ASPECTE PRACTICE PRIVIND CONDIŢIILE DE IMPLEMENTARE A MĂSURILOR DE PROTECŢIE ŞI REGULILE PRIVIND GESTIONAREA ŞI TRANSPORTUL DOCUMENTELOR CLASIFICATE

Obiectivele, sectoarele şi locurile în care sunt gestionate informaţii secrete de stat trebuie protejate fizic împotriva accesului neautorizat, răspunderea pentru organizarea şi aplicarea măsurilor de protecţie revenind, potrivit legii, conducătorilor autorităţilor şi instituţiilor publice, agenţilor economici cu capital integral sau parţial de stat, respectiv fiecărei persoane juridice care gestionează astfel de informaţii.

În funcţie de clasa şi/sau nivelul informaţiilor secrete de stat, zonele în care acestea sunt manipulate sau stocate trebuie organizate şi administrate în aşa fel încât să corespundă uneia din următoarele categorii:

a) **zonă de securitate clasa I** care presupune că orice persoană aflată în interiorul acesteia are acces la informaţii secrete de stat, de nivel "strict secret de importanţă deosebită" şi "strict secret";

b) **zonă de securitate clasa II** pentru gestionarea informaţiilor clasificate secret de stat, nivel "secret";

c) **zonă administrativă** stabilită în jurul zonelor de securitate şi unde vor fi gestionate numai informaţii secrete de serviciu.

Pentru a se evita diseminarea neautorizată a informaţiilor secrete de stat, acestea trebuie gestionate numai în **zone special amenajate care să le asigure protecţia fizică şi care necesită: perimetru clar determinat, controlul sistemului de intrare, indicarea clasei şi nivelului de secretizare a informaţiilor aflate în zonă.**

Intrărilor în zonele de securitate li se va institui **un sistem de control pentru a preveni accesul persoanelor neautorizate la informaţii secrete de stat**. Intrările în zonele de securitate vor fi controlate printr-un sistem de intrare sau printr-unul special de recunoaştere personală aplicat personalului permanent. Se recomandă ca permisul de intrare să nu arate, în clar, identitatea organizaţiei emitente sau locul unde deţinătorul are acces. Pentru controlul intrărilor şi ieşirilor poate fi implementat un sistem de identificare automat, care trebuie considerat suplimentar, fără a presupune înlocuirea totală a pazei**.**

Când se folosesc sisteme de alarmă, televiziune cu circuit închis sau alte dispozitive destinate supravegherii zonelor de securitate sau protecţiei informaţiilor clasificate, sursa de alimentare trebuie să aibă atât conectare permanentă, cât şi de rezervă. Orice defecţiune sau intervenţie neautorizată asupra acestor sisteme trebuie să declanşeze o alarmă sau un alt sistem de avertizare pentru personalul care monitorizează instalaţia respectivă.

Clădirile, spaţiile, locurile în care se află informaţii secrete de stat trebuie protejate împotriva accesului neautorizat, **măsurile de securitate fiind dimensionate în raport cu: caracteristicile clădirii, clasa de secretizare a documentelor, calitatea containerelor şi locul de dispunere a zonelor de securitate.**

Cheile containerelor şi încăperilor de securitate nu trebuie scoase din clădirea sau zona de securitate în care se află documentele clasificate, acestea fiind protejate conform nivelului de secretizare a informaţiilor la care permit accesul. Pentru cazurile de urgenţă, un rând de chei suplimentare (o evidenţă scrisă a fiecărei combinaţii) va fi păstrat în plicuri mate într-un compartiment stabilit de conducerea instituţiei/agentului economic, sub control corespunzător, în containere separate. Cheilor şi plicurilor trebuie să li se asigure protecţie la nivelul de securitate la care acestea permit accesul.

Cheile şi combinaţiile vor fi schimbate: de fiecare dată când are loc o schimbare de personal, când se constată că a avut loc un eveniment de natură să le facă vulnerabile şi la intervale regulate de timp.

Copiatoarele şi dispozitivele telefax trebuie protejate fizic în măsura în care este necesar să se garanteze folosirea lor numai de către persoane autorizate.

