual și în combinație la securitatea calculatoarelor.

Securitatea hardware și firmware utilizează caracteristicile de securitate asigurate de către fabricant prin componentele fizice ale calculatoarelor și se referă la următoarele aspecte:

a) proceduri și documentație de securitate pentru pornirea/oprirea echipamentelor de calcul;

b) instrucțiuni și proceduri de securitate referitoare la conectarea/ deconectarea echipamentelor în/de la rețea;

d) proceduri pentru efectuarea unor verificări regulate ale sigiliilor de pe echipamente și asigurarea că modulele hardware sunt păstrate încuiate, în mod normal, în carcasa echipamentului;

e) configurația calculatorului trebuie să îi asigure acestuia posibilitatea de a putea funcționa în condiții variate (de exemplu trebuie precizat ce terminale / stații de lucru sau periferice pot fi conectate sau deconectate într-o situație specifică de exploatare);

f) proceduri de securizare a configurației calculatorului pregătit pentru întreținere și reparare;

g) proceduri care trebuie urmate în caz de cedare hardware, cu descrierea acțiunilor care trebuie întreprinse și de către cine, în vederea securizării calculatorului la deconectare și ce date trebuie păstrate referitoare la astfel de incidente hardware;

h) proceduri pentru reconectarea terminalelor / stațiilor de lucru de la distanță care au fost deconectate din motive de securitate.

Securitatea software are în vedere utilizarea și controlul oricăror facilități de protecție furnizate prin software: sistem de operare, programe utilitare, programe de aplicație:

a) metode de identificare a utilizatorilor, proceduri de stabilire a conturilor utilizatorilor, a grupurilor de utilizatori și de alocare a identificatorilor utilizatorilor, proceduri de ștergere a conturilor utilizatorilor în cazul plecării personalului de la post sau atunci când a fost detectată o compromitere a contului respectiv;

b) metode de autentificare, inclusiv protecția informațiilor de autentificare (de exemplu, parole de acces), proceduri de control și schimbare a mecanismelor de autentificare;

c) mecanisme de control al accesului și proceduri de implementare a controlului accesului utilizatorilor pentru utilizarea serviciilor și resurselor sistemelor informatice;

d) evidența software-lui, a versiunilor sistemelor de operare și a programelor utilitare, inclusiv cele care vor fi folosite în situații deosebite;

e) controlul asupra facilităților de copiere sau de modificare a: datelor, sistemului de operare, programelor utilitare și a programelor de aplicație;

f) măsuri de precauție ce trebuie luate înainte și după procesare sau în timpul pregătirii diferitelor tipuri de activități clasificate, incluzând rutine de ștergere a memoriei principale, reguli de declasificare sau de suprascriere a versiunilor anterioare și proceduri care să asigure că bufferele sunt curățate și că toate datele din fișierele jurnalelor de audit și de evidență a deschiderii sesiunilor de lucru ale utilizatorilor sistemului au fost listate și suprascrise.

B. Securitatea mediilor de stocare a informațiilor

Într-un sistem informatic și de comunicații, volumul și densitatea informațiilor stocate sau procesate, accesibilitatea lor, ușurința și viteza de copiere a informațiilor, uneori și de la stații aflate la distanță, subliniază nevoia luării unor măsuri de securitate a informațiilor – a mediilor de stocare a acestora. Aceste măsuri vizează următoarele aspecte:

a) proceduri corespunzătoare pentru clasificarea mediilor de stocare;

b) responsabilități și proceduri pentru înregistrarea, controlul și evidența mediilor de stocare;

Toate mediile de stocare secrete de stat se identifică și se controlează în mod corespunzător nivelului de secretizare. Pentru informațiile neclasificate sau secrete de serviciu se aplică regulamente de securitate interne.

Identificarea evidența și controlul mediilor de stocare trebuie să respecte următoarele cerințe:

- mijloc de identificare – numărul, seria și marcajul nivelului de clasificare - pentru fiecare astfel de mediu, în mod separat;
- proceduri bine definite pentru emiterea, primirea, retragerea, distrugerea sau păstrarea mediilor de stocare;
- să existe evidențe manuale sau tipărite la imprimantă, indicând conținutul și nivelul de secretizare a informațiilor înregistrate pe mediile de stocare.

Pentru nivelul strict secret și strict secret de importanță deosebită, informațiile detaliate asupra mediului de stocare, incluzând conținutul și nivelul de clasificare, se țin într-un registru adecvat.

c) proceduri pentru achiziția, păstrarea, evidența și controlul mediilor de stocare pentru calculatoare;

d) proceduri pentru primirea, schimbul și diseminarea documentelor electronice, inclusiv proceduri de verificare privind existența virușilor de calculatoare și a software-ului nociv, aplicate tuturor mediilor de stocare care provin din afara sistemului informatic;

e) responsabilități și proceduri pentru declasificarea /distrugerea *documentelor electronice* și a mediilor de stocare.

Când un mediu de stocare urmează să iasă din uz, trebuie să fie declasificat suprimându-se orice marcaje de clasificare, ulterior putând fi utilizat ca mediu de stocare nesecret.

Informațiile clasificate înregistrate pe medii de stocare refolosibile se șterg doar în conformitate cu procedurile operaționale de securitate.

Dacă mediul de stocare nu poate fi declasificat, atunci trebuie distrus printr-o procedură aprobată.

Sunt interzise declasificarea și refolosirea mediilor de stocare care conțin informații strict secrete de importanță deosebită, acestea putând fi numai distruse, în conformitate cu procedurile operaționale de securitate.

Informațiile clasificate în format electronic stocate pe un mediu de unică folosință - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operaționale de securitate.

C. Securitatea comunicațiilor

Securitatea comunicațiilor – aplicarea măsurilor de securitate în telecomunicații, cu scopul de a proteja mesajele dintr-un sistem de telecomunicații, care ar putea fi interceptate, studiate, analizate și, prin reconstituire, pot conduce la dezvăluiri de informații clasificate.

Securitatea comunicațiilor reprezintă un ansamblu de proceduri, incluzând :

- măsuri de securitate a transmisiilor;
- măsuri de securitate împotriva radiațiilor - TEMPEST;
- măsuri de securitate criptografică.

Securitatea transmisiilor. Toate mijloacele folosite pentru transmiterea informațiilor clasificate prin emisii radio se supun instrucțiunilor de securitate a comunicațiilor emise de către instituția desemnată la nivel național pentru protecția informațiilor clasificate.

Mecanismele de securitate a transmisiilor concură la asigurarea disponibilității și confidențialității informațiilor. Totodată, ca o consecință a îmbunătățirii disponibilității, prin intermediul mecanismelor utilizate pentru a contracara încercările de a bruia sau de a intercepta transmisia propriu-zisă, integritatea datelor este asigurată.

Sunt necesare măsuri pentru contracararea unor amenințări cum ar fi:

- interceptarea neautorizată;
- bruiajul;
- interferențele;
- inducerea în eroare;
- analiza traficului.

Concret pentru un sistem informatic aceste probleme apar la rețelele wireless atunci când schimbul de date între server și celelalte componente ale rețelei se face prin echipamente radio nu prin fire.

