
SECURITATEA INDUSTRIALĂ

EMSAPHIR - EXPERTIZĂ ÎN PROTECȚIA DATELOR PERSONALE ȘI SECURITATEA INFORMAȚIILOR

Cuprins

1. Abordări conceptuale

2. Împuterniciri și verificări de securitate industrială

3. Autorizarea de securitate industrială UE



ABORDĂRI CONCEPTUALE

Securitatea industrială se referă la protecția informațiilor clasificate care fac obiectul contractelor industriale secrete, prevederile actului normativ aplicându-se tuturor persoanelor juridice de drept public sau privat care își desfășoară ori solicită să desfășoare activități contractuale ce presupun accesul la informații clasificate.



Securitatea industrială reprezintă:

- ◎ **ansamblul măsurilor și procedurilor de protecție a informațiilor clasificate aplicabile obiectivelor industriale care desfășoară sau urmează să desfășoare activități contractuale ce implică accesul la astfel de informații, în scopul prevenirii pierderii, compromiterii sau divulgării neautorizate, precum și identificării celor compromise și reducerii pierderilor ²;**
 - ◎ **ansamblul normelor de protecție a informațiilor clasificate vehiculate în domeniul industrial, în legătură cu licitarea, negocierea sau derularea unor contracte cu caracter clasificat ³;**
 - ◎ **protecția informațiilor clasificate la agenții economici cu capital integral sau parțial de stat și celelalte persoane juridice de drept public ori privat, care participă la negocierea sau derularea de contracte clasificate, atribuțiile de coordonare generală și control al măsurilor privitoare la acestea fiind exercitate de către Serviciul Român de Informații prin unitatea sa specializată - Oficiul pentru Supravegherea Secretelor de Stat ⁴;**
-

Securitatea industrială reprezintă:

- ◎ aplicarea de măsuri în vederea asigurării protecției IUEC de către contractanți și subcontractanți în cursul negocierilor anterioare încheierii contractelor și pe toată durata contractelor clasificate. Astfel de contracte nu implică accesul la informații clasificate TRÈS SECRET UE/EU TOP SECRET ⁵;
 - ◎ conceptul definit de politicile, directivele și reglementările de securitate NATO, transpus și în legislația națională în domeniu ⁶, aplicat obiectivelor industriale (sedii, puncte de lucru ale operatorilor economici) care desfășoară sau urmează să desfășoare activități contractuale care implică accesul la informații NATO clasificate de nivel NATO CONFIDENTIAL sau superior
-



DEFINIȚII

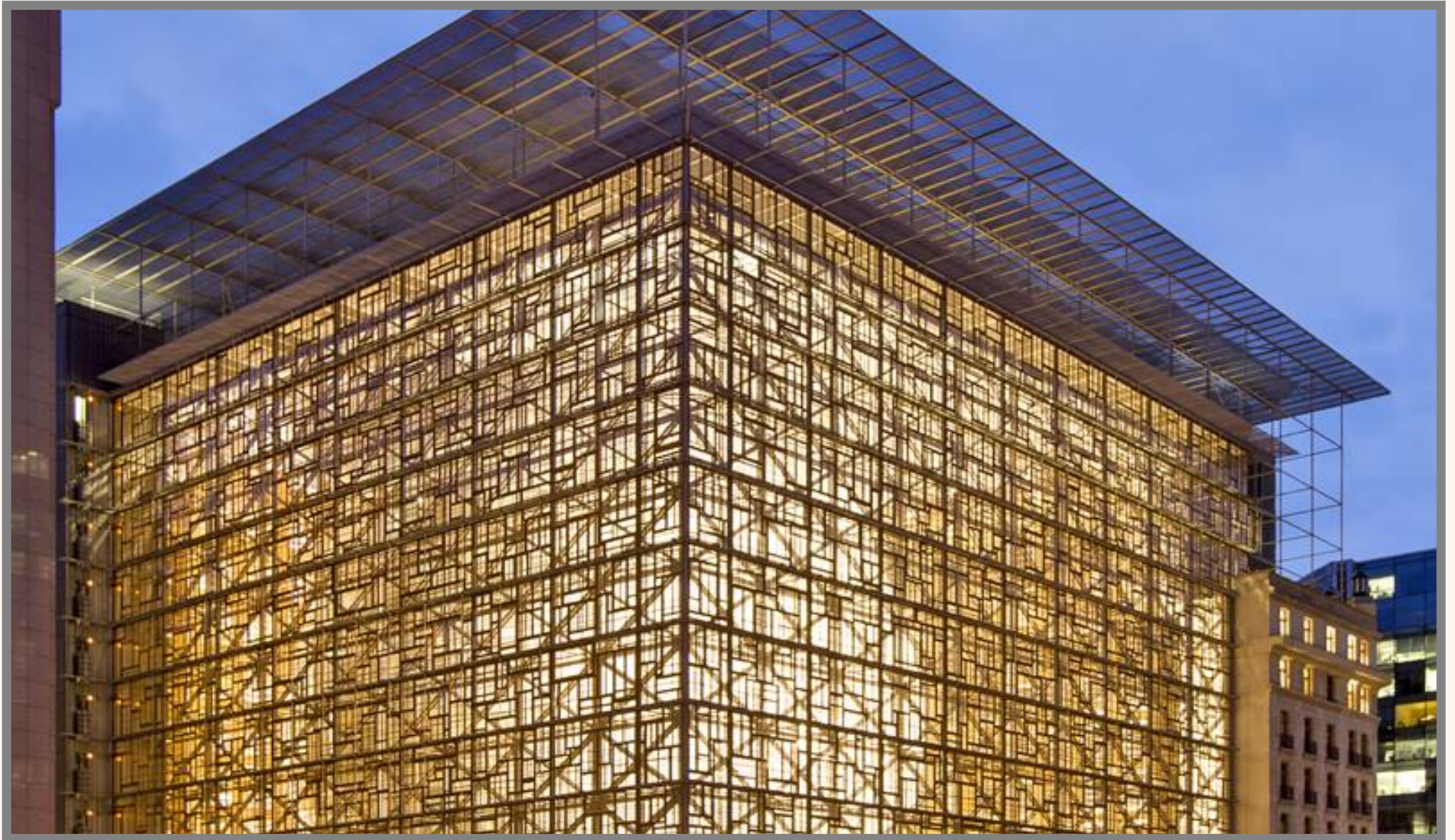
HG nr.585/2002:

- ❖ **securitate industrială** - sistemul de norme și măsuri care reglementează protecția informațiilor clasificate în domeniul activităților contractuale;
 - ❖ **obiectiv industrial** - unitate de cercetare sau cu activitate de producție, care desfășoară activități științifice, tehnologice sau economice ce au legătură cu siguranța sau cu apărarea națională, ori prezintă importanță deosebită pentru interesele economice și tehnico-științifice ale României;
 - ❖ **autorizație de securitate industrială** - document eliberat de Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS - unui obiectiv industrial, prin care se atestă că este abilitat să participe la procedura de negociere a unui contract clasificat;
 - ❖ **aviz de securitate industrială** - document eliberat de către ADS prin care se atestă că obiectivul industrial contractant a implementat toate măsurile de securitate necesare protecției informațiilor clasificate vehiculate în derularea contractului încheiat;
-

DEFINIȚII

HG nr.585/2002:

- ❖ **certificat de securitate industrială** - document eliberat de ORNISS unui obiectiv industrial, prin care se atestă că este abilitat să deruleze activități industriale și/sau de cercetare ce presupun accesul la informații clasificate;
 - ❖ **contractant** - unitate industrială, comercială, de execuție, de cercetare-proiectare sau prestatoare de servicii în cadrul unui contract clasificat;
 - ❖ **contractor** - parte dintr-un contract clasificat, care are calitatea de beneficiar al lucrărilor sau serviciilor executate de contractant;
 - ❖ **subcontractant** - parte care își asumă executarea unei părți a contractului clasificat sub coordonarea contractantului;
 - ❖ **negocieri** - activitățile circumscrise adjudecării unui contract sau subcontract, de la notificarea intenției de organizare a licitației, până la încheierea acesteia;
-



DEFINIȚII

Decizia Consiliului 2013/488/UE:

- ❖ **contract clasificat** - înseamnă un contract încheiat de Secretariatul general al Consiliului (SGC) cu un contractant pentru livrarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la IUEC sau crearea acestora;
 - ❖ **subcontract clasificat** - înseamnă un contract încheiat de un contractant al SGC cu un alt contractant (respectiv, subcontractantul) pentru livrarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la informații UE clasificate (IUEC) sau crearea acestora;
 - ❖ **contractant** - înseamnă o persoană fizică sau juridică având capacitatea juridică de a încheia contracte;
-

DEFINIȚII

Decizia Consiliului 2013/488/UE:

- ❖ **autorizare de securitate industrială (ASI)** înseamnă o decizie administrativă a Autorității Naționale de Securitate (ANS) sau Autorității Desemnate de Securitate (ADS) conform căreia, în ceea ce privește securitatea, un obiectiv poate oferi un nivel de protecție adecvat IUEC clasificate cu un anumit nivel de clasificare a securității;
 - ❖ **anexa de securitate (AS)** înseamnă un set de condiții contractuale speciale, emis de autoritatea contractantă, care este parte integrantă din orice contract clasificat care implică accesul la IUEC sau crearea de IUEC și care identifică cerințele de securitate sau elementele din cadrul contractului care necesită protecție de securitate;
 - ❖ **ghidul clasificărilor de securitate (GCS)** înseamnă un document care descrie elementele unui program sau ale unui contract clasificat, precizând nivelurile aplicabile de protecție a informațiilor. GCS poate fi extins pe toată durata programului sau a contractului respectiv, iar informațiile pot fi reclasificate sau le poate fi redus nivelul de clasificare; în cazul în care există un GCS, acesta face parte din AS.
-