Accesul în încăperile protejate împotriva ascultărilor se va controla în mod special. Periodic, personalul specializat în depistarea dispozitivelor de ascultare va efectua inspecţii fizice şi tehnice. De asemenea, astfel de inspecţii se vor organiza, în mod obligatoriu, ca urmare a oricărei intrări neautorizate, a unei suspiciuni privind accesul personalului extern şi după executarea lucrărilor de reparaţii, întreţinere, zugrăvire, redecorare etc. Niciun obiect nu se va introduce în aceste zone fără a fi verificat de către personalul specializat în depistarea dispozitivelor de ascultare.

În mod curent, în zonele asigurate din punct de vedere tehnic nu se vor instala telefoane. Totuşi, când instalarea acestora este absolut necesară, trebuie prevăzute cu un dispozitiv de deconectare pasiv.

Inspecţiile de securitate tehnică în zonele unde se poartă discuţii extrem de sensibile trebuie întreprinse premergător începerii convorbirilor, atât pentru identificarea fizică a dispozitivelor de ascultare cât şi pentru verificarea sistemelor telefonice, electrice sau de altă natură, care ar putea fi folosite ca mediu de atac.

Înainte de a fi folosite în zonele în care se lucrează ori se discută despre informaţii de nivel "strict secret de importanţă deosebită" şi "strict secret", echipamentele de comunicaţii şi dotările de orice fel din birouri, în principal cele electrice şi electronice, trebuie verificate de specialişti în securitatea comunicaţiilor, pentru a preveni transmiterea ilicită sau din neglijenţă a unor informaţii inteligibile. În aceste zone se va organiza o evidenţă a tipului şi a numărului de inventar ale fiecărei piese de mobilier sau echipament introduse sau mutate din încăperi, care va fi păstrată sub cheie, iar cheile vor fi protejate corespunzător.

Măsurile procedurale de protecţie a informaţiilor secrete de stat vor fi integrate în *Programul de prevenire a scurgerii de informaţii clasificate*, întocmit potrivit Anexei nr. 10 din S*tandardele naţionale de protecţie a informaţiilor clasificate în România*, aprobate prin HG nr. 585/2002, care va fi prezentat, spre avizare, Serviciului Român de Informaţii. Unităţile care gestionează informaţii secrete de stat vor întocmi *Planul de pază şi apărare a obiectivelor, sectoarelor şi locurilor care prezintă importanţă deosebită pentru protecţia informaţiilor clasificate*, ce va fi înregistrat potrivit celui mai înalt nivel de secretizare a informaţiilor protejate şi va cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

Planul de pază şi apărare va fi anexat *Programului de prevenire a scurgerii de informaţii clasificate* şi va cuprinde:

a) date privind delimitarea şi marcarea zonelor de securitate, dispunerea posturilor de pază şi măsurile de supraveghere a perimetrului protejat;
b) sistemul de control al accesului în zonele de securitate;
c) măsurile de avertizare şi alarmare pentru situaţii de urgenţă;
d) planul de evacuare a documentelor şi modul de acţiune în caz de urgenţă;

e) procedura de raportare, cercetare şi evidenţă a incidentelor de securitate.

Răspunderea pentru întocmirea, avizarea şi aplicarea *Programului de prevenire a scurgerii de informaţii clasificate* revine conducătorului unităţii deţinătoare.

Programul de prevenire a scurgerii de informaţii clasificate se actualizează, anual sau ori de câte ori se impune (identificarea unor noi riscuri şi vulnerabilităţi, apariţia unor noi situaţii sau acte normative), modificările efectuate aducându-se de fiecare dată la cunoştinţa SRI, unde se transmit sub formă de completare pentru a fi avizate.

Personalul inclus în sistemul de pază şi apărare a obiectivelor, sectoarelor şi locurilor în care sunt gestionate informaţii secrete de stat trebuie să deţină autorizaţie de acces corespunzător nivelului de secretizare a informaţiilor necesare îndeplinirii atribuţiilor ce îi revin. Pentru eficientizarea sistemelor de pază, în special în zonele de securitate unde, în interesul securităţii, personalul care asigură paza nu are acces, trebuie asigurate măsuri menite să detecteze eventualele încercări de pătrundere fără drept în aceste perimetre, prin folosirea unor modalităţi adecvate (televiziune cu circuit închis, sisteme de alarmă sau pentru inspectare vizuală).