Securitatea emisiilor are în vedere ansamblul măsurilor de testare și de realizare a securității împotriva scurgerii de informații, prin intermediul emisiilor electromagnetice parazite - TEMPEST.

Sistemele informatice care stochează, procesează sau transmit informații secrete de stat, vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromițătoare.

Emisiile parazite apar în jurul echipamentelor informatice dar și a cablurilor prin care circulă informația. La o distanță suficientă (de ordinul metrilor) de aceste cabluri și în funcție și de intensitatea curentului electric care circulă prin cabluri, cu aparatură specială aceste câmpuri electromagnetice pot fi captate iar informația poate fi refăcută. Această situație este valabilă pentru rețelele de cabluri care nu sunt suficient protejate, fac legătura între corpuri de cladiri, etc.

Considerând cazul monitoarelor calculatoarelor trebuie avut în vedere faptul că ele fac parte din categoria perifericelor proiectate și destinate realizării unui scop precis: aducerea informației din sistemul de calcul la o formă convenabilă utilizatorului uman, respectiv percepției optice. În acest caz, cantitatea totală de lumină a ecranului este dată de media ponderată a luminiscenței ultimilor câteva mii de pixeli iluminați de fascicolul de electroni. Așa că, un observator care poate capta, cu ajutorul unui telescop, de exemplu, lumina difuză, reflectată de pereți, mobilă sau alte asemenea obiecte aflate în apropierea ecranului și poate transforma fluxul luminos în semnal electric, poate obține, după aplicarea unei filtrări corespunzătoare, semnalul video care a produs-o.

Specificațiile standardizate de testare a protecției Tempest în cazul emisiei energetice de natură electromagnetică, sunt acelea ale limitei spațiului controlat. Acesta se definește ca distanța față de sursă la care atacatorul poate avea acces și unde raportul semnal/zgomot trebuie să fie de valoare suficient de mică pentru a împiedica separarea radiației compromițătoare de zgomotul de fond și decodificarea acesteia.

Instalarea inițială a sistemului informatic și de comunicații sau orice modificare majoră adusă acestuia vor fi executate de persoane autorizate, în condițiile de securitate prezentate în standarde. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are acces la informații de cel mai înalt nivel de clasificare pe care respectivul sistem informatic le va stoca, procesa sau transmite.

Securitatea criptografică. Sistemul ori subsistemul informatic destinat preluării, prelucrării, stocării și transmisiei de date și informații secrete de stat trebuie să fie prevăzut cu sistem de secretizare prin metode, mijloace și echipamente pentru asigurarea integrității, confidențialității și disponibilității acestora.

Modul în care este prezentată informația în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanță, nu trebuie să influențeze nivelul de clasificare acordat informațiilor respective.

D. Securitatea fizică

Măsurile de securitate fizică sunt necesare pentru a asigura prevenirea accesului neautorizat la informații clasificate, efectuării de operațiuni neautorizate, blocării resurselor și serviciilor calculatoarelor și pentru protejarea echipamentelor de calcul (furturi, distrugeri, etc). Securitatea fizică a sistemelor de calcul și comunicație – ca o componentă INFOSEC – are în vedere mediul în care acestea funcționează (încăperile în care sunt amplasate, alimentarea cu energie alectrică, condițiile de mediu, protecția împotriva incendiilor a inundațiilor, funcționarea în situații de urgență), dar și accesul personalului în zonele în care sunt amplasate.

Orice persoană capabilă să intre într-un loc care conține echipament de calcul poate fi în situația de a interacționa sau de a avaria echipamentul și poate avea acces la informațiile clasificate prelucrate de acesta. Amenințările la adresa securității calculatoarelor pot veni din partea oricărei persoane care are pregătirea profesională și cunoștințe corespunzătoare despre sistemele de calcul și posibilitatea de acces la acestea.

Astfel, în zonele în care sunt amplasate sisteme informatice care procesează informații clasificate, este necesar să se aplice măsuri generale de securitate, cum ar fi:

a) intrarea personalului și a materialelor, precum și plecarea în/din aceste zone să fie controlate prin mijloace bine stabilite;

b) zonele şi locurile în care securitatea sistemelor informatice poate fi afectată, nu trebuie să fie niciodată ocupate de un singur angajat autorizat (regula celor doi);

Persoanelor care solicită acces temporar sau cu intermitenţe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori, fiind însoţiţi permanent, pentru a avea garanţia că nu pot avea acces la informaţii clasificate şi nici la echipamentele utilizate.

Protecţia antivirus – ca o componentă a protecţiei sistemelor informatice, a informaţiei în format electronic, trebuie să conţină proceduri şi mecanisme de protecţie antivirus atât manuale cât şi automate şi include următoarele măsuri de securitate:

a) verificarea sistemelor de operare instalate, a pachetelor software şi a programelor utilitare, privind prezenţa viruşilor sau a altui software nociv, cu proceduri pentru ştergerea acestora în cazul detectării lor;

b) verificarea în permanenţă a fişierelor-datelor stocate în sistemele de calcul – verificare antivirus în timpul procesării, accesării, la introducerea/extragerea datelor în/din sistemele de calcul sau la intervale de timp bine stabilite;

c) verificarea conţinutului mediilor de stocare (informaţii şi software) primite din surse externe, cu proceduri pentru dezinfectarea lor;

d) actualizarea în permanenţă a versiunilor de programe antivirus şi utilizarea mai multor produse antivirus (binenţeles licenţiate) – atât pe server-e cât şi pe staţiile de lucru;

e) raportarea incidentelor cauzate de viruşi, atât către expeditorul mediului de stocare infestat, cât şi către structura de securitate.

C A P I T O L U L VIII

CONTROLUL MĂSURILOR PRIVITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE

Implementarea măsurilor de protecție a informațiilor clasificate destinate asigurării securității documentelor secrete de stat și/sau secrete de serviciu, reprezintă o obligație a tuturor autorităților și instituțiilor publice, agenților economici cu capital integral sau parțial de stat ori persoanelor juridice de drept public sau privat care gestionează astfel de informații.

În exercitarea competențelor ce îi revin în temeiul Legii nr. 182/2002, Serviciul Român de Informații, prin unitatea sa specializată – Oficiul pentru Supravegherea Secretelor de Stat, asigură coordonarea generală a activității și controlul măsurilor privitoare la protecția informațiilor clasificate la deținătorii de date și documente secrete de stat și secrete de serviciu, din sfera sa de competență. Domeniul de activitate și responsabilitate al celorlalte autorități desemnate de securitate - Ministerul Apărării Naționale, Ministerul Administrației și Internelor, Ministerul Justiției, Serviciul de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale - este strict delimitat de cadrul legislativ în domeniu.

Dintre principalele atribuții ale Serviciului menționăm: verificarea modului în care sunt respectate și aplicate normele legale în materie, constatarea nerespectării acestora, aplicarea sancțiunilor contravenționale și sesizarea organelor de urmărire penală, în situația în care faptele constatate întrunesc elementele constitutive ale unor infracțiuni.