În situaţia în care personalul care asigură paza unei entităţi deţinătoare de informaţii secrete de stat are atribuţii în ceea ce priveşte evacuarea unor astfel de informaţii şi pe cale de consecinţe angajaţii firmei de pază au acces în zone de securitate clasa I sau clasa a II-a este necesară încheierea unui **contract clasificat.**

De asemenea, este necesară încheierea unui contract clasificat şi în cazul în care unităţile deţinătoare de informaţii secrete de stat implementează măsurile protective prevăzute de legislaţia în domeniul protecţiei informaţiilor clasificate (în aceste cazuri angajaţii firmelor prestatoare vor avea acces în zonele de securitate ale unităţii deţinătoare de astfel de informaţii, iar proiectul pus la dispoziţia beneficiarului va include totalitatea măsurilor protective furnizate - detalii care sunt consemnate în *Planul de pază şi apărare a obiectivelor sectoarelor şi locurilor ce prezintă importanţă deosebită pentru protecţia informaţiilor clasificate* - document clasificat secret de stat, cu nivelul de secretizare corespunzător informaţiilor protejate).

Contractanţii şi **subcontractanţii** care intenţionează să se implice în activităţi contractuale clasificate sunt obligaţi să implementeze şi să respecte toate măsurile de protecţie a informaţiilor secrete de stat puse la dispoziţie sau care au fost generate pe timpul derulării respectivelor contracte clasificate.

*****

În acest sens, exemplificăm cazul unei autorităţi publice centrale care, în Fişa de date a anunţului de participare simplificat publicat în conformitate cu prevederile Legii nr. 98 din 23.05.2016 privind achiziţiile publice, la Capitolul "Prezentarea ofertei" a făcut menţiunea următoare: "având în vedere faptul că în cadrul instituţiei se gestionează informaţii secrete de stat, prestatorul are obligaţia obţinerii certificatului de securitate industrială ORNISS (nivel de secretizare "secret"), conform Standardelor naţionale, aprobate prin HG nr. 585/2002, iar agenţii de pază desemnaţi de prestator pentru a activa în cadrul contractorului trebuie să fie avizaţi de către ORNISS pentru accesul la informaţii clasificate (nivel de secretizare "secret")". Astfel, autoritatea contractantă a pus în vedere operatorilor economici încă din faza incipientă a procedurii de achiziţie publică necesitatea întreprinderii demersurilor legale în domeniul securităţii industriale.

*****

Pe parcursul unei inspecţii de securitate efectuate de SRI la un operator economic angrenat în derularea unui contract clasificat de achiziţie de servicii de pază şi intervenţie (beneficiar fiind o entitate care deţine informaţii secrete de stat, nivel maxim de secretizare "strict secret"), s-a constatat că acesta a subcontractat, pe o perioadă de un an, cu posibilitatea de prelungire pentru noi perioade de 12 luni, serviciile de intervenţie în obiective ale beneficiarului către o altă societate comercială, fără ca între părţi să fie încheiată o Anexă de securitate (obligaţie a operatorului economic ce a făcut obiectul inspecţiei de securitate prin raportare la dispoziţiile art. 201 din Standardele aprobate prin HG nr. 585/2002) şi fără ca al doilea agent economic să obţină certificatul de securitate industrială (în pofida faptului că în cuprinsul contractului încheiat între cei doi operatori economici era prevăzut acest aspect - întocmirea tuturor formalităţilor necesare pentru obţinerea autorizaţiilor ORNISS, pentru personalul ce lucrează în locaţiile (...), precum şi certificatul de securitate industrială, conform HG nr. 585/2002).

Contractul clasificat reprezintă orice contract încheiat între părţi, în condiţiile legii, în cadrul căruia se cuprind şi se vehiculează informaţii clasificate. Partea contractantă deţinătoare a informaţiilor clasificate ce vor fi accesate pe perioada derulării unui astfel de contract este responsabilă pentru clasificarea şi definirea tuturor componentelor acestuia, conform normelor în vigoare, sens în care poate solicita sprijin de la autoritatea desemnată de securitate, potrivit competenţelor materiale stabilite prin *Legea nr. 182/2002 privind protecţia informaţiilor clasificate.*

La clasificarea contractelor se aplică următoarele reguli:

a) în toate stadiile de planificare şi execuţie, contractul se clasifică pe niveluri corespunzătoare, în funcţie de conţinutul informaţiilor;

b) clasificările se aplică numai acelor părţi ale contractului care trebuie protejate;

c) când în derularea unui contract se folosesc informaţii din mai multe surse, cu niveluri de clasificare diferite, contractul va fi clasificat în funcţie de nivelul cel mai înalt al informaţiilor, iar măsurile de protecţie vor fi stabilite în mod corespunzător;

d) declasificarea sau trecerea la o altă clasă sau nivel de secretizare a unei informaţii din cadrul contractului se aprobă de conducătorul persoanei juridice care a autorizat clasificarea iniţială.

În cazul în care apare necesitatea protejării informaţiilor dintr-un contract care, anterior, nu a fost necesar a fi clasificat, contractorul are obligaţia declanşării procedurilor de clasificare şi protejare conform reglementarilor în vigoare.

*****

La nivelul unei autorităţi publice se află în derulare un contract privind implementarea unui "sistem integrat de securitate", încheiat cu un consorţiu format din mai mulţi operatori economici.

Obiectul contractului îl constituie proiectarea, furnizarea şi implementarea unui sistem integrat de securitate a unor obiective ce sunt desemnate infrastructuri critice naţionale în conformitate cu prevederile OUG nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice.

La data încheierii contractului nu au fost prevăzute clauze referitoare la respectarea dispoziţiilor legale în domeniul protecţiei infrastructurilor critice.

La sesizarea structurii de securitate a autorităţii publice, derularea contractului a fost stopată ulterior desemnării obiectivelor ca infrastructuri critice naţionale, întrucât a fost necesară elaborarea unor documentaţii ce conţin informaţii clasificate, nivel maxim "secret", circumscrise planurilor de securitate ale operatorilor de infrastructură critică prevăzute de OUG nr. 98/2010.

În context, au fost aplicate dispoziţiile art. 204 din Standardele aprobate prin HG nr. 585/2002, potrivit cărora în cazul în care apare nevoia de protejare a informaţiilor dintr-un contract care anterior nu a fost clasificat, contractorul are obligaţia declanşării procedurilor de clasificare şi protejare conform legii. De asemenea, au fost stabilite clauze şi proceduri de protecţie care au fost cuprinse în anexa de securitate şi s-a pus în vedere operatorilor economici care alcătuiesc consorţiul necesitatea obţinerii certificatelor de securitate industrială în vederea continuării relaţiei contractuale.

*****

O autoritate publică a încheiat cu un operator economic un ***Acord-cadru*** *(cu perioada de valabilitate de patru ani) şi patru* ***contracte subsecvente*** *(pentru fiecare an în parte un contract subsecvent) pe parcursul cărora au fost vehiculate informaţii secrete de stat, nivel "secret". Deşi operatorul economic a solicitat şi obţinut eliberarea certificatului de securitate industrială pentru punerea în executare a Acordului-cadru, contractele subsecvente au fost puse în executare fără ca ORNISS să fi eliberat certificatele de securitate industrială aferente fiecărui contract clasificat în parte.*

Clauzele şi procedurile de protecţie a informaţiilor secrete de stat ce fac obiectul activităţii contractuale trebuie stipulate în Anexa de securitate aferentă fiecărui contract clasificat.

Anexa de securitate se întocmeşte de către partea contractantă deţinătoare a informaţiilor secrete de stat ce vor fi utilizate în derularea contractului clasificat şi cuprinde clauzele şi procedurile de protecţie ce trebuie respectate de contractant pe perioada de derulare a acestuia. Aceste prevederi contractuale vor fi supuse, periodic, inspecţiilor şi verificărilor de către autoritatea desemnată de securitate competentă.

Cu titlu de exemplu enumerăm cerinţe necesar a fi prevăzute în Anexa de securitate a unui contract clasificat:

- menţionarea datelor de identificare ale părţilor contractante;
- prezentarea listei cu informaţiile clasificate aferente contactului, listei obiectivelor, sectoarelor şi locurilor în care se gestionează/accesează informaţii clasificate sau se desfăşoară activităţi ce presupun accesul la astfel de informaţii, precum şi a listei angajaţilor contractantului, care sunt autorizaţi pentru accesul la informaţii clasificate;
- enunţarea unor clauze care să cuprindă măsurile de securitate efective, cum ar fi:
  - modalitatea de transmitere, transport şi stocare a documentelor şi materialelor ce conţin informaţii secrete de stat;
  - condiţiile privind subcontractarea în sensul asigurării că subcontractantul deţine autorizaţie sau certificat de securitate industrială şi obligaţia de înştiinţare a contractorului;
  - modul în care se pot copia sau multiplica documentele sau materialele clasificate ce sunt încredinţate de către emitent, cu excepţia cazurilor în care este necesară aprobarea expresă a contractorului;
  - obligaţia contractantului să înapoieze toate informaţiile clasificate ce i-au fost încredinţate, precum şi pe cele generate pe timpul derulării contractului, cu excepţia cazului în care asemenea informaţii au fost distruse autorizat sau păstrarea lor a fost autorizată de către contractor pentru o perioadă de timp strict determinată;
  - obligaţia contractantului de a comunica ORNISS toate modificările survenite privind datele de securitate incluse în chestionarul completat, pe întreaga durată de valabilitate a autorizaţiei sau certificatului de securitate industrială.