Controlul măsurilor privitoare la protecția informațiilor clasificate se realizează de către agenți constatatori din cadrul Oficiului pentru Supravegherea Secretelor de Stat și constă în verificarea concretă a modului în care documentele secrete de stat și secrete de serviciu sunt gestionate de către entitățile deținătoare, raportat la prevederile *Legii nr. 182/2002 privind protecția informațiilor clasificate*, *HG nr. 585/2002 pentru aprobarea Standardelor de protecție a informațiilor clasificate în România*, *HG nr. 781/2002 privind protecția informațiilor secrete de serviciu* și *HG nr. 1349/2002 privind colectarea, transportul, distribuirea și protecția, pe teritoriul României, a corespondenței clasificate*.

Potrivit legii, reprezentanții instituțiilor cu atribuții de coordonare și control pe linia protecției informațiilor clasificate au acces, pe baza delegațiilor speciale și legitimațiilor de serviciu, în toate locațiile unde sunt gestionate documente secrete de stat și secrete de serviciu, conducătorii unităților controlate având obligația de a le pune la dispoziție toate datele solicitate privind modul de aplicare a măsurilor protective în materie. Nerespectarea acestor dispoziții constituie contravenții la normele privind protecția informațiilor clasificate și se sancționează, conform prevederilor legale.

La prezentarea într-o unitate ce urmează a fi controlată, agenții constatatori prezintă obiectivele activității conducătorului entității în cauză sau, în lipsa acestuia, înlocuitorului său legal, controalele desfășurându-se, de regulă, în prezența persoanelor cu atribuții nemijlocite în domeniul

protecției informațiilor clasificate (ex: funcționarul de securitate, membrii structurii), printre atribuțiile cărora se numără și relaționarea cu Autoritatea Desemnată de Securitate.

În funcție de obiectivele urmărite, controalele pot fi *de fond*, *tematice* și *în situații de urgență*, iar după modul în care sunt stabilite și organizate – *planificate*, *inopinate* și *determinate de situații de urgență*.

Controalele de fond urmăresc verificarea întregului sistem organizatoric, structural și funcțional de protecție a informațiilor clasificate, cele *tematice* vizează anumite domenii ale activității de protecție a informațiilor clasificate, iar cele *în situații de urgență* - verificarea unor aspecte punctuale, stabilite ca urmare a identificării unui risc de securitate.

* *
*

Pe parcursul controalelor se verifică modul în care, la nivelul unităților ce gestionează informații clasificate, se aplică și se respectă prevederile actelor normative în vigoare referitoare *protecția juridică*, *protecția prin măsuri procedurale*, *protecția fizică*, *protecția personalului* și *protecția surselor generatoare de informații*, acționându-se pentru stabilirea demersurilor întreprinse în vederea protejării acestora și prevenirii producerii unor incidente de securitate de natură a determina compromiterea informațiilor.

În scopul implementării măsurilor protective conform actualei legislații în materie, în cadrul fiecărei entități deținătoare de documente secrete de stat și secrete de serviciu, se numește, printr-un act administrativ al conducătorului acesteia, *structura de securitate* ori, după caz, *funcționarul de securitate*.

Conform legii, șeful structurii de securitate, respectiv funcționarul de securitate, trebuie să aibă calitatea de adjunct al conducătorului persoanei juridice sau membru al consiliului de administrație al unității.

Pe componentele *protecției juridice* și *prin măsuri procedurale*, agenții constatatori verifică dacă au fost elaborate, actualizate sau completate raportat la situația existentă la nivelul fiecărei unități, documentele procedurale prevăzute de lege (ex: *Programul de prevenire a scurgerii de informații clasificate*, *Planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor clasificate*, *Normele interne de protecție a informațiilor clasificate*, *Ghidul pe baza căruia se realizează încadrarea corectă și uniformă în nivelurile de secretizare a informațiilor secrete de stat*, *Lista cuprinzând categoriile de informații secrete de stat etc*).

Întocmirea documentelor procedurale nu trebuie să aibă un caracter pur formal, în conținutul acestora impunându-se a se reflecta cu exactitate starea de fapt din cadrul fiecărei entități gestionare de documente clasificate.

În contextul activităților de control la deținătorii de documente clasificate stabilite astfel potrivit HCM nr. 19/1972, se acordă o atenție deosebită finalizării activității de încadrare a acestora în noi clase/niveluri de secretizare, întrucât pentru prezentarea de propuneri în acest sens către persoanele sau autoritățile publice împuternicite legiuitorul a stabilit un termen de 12 luni de la data intrării în vigoare a HG nr. 585/2002, iar neîndeplinirea acestei măsuri constituie contravenție la regimul protecției informațiilor clasificate.

Verificarea modului în care sunt gestionate informațiile clasificate nu se realizează exclusiv de către Autoritatea Desemenată de Securitate, ci și de conducătorii unităților deținătoare de astfel de documente și de persoanele cu atribuții

nemijlocite în domeniu desemnate la nivelul fiecărei entități. Activitățile de control intern se efectuează periodic și pot fi atât planificate, cât și inopinate.

De asemenea, în vederea aplicării corecte și unitare a măsurilor de protecție a informațiilor clasificate, persoanele juridice de drept public sau privat ce au în subordine alte unități deținătoare de documente secrete de stat și/sau secrete de serviciu au obligația de a coordona activitatea acestora în domeniu, ceea ce presupune inclusiv evaluarea și analizarea periodică pe acest segment a modului în care se gestionează informațiile clasificate. În acest sens, anual se întocmește *Planul de control intern*, aprobat de conducătorul unității, care cuprinde, printre altele, tematica activităților, perioada în care vor fi realizate, departamentele/entitatățile ce vor fi controlate, cine execută aceste activități etc. Concluziile activităților de control intern se consemnează în procese verbale, alături de măsurile dispuse pentru înlăturarea eventualelor deficiențe constatate, ulterior urmând a se verifica dacă acestea au fost duse la îndeplinire.

Nerespectarea normelor legale în domeniu, încălcarea reglementărilor de securitate sau îndeplinirea defectuoasă a obligațiilor legale în materia protecției informațiilor clasificate pot determina compromiterea acestora, în funcție de clasa documentelor fiind aduse prejudicii siguranței naționale (în cazul informațiilor secrete de stat) sau persoanelor juridice de drept public sau privat (în cazul informațiilor secrete de serviciu).

În situația în care, la nivelul unităților deținătoare de informații clasificate, sunt identificate premisele producerii unor incidente de securitate (ex: lipsa din gestiune a unor documente secrete de stat și/sau secrete de serviciu; transmiterea acestora către alte entități fără respectarea prevederilor legale; distribuirea unor materiale clasificate către

persoane neautorizate corespunzător să le acceseze etc.), se va înștiința, de îndată, instituția cu atribuții de coordonare și control în domeniu (neîndeplinirea măsurii de a aduce la cunoștința Autorității Desemnate de Securitate indiciile din care pot rezulta premise de insecuritate pentru documente clasificate constituie contravenție la normele legale în materie) și se va desemna o comisie de cercetare administrativă care să acționeze pentru stabilirea condițiilor în care s-a produs incidentul și să propună măsurile ce se impun.

Totodată, dacă se constată săvârșirea de infracțiuni la protecția secretului de stat, conducătorului unității deținătoare îi revine obligația de a sesiza organele de urmărire penală și de a le pune la dispoziție materialele necesare probării faptelor.