Pentru participarea la negocierea, respectiv la derularea unui contract clasificat, conducătorul operatorului economic transmite ORNISS o cerere pentru eliberarea autorizaţiei/certificatului de securitate industrială**.**

Autorizaţia de securitate industrială are valabilitate până la încheierea contractului sau până la retragerea de la negocieri.

Contractul clasificat va putea fi pus în executare numai în condiţiile în care:

- ORNISS a emis certificatul de securitate industrială;
- au fost eliberate certificate de securitate sau autorizaţii de acces pentru persoanele care, în îndeplinirea sarcinilor ce le revin, necesită acces la informaţii secrete de stat;
- personalul autorizat al contractantului a fost instruit asupra reglementărilor de securitate industrială de către structura/funcţionarul de securitate şi a semnat fişa individuală de pregătire.

Termenul de valabilitate a certificatului de securitate industrială este determinat de perioada derulării contractului clasificat, dar nu mai mult de trei ani, după care contractantul este obligat să solicite revalidarea acestuia.

***** ***** ***** **** **** ****

Activităţile de evidenţă, întocmire, păstrare, procesare, manipulare şi multiplicare a documentelor clasificate se realizează în cadrul **compartimentelor speciale**, subordonate conducătorului unităţii ce gestionează astfel de documente.

Redactarea documentelor clasificate presupune respectarea următoarelor reguli:

- menţionarea, în antet, a unităţii emitente, a numărului şi datei înregistrării, a clasei sau nivelului de secretizare, a numărului de exemplare şi, după caz, a destinatarului;
- numerele de înregistrare se înscriu pe toate exemplarele documentului şi pe anexele acestora, fiind precedate de un zero (0) pentru documentele de nivel "secret", de două zerouri (00) pentru cele de nivel "strict secret", de trei zerouri (000) pentru cele "strict secret de importanţă deosebită" şi de litera "S" pentru secrete de serviciu;
- la sfârşitul documentului se înscriu în clar, după caz, rangul, funcţia, numele şi prenumele conducătorului unităţii emitente, precum şi ale celui care îl întocmeşte, urmate de semnăturile acestora şi ştampila unităţii;
- înscrierea, pe fiecare pagina a documentului, a clasei sau nivelului de secretizare atribuit acestuia;
- pe fiecare pagină a documentelor ce conţin informaţii clasificate se înscrie numărul curent al paginii, urmat de numărul total al acestora.

Documentele clasificate vor fi marcate, inscripţionate şi gestionate numai de către persoane care deţin autorizaţie sau certificat de securitate corespunzător nivelului de clasificare a acestora.

Toate documentele care conţin informaţii clasificate, indiferent de formă au înscrise, pe fiecare pagină, nivelul de secretizare.

Nivelul de secretizare se marchează prin ştampilare, dactilografiere, tipărire sau ograf, astfel:

a) în partea dreaptă sus şi jos, pe exteriorul copertelor, pe pagina cu titlul şi pe prima pagina a documentului;

b) în partea de jos şi de sus, la mijlocul paginii, pe toate celelalte pagini ale documentului;

c) sub legendă, titlu sau scara de reprezentare şi în exterior - pe verso - atunci când acestea sunt pliate, pe toate schemele, diagramele, hărţile, desenele şi alte asemenea documente.

Documentele clasificate secrete de stat pot fi procesate/stocate **exclusiv pe sisteme informatice acreditate de către ORNISS,** în condiţiile legii, în caz contrar, acestea se vor redacta olograf sau prin folosirea unei maşini de scris mecanice.

Toate documentele clasificate aflate în lucru sau în stadiu de proiect vor avea înscrise menţiunile "*Document în lucru*" sau "*Proiect*" şi vor fi marcate potrivit clasei sau nivelului de secretizare a informaţiilor ce le conţin. Gestionarea documentelor clasificate aflate în lucru sau în stadiu de proiect se face în aceleaşi condiţii ca şi a celor în forma definitivă.

Multiplicarea documentelor 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 atât pe original, cât şi pe toate copiile rezultate. Pe documentul original marcarea se aplică în partea dreaptă jos a ultimei pagini.
Pe copiile rezultate, marcarea se aplică pe prima pagina, sub numărul de înregistrare. În cazul copierii succesive, la date diferite, a unui document clasificat, documentul original va fi marcat la fiecare operaţiune, ce va fi, de asemenea, înscrisă în registru. Exemplarele rezultate în urma copierii se numerotează în ordine succesivă, chiar dacă operaţiunea se efectuează de mai multe ori şi la date diferite.

Transmiterea informaţiilor secrete de stat se realizează cu aprobarea emitentului şi cu respectarea principiului *"necesităţii de a cunoaşte"* - către destinatarul extern: **numai dacă reprezentantul destinatarului este autorizat corespunzător pentru acces la astfel de informaţii.**

Distrugerea documentelor clasificate se realizează de către emitenţi, în funcţie de clasa / nivelul de secretizare, pe bază de proces-verbal şi se menţionează în Registrul de evidenţă, prin consemnarea numărului de înregistrare al procesului-verbal de distrugere. 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.

Transportul documentelor clasificate pe teritoriul României se realizează de unitatea specializată a SRI, potrivit normelor stabilite prin HG nr. 1349/2002. Conducătorii instituţiilor deţinătoare de informaţii secrete de stat au obligaţia să desemneze cel puţin un delegat împuternicit pentru transportul şi executarea operaţiunilor de predare-primire a corespondenţei clasificate, în punctele de colectare-distribuire (art. 9 din HG nr. 1349/2002).

*****

Pe parcursul unei activităţi realizate de SRI în aplicarea prevederilor art. 34, lit. e) din Legea nr. 182/2002 privind protecţia informaţiilor clasificate[1] la un minister s-a constatat că:

- au fost organizate exclusiv zone de securitate clasa I şi zone administrative, însă în cadrul instituţiei existau angajaţi autorizaţi pentru accesul la informaţii secrete de stat, nivel "secret" (în conformitate cu dispoziţiile art. 98 din Standardele naţionale, aprobate prin HG nr. 585/2002 - "zona de securitate clasa I presupune că orice persoană aflată în interiorul acesteia are acces la informaţii secrete de stat, de nivel strict secret de importanţă deosebită şi strict secret");

- predarea-primirea corespondenţei clasificate se efectua într-o locaţie care nu era organizată zonă de securitate sau administrativă.

Aspecte problematice privind transportul corespondenţei clasificate şi oficiale neclasificate:

1. Nerespectarea regulilor privind inscripţionarea corespondenţei:

- scris ilizibil ce face imposibilă identificarea destinatarului;
- neinscripţionarea expeditorului care, coroborat cu lipsa ştampilelor sau sigiliilor, face imposibilă returnarea / trimiterea la destinatar;
- menţionarea destinatarului prin prescurtări sau iniţiale (ex. ANI, care are mai multe semnificaţii);
- neconcordanţe între denumirea şi adresa destinatarului, de natură a face imposibilă identificarea sa;
- trimiteri adresate către o localitate, fără a preciza instituţia destinatară;
- trimiteri către destinatari fără precizarea judeţului (apar probleme de dirijare, întrucât există localităţi cu aceeaşi denumire în judeţe diferite);
- inscripţionarea unor indicative alfa - numerice la destinatar (UM 02245, UT 365, UAT Griviţa) fără precizări explicite referitoare la denumirea completă şi adresa exactă ale acestuia.

*****

La o instituţie publică trimiterile expediate sunt completate olograf, scrisul ilizibil creând dificultăţi în identificarea destinatarului.

O agenţie guvernamentală nu inscripţionează trimiterile cu datele expeditorului, fapt care coroborat cu lipsa ştampilelor face imposibilă returnarea către destinatar.

La nivelul mai multor ministere au fost identificate nenumărate cazuri de menţionare a destinatarului prin prescurtări sau iniţiale, situaţii potenţial generatoare de confuzii cu privire la beneficiarul final.