Având în vedere modificările structural organizatorice survenite mai ales la nivelul autorităților și instituțiilor publice, fluctuațiile de personal (atât din funcții de conducere, cât și cu atribuții în domeniul protecției informațiilor clasificate) generează instabilitate și pot determina premise de apariție a vulnerabilităților la adresa securității informațiilor clasificate, sens în care echipele de control acordă o atenție deosebită măsurilor întreprinse pe componenta *protecției personalului* (ex: autorizarea, în condițiile legii, a tuturor persoanelor ce încadrează funcțiile nominalizate pentru acces la informații secrete de stat și secrete de serviciu; organizarea evidenței certificatelor de securitate/autorizațiilor de acces la documente clasificate ș.a.).

Pentru diminuarea riscurilor de securitate la adresa documentelor secrete de stat și secrete de serviciu, prevenirea diseminării neautorizate și gestionării defectuoase a acestora, se impune organizarea riguroasă și constantă, în baza unui *Plan* întocmit anual, a activităților de instruire protectivă cu personalul care, în îndeplinirea atribuțiilor de serviciu, accesează informații clasificate. Activitățile se consemnează, sub

semnătura titularilor, în fișele de pregătire individuală care se păstrează de către structura/funcționarul de securitate.

Respectarea *regulilor generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor clasificate* și asigurarea măsurilor necesare de evidență a acestora, asigură stabilirea, în orice moment, a locului în care se află documentele secrete de stat și secrete de serviciu din gestiune, identificarea persoanelor cărora le-au fost repartizate și gestionarea lor în conformitate cu prevederile legale.

Cu prilejul controalelor se verifică și dacă au fost instituite și completate corespunzător registrele și condicile prevăzute de actualul cadru legislativ în materie, precum și dacă operațiunile de multiplicare, arhivare și distrugere sunt efectuate conform legii. Clasa/nivelul de secretizare a documentelor se atribuie numai în baza listelor cuprinzând categoriile de informații secrete de stat și/sau secrete de serviciu, respectiv Ghidului de încadrare corectă și uniformă a informațiilor, acestea urmând a fi marcate și protejate corespunzător.

Prin consultarea borderourilor de expediție (ce se păstrează de către persoanele delegate pentru predarea-primirea corespondenței clasificate) și a registrelor de evidență se va stabili dacă documentele secrete de stat și secrete de serviciu se transportă cu respectarea strictă a HG nr. 1349/2002, respectiv prin unitatea specializată a Serviciului Român de Informații.

La nivelul deținătorilor de informații secrete de stat și/sau secrete de serviciu care gestionează astfel de documente și prin prisma participării la negocierea/derularea unor contracte clasificate se impune respectarea cu strictețe a prevederilor legale în materia *securității industriale*, aceste aspecte fiind verificate de agenții constatatori pe parcursul controalelor. În scopul desfășurării de activități contractuale ce presupun acces

la informații clasificate, reprezentanții persoanelor juridice trebuie să asigure cadrul organizatoric și procedural pentru implementarea tuturor măsurilor protective și pentru gestionarea corectă a documentelor primite/elaborate în acest context.

În ceea ce privește măsurile de *protecție fizică*, acestea trebuie dimensionate în raport de clasa/nivelul de secretizare a informațiilor, volumul și localizarea acestora (ex: gratii la ferestre, încuietori la uși, pază la intrări, siteme automate pentru supraveghere, control, acces). Totodată, încăperile unde sunt păstrate documentele clasificate vor fi marcate ca zone de securitate sau zone administrative, după caz și se vor stabili reguli cu privire la circulația în aceste incinte, astfel încât să fie permis accesul exclusiv al posesorilor de certificate de securitate/autorizații de acces.

Pe fondul înregistrării, din ce în ce mai frecvent, a unor incidente de securitate generate de diseminarea neautorizată a informațiilor clasificate în format electronic, finalizarea procedurilor de acreditare a sistemelor informatice și de comunicații aparținând unităților deținătoare de informații secrete de stat și protejarea corespunzătoare a stațiilor de lucru pe care se prelucrează și stochează informații secrete de serviciu trebuie să devină un obiectiv prioritar al acestora.

Concluziile activității de control și măsurile dispuse pentru remedierea disfuncțiilor, cuprinse în *documentul de constatare*, sunt prezentate conducătorului unității /înlocuitorului său legal și persoanelor în prezența cărora s-a desfășurat controlul (de regulă, funcționarului de securitate sau șefului structurii de securitate/membrilor structurii de securitate), care semnează de luare la cunoștință. Precizăm faptul că măsurile și termenele stabilite de echipa de control pentru înlăturarea deficiențelor existente pe linia protecției informațiilor clasificate nu reprezintă

simple recomandări, ci au caracter obligatoriu, venind în sprijinul deținătorilor de documente clasificate la nivelul cărora există lacune în sistemul protectiv, care pot genera vulnerabilități ale acestuia.

În situația în care, pe timpul activității se constată cazuri de încălcare/nerespectare a prevederilor legale în materie ce constituie contravenții la normele privind protecția informațiilor clasificate, agenții constatatori încheie *Procesul verbal de constatare a contravențiilor și de aplicare a sancțiunilor*.

Un exemplar al documentului de constatare și, atunci când se impune, al procesului verbal sunt predate reprezentantului legal al persoanei juridice controlate (cu excepția situației în care contravenientul este altul decât persoana juridică ce a făcut obiectul controlului sau conducătorul unității, în acest caz actul sancționator fiind înmânat persoanei în cauză).

Activitatea de control va fi consemnată și în Registrul Unic de Control prevăzut de Legea nr. 252/2003, dacă un astfel de document a fost instituit la nivelul entității controlate.

Respectarea măsurilor de protecție a informațiilor clasificate trebuie să reprezinte o preocupare constantă a deținătorilor de astfel de date, formalismul și interpretarea personală a dispozițiilor legale în materie favorizând apariția premiselor producerii unor incidente de securitate, cu consecințe negative și prejudicii atât în planul siguranței naționale, cât și în activitatea persoanelor juridice de drept public sau privat.

I. ***Măsuri protective adoptate ulterior reorganizării autorităților și instituțiilor publice***

În ultimii ani, comasarea, divizarea unor ministere și preluarea atribuțiilor unor agenții guvernamentale în cadrul acestora, schimbarea raporturilor de subordonare și coordonare etc, au generat influențe inclusiv în domeniul

protecției informațiilor clasificate, implementarea măsurilor protective având de suferit din punctul de vedere al continuității acestor demersuri și al caracterului lor unitar.

Documentele procedurale elaborate în aplicarea prevederilor legislației în materia protecției informațiilor clasificate, anterior modificărilor structural-organizatorice, și-au încetat aplicabilitatea, impunându-se să fie stabilite, practic după fiecare reorganizare, aceleași măsuri incipiente (ex: organizarea *structurii de securitate* și a *compartimentului special* pentru gestionarea documentelor clasificate; elaborarea *listelor cuprinzând categoriile de informații clasificate* din domeniul de activitate, cu consultarea obligatorie a tuturor entităților aflate în subordinea, coordonarea sau sub autoritatea instituțiilor centrale; întocmirea *listelor cu obiectivele, sectoarele și locurile care prezintă importanță deosebită pentru protecția informațiilor clasificate*, în baza consultărilor cu unitățile teritoriale subordonate; stabilirea funcțiilor și persoanelor care, în îndeplinirea atribuțiilor de serviciu, necesită acces la documente secrete de stat și secrete de serviciu; reconfigurarea *Programului de prevenire a scurgerii de informații clasificate* și a *Planului de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor clasificate* prevăzut la art. 120 din *Standardele naționale* etc).