*****

La un minister, persoanele abilitate să efectueze schimbul de corespondenţă cu reprezentanţii unităţii specializate SRI sunt permanent instruite şi coordonate, fapt ce se reflectă în calitatea cooperării, eficienţă şi operativitate.

2. Ambalare, greutate şi volumetrie:

---

[1] *În vederea coordonării activităţii şi exercitării controlului asupra măsurilor privitoare la protecţia informaţiilor clasificate din sfera sa de competenţă, Serviciul Român de Informaţii realizează, la faţa locului, verificări şi revizuiri de* Programe care vizează protecţia informaţiilor clasificate

- ambalare neconformă (ambalaj de proastă calitate/neadaptat conţinutului, de natură de a se deteriora la transport);

- nerespectarea regulilor de asigurare a corespondenţei cu greutate mai mare;

- ştampilarea şi sigilarea tuturor trimiterilor;

- nerespectarea regulilor privind greutatea maximă a trimiterilor / volumul maxim per trimitere;

- în situaţia expedierii de mai multe trimiteri către acelaşi destinatar, acestea vor fi ambalate şi înregistrate ca o singură trimitere, cu borderou de expediţie în interiorul trimiterii;

- trimiterile care conţin substanţe/materiale supuse unui regim special de transport şi/sau care emană mirosuri sau pot prezenta scurgeri nu se acceptă la transport decât cu aprobarea şefului unităţii specializate şi numai după ambalarea corespunzătoare, în prezenţa şefului echipei de curieri (aprobarea se acordă pentru acceptarea în sistem a trimiterii ambalate în conformitate cu cerinţele legale şi nu presupune obligativitatea acceptării ei de către şeful echipei de curieri în lipsa respectării condiţiilor de ambalare / securizare);

- anunţarea cu cel puţin o zi înainte a necesităţii de transport a unui volum mare de corespondenţă, peste media cotidiană/expeditor (pentru volum mare de corespondenţă neclasificată, unitatea specializată pune la dispoziţia expeditorilor servicii de registratură zilnic între orele 07.00-19.00, excepţie vineri 07.00-16.00, la **sediul din str. Hrisovului nr. 18A, sector 1**, cu anunţarea telefonică prealabilă).

3. Respectarea normelor legale şi procedurale privind predarea-primirea corespondenţei:

- transmiterea actualizărilor referitoare la datele din cererea de includere în sistem ori de câte ori apar modificări;

- actualizarea permanentă a delegaţiilor de predare-primire corespondenţă pentru persoanele desemnate (înlocuire delegaţi, expirare autorizaţii/certificate de securitate, modificare nivel de acces, schimbare punct de lucru/încăpere predare-primire, etc);

- menţinerea permanentă a standardelor de securitate stabilite la includerea în sistem, astfel încât să nu fie necesară suspendarea temporară a serviciilor, până la remediere.

4. Solicitările de transport în regim de urgenţă:

- iniţial, HG 1349/2002 a fost destinată exclusiv corespondenţei clasificate, însă prin HG 172/2004 prevederile au fost extinse şi către corespondenţa oficială neclasificată. Prevederile referitoare la transportul în regim de urgenţă se referă, în mod direct, la corespondenţa clasificată, pentru care instituţiile beneficiare ale sistemului nu au competenţe de transport. Transportul corespondenţei neclasificate urgente către destinatari din aceeaşi localitate / acelaşi judeţ se poate realiza de către reprezentanţii expeditorului sau destinatarului, după caz. În ceea ce priveşte transportul pe trasee interjudeţene al acestui tip de corespondenţă, unitatea specializată răspunde solicitărilor în cazuri întemeiate (în special solicitări venite dinspre instituţiile cu atribuţii în justiţie şi domeniul aplicării legii). De asemenea, unitatea specializată permite utilizarea serviciilor de registratură pentru trimiteri neclasificate, expediate în afara graficului normal de lucru;

- pentru urgenţele solicitate în afara programului normal de lucru (după orele 16.00) expeditorul are obligaţia de a se asigura că la destinatar există un delegat care să preia corespondenţa, unitatea specializată confruntându-se cu multiple cazuri de "lipsă destinatar" pentru astfel de solicitări.

5. Sunt interzise la transport prin sistemul organizat de SRI: felicitările de orice natură; ziare, reviste, broşuri, etc..