Ulterior intrării în vigoare a noilor actelor normative ce reglementează organizarea și funcționarea entităților deținătoare de informații clasificate este esențial să se stabilească, în primul rând, dacă au intervenit modificări în ceea ce privește clasa/nivelul maxim de secretizare a informațiilor gestionate.

În situația divizării unor unități, se va acționa pentru identificarea tuturor locațiilor în care sunt gestionate informații și materialele clasificate, inventarierea acestora și încheierea de

protocoale de predare-primire, inclusiv în ceea ce privește actele de cercetare administrativă a incidentelor de securitate către structura de securitate a noii entități competente din punctul de vedere al domeniului de activitate, în vederea definitivării cercetărilor și soluționării incidentelor conform legii.

Complementar obligațiilor ce le revin autorităților și instituțiilor publice centrale, de a-și implementa măsurile protective raportat la schimbările determinate de reorganizările structural-organizatorice, acestea trebuie să se implice în coordonarea pe linia protecției informațiilor clasificate a unităților din subordine/ sub autoritatea/din coordonare și pentru a verifica modul în care la nivelul acestora se respectă și se aplică prevederile legale în materie.

De cele mai multe ori, odată cu reorganizarea au fost abrogate și hotărârile de Guvern prin care fuseseră aprobate *listele cuprinzând categoriile de informații secrete de stat* aparținând instituțiilor în cauză, fiind supuse aprobării Guvernului noi astfel de liste, raportat la situația existentă. În acest context, comunicarea tuturor documentelor actualizate care au aplicabilitate și la nivelul unităților subordonate (ex: *Ghidul pe baza căruia se realizează clasificarea corectă și uniformă a informațiilor*, *Normele interne privind protecția informațiilor clasificate* etc.) este imperios necesară, în vederea aplicării unitare a prevederilor legale în materie.

În practică, au fost întâlnite situații în care unități subordonate unor instituții și autorități publice dețineau extrase din vechile liste cuprinzând categoriile de informații clasificate, astfel încât, ulterior reorganizării, la nivel local clasificarea informațiilor se realiza în absența unei baze legale, iar pe fondul lipsei coordonării și controlului intern, instituțiile centrale nu avea cunoștință despre aceste aspecte. În alte cazuri, documentele nu se clasificau corespunzător noilor liste, deși

acestea cuprindeau categorii de astfel de documente specifice activității entităților teritoriale.

Este absolut necesar ca documentele procedurale să aibă un caracter practic-aplicativ, în conținutul acestora trebuind înfățișat modul concret de gestionare a documentelor clasificate (ex: stabilirea, prin *Normele interne*, a fluxului documentelor clasificate în instituție). Absența detaliilor referitoare la modul de gestionare a informațiilor (evidență, întocmire, păstrare, procesare, multiplicare, manipulare, transport, transmitere, distrugere) sau prezentarea lacunară a acestora au determinat, nu în puține cazuri, producerea unor incidente de securitate.

De asemenea, nerespectarea regulilor privind redactarea documentelor clasificate (ex: înscrierea, pe fiecare pagină, a clasei sau nivelului de secretizare atribuit acestuia; menționarea, în antet, a unității emitente, numărului și datei înregistrării și a numărului de exemplare; indicarea, după caz, la sfârșitul textului documentului de bază, a numărului de înregistrare, numărului de file și clasei/nivelului de secretizare a anexelor) favorizează apariția riscurilor de securitate. Spre exemplu, un document clasificat care nu este marcat și înregistrat corespunzător, scos astfel de sub incidența prevederilor legale în materie, poate fi accesat de persoane neautorizate sau fără respectarea principiului necesității de a cunoaște, multiplicat/distrus/arhivat, fără respectarea prevederilor legale în domeniu sau transmis altor entități, cu încălcarea prevederilor *HG nr. 1349/2002 privind colectarea, transportul, distribuirea și protecția, pe teritoriu României, a corespondenței clasificate* (în această ultimă situație, materialul va fi gestionat și la nivelul destinatarilor fără a se cunoaște caracterul său clasificat, nefiind protejat conform legii).

În ceea ce privește *programele de prevenire a scurgerii de informații clasificate*, actualizările acestora trebuie efectuate cu operativitate, iar modificările și completările transmise

Serviciului Român de Informații ori de câte ori situația o impune. Cu prilejul controalelor efectuate a reieșit că, nu de puține lor, acestea au fost actualizate ulterior primirii notificărilor acțiunilor de control.

În practică, s-a constatat că, pe fondul modificărilor structural-organizatorice, fluctuațiile de personal (atât cu funcții de conducere, cât și cu atribuții nemijlocite în domeniul protecției informațiilor clasificate) pot genera riscuri și vulnerabilități la adresa securității informațiilor clasificate. La apariția acestora concură și cunoașterea deficitară a dispozițiilor legale în materie ori tratarea cu superficialitate a domeniului protecției informațiilor clasificate de către unele persoane cu responsabilități pe această linie. În vederea evitării unor asemenea situații, trebuie să se acorde o mai mare importanță activităților de control intern și de instruire protectivă, caracterul riguros și constant al acestora contribuind la prevenirea diseminării neautorizate și gestionării defectuoase a documentelor clasificate.

Conform celor stabilite prin *listele funcțiilor care necesită acces la informații secrete de stat*, conducătorilor unităților le revine obligația de a solicita, în scris, ORNISS, autorizarea accesului la astfel de informații pentru toate persoanele ce ocupă funcțiile în cauză. Nerespectarea prevederilor legale în acest sens (inclusiv sub motivul că angajații nominalizați tergiversează sau chiar refuză completarea chestionarelor de securitate) constituie contravenție la normele privind protecția informațiilor clasificate.

O situație aparte o reprezintă avizarea negativă pentru acces la informații secrete de stat, atât a personalului care își desfășoară activitatea la „centru”, cât și pentru cel ce încadrează unitățile subordonate. Au existat cazuri concrete în care, deși ORNISS a comunicat structurilor centrale ale unor instituții publice astfel de avize pentru persoane a căror activitate se

desfășura la nivel teritorial, acest aspect nu au fost aduse la cunoștința persoanelor în cauză/structurilor teritoriale ale instituției și nu au fost dispuse măsuri pentru restricționarea accesului la informații secrete de stat, în conformitate cu dispozițiile legale.

Reorganizarea instituțională poate produce schimbări inclusiv în sistemul de *protecție fizică* a informațiilor clasificate (spre exemplu schimbarea amplasamentului Compartimentului Documente Clasificate, reconfigurarea zonelor de securitate și administrative, înlocuirea societăților de pază etc.), toate acestea trebuind evidențiate în *planurile de pază și apărare* prevăzute de art. 120 din *Standarde*. În eventualitatea în care intervin modificări în ceea ce privește sediul noii entități sau clasa/nivelul de secretizare a informațiilor gestionate, este obligatoriu ca măsurile protective pe acest segment să fie reevaluate, dimensionate și implementate în raport cu noua situație de fapt, urmând a fi evidențiate și în cuprinsul documentelor procedurale prevăzute de legislația în materie și aduse la cunoștința autorității desemnate de securitate.

Nu în ultimul rând, implementarea măsurilor protective trebuie să vizeze și sursele generatoare de informații, la nivelul multor autorități publice și instituții centrale fiind constatate neconformități privind aplicarea legislației în domeniul protecției informațiilor clasificate vehiculate în format electronic. În acest sens, tuturor persoanelor juridice de drept public sau privat care gestionează informații secrete de stat le revine obligația de a relaționa cu ORNISS în vederea acreditării sistemelor informatice și de comunicații proprii.

Studiu de caz:

Ulterior intrării în vigoare a Legii nr. 329/2009 privind reorganizarea unor autorități și instituții publice, raționalizarea cheltuielilor publice, susținerea mediului de afaceri și respectarea acordurilor-cadru cu Comisia Europeană și Fondul Monetar Internațional, OSSS a realizat a activitate de control la o instituție înființată urmare comasării prin fuziune a două entități care funcționau în localități diferite și la nivelul cărora se gestionau informații secrete de stat și secrete de serviciu.

După reorganizare, în cadrul noii entități a fost organizată activitatea structurii de securitate și s-a procedat la preluarea documentelor clasificate gestionate de la instituția desființată, transformată în punct de lucru. În acest din urmă sens, a fost întocmit un proces verbal de predare-primire a informațiilor clasificate, tipizatelor de evidență, autorizațiilor de acces și a altor materiale conexe.

Astfel, reprezentanții instituției controlate considerau că la nivelul punctului de lucru nu se mai dețineau documente clasificate și că nu se mai impunea instituirea măsurilor protective legale.

Cu prilejul controlului a reieșit că, în fapt, la sediul respectivei entități se mai transmiteau, periodic, informații clasificate, după consultare, acestea restituindu-se unității centrale.

O astfel de situație reclamă, de asemenea, implementarea tuturor măsurilor stabilite de legislația în materie, raportat la clasa/nivelul maxim de secretizare a informațiilor gestionate, chiar și pentru o perioadă scurtă de timp.

Printre măsurile prioritare stabilite în contextul controlului în sarcina structurii centrale s-au regăsit:

- inventarierea tuturor documentelor secrete de stat și secrete de serviciu gestionate de către entitatea nou înființată și înștiințarea SRI în legătură cu eventualele premise ale producerii unor incidente de securitate;

- reevaluarea și elaborarea tuturor documentelor procedurale prevăzute de lege și înaintarea SRI, spre avizare, a Programului de prevenire a scurgerii de informații clasificate, având anexat Planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor clasificate;

- inițierea procedurilor legale în vederea eliberării documentelor de acces la informații clasificate pentru salariații instituției (inclusiv pentru cei din cadrul punctului de lucru), conform listelor funcțiilor și persoanelor care necesită acces la astfel de informații, stabilite de conducerea instituției;

- relaționarea cu ORNISS pentru acreditarea sistemelor informatice și de comunicații.

II. Informațiile clasificate gestionate de persoanele juridice aflate în procedura insolvenței

Datorită lipsei personalului specializat, a fondurilor băneşti şi probabil a incertitudinii, unitățile intrate în procedura insolvenței, reglementată de Legea nr. 85/2006, cu modificările și completările ulterioare, se află într-o situație specială în ceea ce privește protecția informațiilor clasificate gestionate.

Din acest punct de vedere, principala responsabilitate ce revine administratorilor/lichidatorilor judiciari constă în clarificarea regimului juridic al documentelor clasificate deținute de societățile în cauză, anterior finalizării operațiunilor de lichidare a acestora. Prin *clarificarea regimului juridic* trebuie să se aibă în vedere, în principal, încadrarea în noi clase de secretizare a informațiilor clasificate potrivit Hotărârii Consiliului de Miniştri nr. 19/1972, declasificarea, în condițiile legislației în domeniu, a informațiilor proprii, respectiv remiterea acestora către emitenți. Până la finalizarea demersurilor menționate, trebuie asigurate măsuri minime de

protecție a documentelor clasificate aflate în gestiunea agenților economici, cum ar fi: autorizarea corespunzătoare a persoanelor care le inventariază și gestionează, păstrarea acestora în locații ce vor fi marcate corespunzător clasei/nivelului de secretizare a informațiilor, remiterea către emitenți numai prin unitatea specializată a SRI ș.a.

Studiu de caz:

Pe fondul preconizatei lichidări a unei societăți comerciale, deținătoare de informații secrete de stat, nivel maxim de secretizare „strict secret de importanță deosebită", stabilite astfel conform HCM nr. 19/1972 și secrete de serviciu, clasificate potrivit Legii nr. 182/2002 și actelor normative subsecvente, a fost efectuat un control pe linia protecției acestor informații.

Deși preluase întreaga responsabilitate a conducerii activității debitorului, în condițiile art. 25 lit. b) din Legea nr. 85/2006 cu modificările și completările ulterioare, lichidatorul judiciar nu procedase la inventarierea tuturor documentelor clasificate aflate în gestiunea agentului economic și nu se implementaseră măsurile protective prevăzute de legislația în domeniu.

Agenții constatatori au stabilit ca, în regim de urgență, să fie dispusă inventarierea tuturor documentelor clasificate din gestiunea societății și să fie prezentate, persoanelor/autorităților publice competente să atribuie niveluri de secretizare, propuneri în vederea încadrării informațiilor clasificate potrivit HCM nr. 19/1972 în noi clase sau niveluri de secretizare, după caz.

Totodată, întrucât nicio persoană din cadrul unității/firmei lichidatoare nu fusese autorizată să acceseze informații secrete de stat, au fost iterate dispozițiile legale referitoare la avizarea accesului la astfel de informații a persoanelor nominalizate să le acceseze – inventarieze.

Având în vederea situația de fapt din cadrul societății, s-a mai stabilit să fie contactați emitenții documentelor clasificate din gestiunea acesteia/succesorii acestora în drepturi/fostul minister de resort, în vederea clarificării actualului regim juridic al informațiilor, și, după caz, pentru obținerea acordului de remitere a documentelor clasificate emise de respectivele entități, prin unitatea specializată a Serviciului Român de Informații în colectarea, transportul, distribuirea și protecția corespondenței clasificate, astfel încât, anterior radierii agentului economic din Registrul Comerțului, informațiile clasificate să fie declasificate în condițiile legii/remise emitenților.

III. Protecția informațiilor clasificate la agenții economici având ca obiect de activitate inventarierea și arhivarea

Sub motivația lipsei personalului și volumului mare de documente din gestiune (mai ales circumscrise HCM nr. 19/1972), o parte a deținătorilor de informații clasificate au apelat la contractarea unor servicii de inventariere și arhivare, inclusiv a informațiilor clasificate, cu firme specializate.

În cele mai multe cazuri, în contractele respective nu au fost inserate clauze referitoare la protecția informațiilor clasificate, în condițiile în care exista posibilitatea ca prestatorii de servicii, în executarea contractelor, să identifice astfel de informații în arhivele unităților. Totodată, conducătorii unităților deținătoare de documente secrete de stat/secrete de serviciu nu s-au asigurat că angajații firmelor contractante sunt autorizați, în condițiile legii, să acceseze informații din clasa de secretizare supusă inventarierii/arhivării.

În aplicarea prevederilor legislației în domeniu, pentru negocierea/executarea unor contracte ce presupun accesul la informații secret de stat, este necesar să se întreprindă măsurile

ce se impun pe palierul *securității industriale* (încheierea anexelor de securitate la respectivele contracte, obținerea de către contractanți a autorizațiilor de securitate industrială / certificatelor de securitate industrială etc).

În cazul în care conducătorii unităților deținătoare de documente clasificate (atât în baza Legii nr. 182/2002 și actelor normative subsecvente, cât și potrivit HCM nr. 19/1972), decid externalizarea serviciilor care implică orice operațiune considerată „gestionare", în sensul art. 3 din *Standardele naționale*, a acestor informații, trebuie să conștientizeze că acest fapt se poate realiza numai cu stricta respectare a cadrului normativ în materie, pentru prevenirea producerii unor incidente de securitate, săvârșirii de contravenții la normele privind protecția informațiilor clasificate sau chiar de infracțiuni la protecția secretului de stat.

Studiu de caz:

Cu ocazia unui control realizat la un agent economic a reieșit că reprezentanții legali ai acestuia au încheiat un contract de prestări servicii având ca obiect „administrarea și depozitarea arhivei" cu o firmă specializată. Conform clauzelor contractuale, prestatorul de serviciu nu își asuma răspunderea pentru lipsa unor documentații sau dosare din arhiva beneficiarului.

Documentațiile, de nivel maxim de secretizare „strict secret", au fost preluate de firma contractată și transportate prin mijloace proprii la sediul acesteia, cu încălcarea dispozițiilor art. 13 alin. (1) din HG nr. 1349/2002.

Raportat la cele constatate, s-a dispus relaționarea dintre contractor și contractant în vederea reglementării situației juridice și responsabilităților ce revin celor două părți pentru protecția eventualelor informații clasificate preluate în baza contractului încheiat, fiind stabilite și măsuri în aplicarea prevederilor art. 88-90 din Standardele naționale.

Deoarece punerea la dispoziția societății de inventariere a documentelor secrete de stat întrunea elementele constitutive ale infracțiunii prevăzute de art. 252 Cod penal – Neglijența în păstrarea secretului de stat, potrivit căruia ("neglijența care are drept urmare distrugerea, alterarea, pierderea sau sustragerea unui document ce constituie secret de stat, precum și neglijența care a dat prilej altei persoane să afle un asemenea secret, dacă fapta este de natură să aducă atingere intereselor statului"), au fost sesizate organele de urmărire penală competente.

O situație similară a fost identificată la nivelul unei instituții publice, care contractase cu o firmă specializată pentru inventarierea documentelor din arhiva proprie. Deși se cunoștea faptul că printre documentele depozitate în spațiul de arhivă se regăseau inclusiv unele cu caracter clasificat, stabilite astfel potrivit HCM nr. 19/1972, reprezentanții unității controlate au ignorat acest aspect și nu au întreprins niciun demers de clasificare a contractului și de protejare a acestora. Mai mult, nici după identificarea unor astfel de informații de către angajații agentului economic desemnați cu organizarea arhivei instituției în cauză nu au fost declanșate procedurile pe segmentul securității industriale, sens în care au fost dispuse măsuri pentru intrarea în legalitate.

IV. Securitatea documentelor clasificate aparținând statului român, aflate în custodia unor persoane juridice de drept public sau privat

Fiecare deținător de secrete are obligația de a implementa, raportat la clasa/nivelul de secretizare a acestora, toate măsurile protective prevăzute de lege, inclusiv în situația în care gestionează exclusiv informații emise de alte entități.

Respectarea normelor legale în materie și asigurarea protecției permanente a documentelor secrete de stat și secrete de serviciu trebuie să reprezinte o preocupare constantă a conducătorilor unităților care le gestionează, a structurilor / funcționarilor de securitate, precum și a tuturor persoanelor care, în exercitarea atribuțiilor de serviciu, accesează astfel de informații.

O categorie aparte o reprezintă datele și informațiile clasificate, indiferent de modalitatea de stocare, ce aparțin statului român și care se referă la proprietatea publică, vehiculate, cu precădere, în contextul unor activități contractuale.

Legislația în domeniu prevede, în mod expres, ca partea contractantă deținătoare de informații clasificate ce vor fi utilizate în derularea unui contract să acționeze pentru clasificarea și definirea tuturor componentelor acestuia, urmând a stipula într-o anexă de securitate clauzele și procedurile de protecție.

În situația în care pe parcursul derulării contractelor, inițial neclasificate, apare necesitatea protejării unor date și informații, contractorii (beneficiarii lucrărilor și serviciilor executate de unitățile prestatoare) vor declanșa procedurile de clasificare a acestora.

De asemenea, în ipoteza în care contractanții intenționează să cedeze unor subcontractanți realizarea unor părți din contractele clasificate, obligația ce le revine este de a se asigura că aceștia din urmă dețin autorizații sau certificate de securitate industrială, după caz.

Pe de altă parte, reprezentanții instituțiilor care pun la dispoziția diverselor entități informații clasificate, cu atât mai mult în cazurile în care acestea reprezintă proprietate publică a statului, au obligația de a verifica modul în care custozii le asigură protecția. Avem în vedere atât protecția fizică a

respectivelor documente, a personalului desemnat să le acceseze, cât respectarea regulilor de evidență, întocmire a materialelor subsecvente, păstrare, procesare, multiplicare, manipulare, transport, transmitere și distrugere.

Studiu de caz:

În contextul unei activități de control la o instituție a statului, a rezultat că acesta încheiase o serie de contracte neclasificate, cu toate că în cadrul cărora se vehiculau date secrete de stat și secrete de serviciu aparținând statului român, cu mai mulți agenți economici.

În absența măsurilor protective la nivelul agenților economici în cauză, documentațiile erau gestionate cu încălcarea dispozițiilor legale în materie și expuse în permanență pericolului de a fi compromise (prin acces neautorizat, pierdere, distrugere etc.). Mai mult, documentațiile rezultate din activitățile stabilite prin contracte, emise atât de contractor cât și de contractant nu purtau marcajele corespunzătoare conținutului lor, astfel că erau scoase de sub incidența prevederilor legii.

Deși în cuprinsul contractelor se stipula obligativitatea realizării de către instituția statului a unor controale privind modul de gestionare a informațiilor puse la dispoziție în contextul derulării activităților circumscrise contractului, acestea nu fuseseră realizate și nu exista nicio evidență a documentelor clasificate transmise agenților economici.

Raportat la cele constatate, s-a dispus ca, în regim de urgență, să se acționeze pentru identificarea tuturor entităților cărora le-au fost puse la dispoziție documente secrete de stat și secrete de serviciu, stabilirea cu certitudine a clasei/nivelului de secretizare a documentelor în cauză, verificarea modului în care acestora li se asigură protecția, prin efectuarea de controale în cadrul agenților economici și punerea în aplicare a dispozițiilor Standardelor naționale privind regulile de evidență, întocmire,

păstrare, procesare, multiplicare, manipulare, transport, transmitere și distrugere a informațiilor clasificate.

Totodată, raportat la nivelul de secretizare a documentațiilor,, s-a stabilit să fie întreprinse demersurilor legale în domeniul securității industriale, atât de contractor (clasificarea contractelor și încheierea anexelor de securitate), cât și de contractanți (obținerea certificatelor de securitate industrială emise de Oficiul Registrului Național al Informațiilor Secrete de Stat).

Nu în ultimul rând, pentru a evita excluderea de sub incidența reglementărilor protective în vigoare a unor informații circumscrise secretului de stat, s-a stabilit ca unitatea controlată să analizeze categoriile de astfel de informații specifice obiectului său de activitate și să reanalizeze lista cuprinzând aceste categorii, urmând a o supune spre aprobare Guvernului.

V. Protecția informațiilor clasificate potrivit HCM nr. 19/1972 până la încadrarea în noi clase/niveluri de secretizare

Potrivit art. 18 alin. (1) din *Standardele naționale de protecție a informațiilor clasificate în România*, aprobate prin HG nr. 585/2002, în termen de 12 luni de la intrarea în vigoare a acestui act normativ trebuia clarificată situația juridică a informațiilor clasificate potrivit HCM nr. 19/1972, sens în care toate unitățile deținătoare de astfel de informații trebuiau să prezinte, persoanelor sau autorităților publice împuternicite (evidențiate la art. 19 din Legea nr. 182/2002), propuneri privind încadrarea acestora în noi clase și niveluri de secretizare, după caz.

Conform alin. (2) al art. 18, până la finalizarea acestor demersuri, informațiile secrete de stat și secrete de serviciu, circumscrise vechiului cadru legislativ în materie, își păstrează clasa/nivelul de secretizare și sunt protejate corespunzător

actualei legislații (Legea nr. 182/2002 *privind protecția informațiilor clasificate*, HG nr. 585/2002 *pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România*, HG nr. 781/2002 *privind protecția informațiilor secrete de serviciu* şi HG nr. 1349/2002 *privind colectarea, transportul, distribuirea şi protecția, pe teritoriul României, a corespondenței clasificate*).

Deşi dispozițiile legale cu privire la reglementarea situației acestor documente sunt clare, iar termenul indicat de legiuitor este strict determinat, mai există deținători de informații clasificate în baza HCM nr. 19/1972 (autorități şi instituții publice centrale, unități aflate în subordinea, coordonarea sau sub autoritatea acestora, precum şi agenți economici) care nu au finalizat activitatea de încadrare a acestora în noi clase/niveluri de secretizare.

O parte dintre aceştia au considerat, în mod eronat, că este suficientă înaintarea către persoanele sau autoritățile publice împuternicite să atribuie niveluri de secretizare a unor propuneri cu caracter general, care să vizeze reîncadrarea tuturor documentelor secrete de stat circumscrise HCM nr. 19/1972 din gestiune în clasa *„secret de serviciu”*, abordare contrară legislației în domeniu.

Primul pas pentru clarificarea situației juridice a informațiilor din categoria celor despre care facem vorbire este inventarierea acestora şi confruntarea documentelor identificate fizic în gestiune cu cele consemnate în formele de evidență (registre, condici, borderouri). Având în vedere că documentațiile în cauză au fost emise cu mult timp în urmă, precum şi faptul că la nivelul deținătorilor, peste ani, au intervenit numeroase modificări (ex: schimbări de sedii; fluctuații de personal etc.), în mai multe situații au fost semnalate neconcordanțe între existentul în gestiune şi consemnările din registre. Pe de altă parte, s-a constatat că unele unități nu mai regăsesc registrele de

evidență, astfel că rezultatele inventarierii nu pot fi confruntate cu acestea şi nu se poate stabili dacă au fost identificate toate documentele clasificate ce au intrat în gestiunea entității respective.În toate aceste situații, se impune înştiinţarea autorității desemnate de securitate.

Neregăsirea unor documente clasificate constituie premisele producerii unui incident de securitate, sens în care, la nivelul deținătorilor de documente clasificate, se va acționa în conformitate cu prevederile art. 88-90 din *Standardele naționale* (pentru informațiile secrete de stat), respectiv art. 11 din HG nr. 781/2002 (pentru informațiile secrete de serviciu). Astfel, conducătorii unităților au obligația de a desemna, printr-un act intern, o comisie de cercetare administrativă care să stabilească împrejurările în care s-a produs incidentul de securitate, dacă respectivele documente au fost compromise şi să propună măsuri de remediere. Aspectele rezultate în urma cercetării administrative şi măsurile dispuse la finalizarea acesteia trebuie, de asemenea, comunicate autorității desemnate de securitate.

Propunerile de încadrare în noi clase/niveluri de secretizare a documentelor clasificate stabilite astfel potrivit HCM nr. 19/1972 vor fi formulate numai după evaluarea acestora, analizându-se dacă se impune sau nu păstrarea clasei/nivelului de secretizare.

Până la finalizarea activităților sus menționate şi stabilirea noii clase/nivelului de secretizare pentru toate documentele clasificate în baza vechiului cadru normativ, acestea vor fi protejate corespunzător actualei legislații. Spre exemplu, persoanele desemnate cu inventarierea şi evaluarea acestora trebuie să fie autorizate corespunzător, iar măsurile de protecție fizică dimensionate în raport cu caracterul informațiilor (locațiile în care sunt păstrate vor fi marcate ca zone de securitate sau administrative şi vor fi asigurate împotriva accesului neautorizat

cu sisteme de control, antiefracție, antiincendiu, de supraveghere video etc.).

Având în vedere că anumiți emitenți solicită remiterea unor documente clasificate, reiterăm obligativitatea restituirii acestora exclusiv prin intermediul unității specializate a Serviciului Român de Informații, conform dispozițiilor HG nr. 1349/2002.

Studiu de caz:

Șeful structurii de securitate a unei unități deținătoare de informații clasificate potrivit HCM nr. 19/1972 a înaintat conducerii entității în cadrul căreia își desfășura activitatea, un referat prin care propunea distrugerea documentelor clasificate emise de unitatea în cauză, pe motiv că datele și informațiile conținute ar fi perimate și nu mai reprezentau interes.

Pe fondul necunoașterii prevederilor legale în domeniu, referatul menționat a fost aprobat, iar documentațiile clasificate considerate „perimate" și „lipsite de interes" au fost distruse.

Potrivit procesului verbal prezentat agenților constatatori cu ocazia acțiunii de control, au fost distruse, prin incinerare, documentații secrete de stat și secrete de serviciu aparținând atât organizației controlate, cât și altor emitenți.

Fapta descrisă - distrugerea ilegală a documentelor clasificate – constituie incident de securitate și se circumscrie prevederilor art. 252 Cod penal – „neglijență în păstrarea secretului de stat", fiind susceptibilă de a atrage răspunderea penală, atât a șefului structurii de securitate, cât și a conducerii persoanei juridice.

*

* *