DEFINIȚII

NATO:

- ❖ **contract NATO clasificat** - orice contract încheiat de o instituție militară sau civilă NATO sau de o țară membră NATO în vederea realizării unui program/proiect inițiat, negociat sau administrat de NATO și care necesită acces sau generează informații NATO clasificate;
 - ❖ **certificatul de securitate industrială NATO** se eliberează atât pentru negocierea, cât și pentru derularea contractelor NATO clasificate;
 - ❖ **certificare de securitate** - ORNISS inițiază, coordonează și participă la verificările de securitate asupra obiectivelor industriale implicate în activități contractuale clasificate NATO;
 - ❖ **norme de securitate industrială NATO** - măsurile pentru protecția informațiilor clasificate NATO care trebuie aplicate într-un contract sau subcontracta clasificat NATO ⁷;
-

DEFINIȚII

NATO:

- ❖ **certificat de securitate industrială** - document eliberat la cererea unei autorități naționale de securitate dintr-un stat membru NATO pentru agenții economici sau personalul implicați în negocierea sau executarea unui contract ori subcontract clasificat NATO;
 - ❖ **agent economic care derulează un contract clasificat NATO** - firmă care trebuie să îndeplinească mai multe condiții, înainte de a primi informații clasificate NATO în cadrul unui contract clasificat NATO: să asigure măsuri de protecție a acestora; să dețină certificat de securitate pentru obiectivul industrial implicat în contract; personalul implicat în derularea contractului clasificat NATO - personal care trebuie să dețină certificat de securitate de nivel corespunzător nivelului de clasificare a informațiilor NATO la care au acces;
 - ❖ **structura de securitate/funcționar de securitate** - sunt desemnate în obiectivele implicate în derularea contractelor sau subcontractelor clasificate NATO, cu atribuții specifice tipului de contract derulat ⁸.
-

ÎMPUTERNICIRI ȘI VERIFICĂRI DE SECURITATE INDUSTRIALĂ

Atribuțiile autorităților desemnate de securitate, conform competenței legale:

- (a) **verificări de securitate** necesare acordării avizului de securitate industrială, pe care îl transmite la ORNISS în vederea eliberării ASI sau CSI;
- (b) **asistență de specialitate** obiectivelor industriale în vederea implementării standardelor de securitate în domeniul protecției informațiilor clasificate;
- (c) **pregătirea personalului** cu atribuții pe linia protecției informațiilor clasificate;
- (d) **verificări ale încălcărilor** ale reglementărilor de protecție, distrugeri, dispariții, dezvăluiri neautorizate de informații clasificate, furnizate sau produse în cadrul unui contract clasificat;
- (e) asigurarea desemnării **structurii/funcționarului de securitate** de către fiecare obiectiv industrial în vederea exercitării efective a atribuțiilor pe linia

protecției informațiilor clasificate, în cadrul contractelor clasificate;

- (f) monitorizarea modului de **asigurare a protecției informațiilor clasificate** în procesul de negociere și derulare a contractelor clasificate;
 - (g) **avizarea programelor de prevenire a scurgerii informațiilor clasificate (PPSIC)** din obiectivele industriale, anexelor de securitate ale contractelor clasificate și monitorizarea respectării prevederilor acestora;
 - (h) **controale de securitate** și informarea ORNISS asupra concluziilor rezultate;
 - (i) **soluționarea sesizărilor**, reclamațiilor și observațiilor referitoare la modul de aplicare și respectare a standardelor de protecție în cadrul contractelor clasificate, prin verificări și propuneri de soluționare adresate ORNISS (art. 200 din Standarde)
-

OBIECTIVELE ACTIVITĂȚII DE VERIFICARE PENTRU ELIBERAREA ASI ȘI CSI

- (a) prevenirea accesului persoanelor neautorizate la informații clasificate,
- (b) garantarea că informațiile clasificate sunt distribuite pe baza principiului necesității de a cunoaște;
- (c) identificarea persoanelor care pot pune în pericol protecția informațiilor clasificate și interzicerea accesului acestora la astfel de informații;
- (d) garantarea faptului că obiectivele industriale au capacitatea de a proteja informațiile clasificate în procesul de negociere, respectiv de derulare a contractului (art.217)



Obligațiile obiectivului industrial pentru eliberarea ASI și CSI:

- (a) să posede **program de prevenire a scurgerii de informații clasificate**, avizat conform reglementărilor în vigoare;
- (b) să fie **stabil din punct de vedere economic**:
 - (1) nu este în proces de lichidare;
 - (2) nu este în stare de faliment ori nu se află în procedura reorganizării judiciare sau a falimentului;
 - (3) nu este implicat într-un litigiu care îi afectează stabilitatea economică;
 - (4) își îndeplinește obligațiile financiare către stat, persoane fizice sau juridice (art. 219);
- (c) să nu fi înregistrat o greșeală de management cu implicații grave asupra stării de securitate a informațiilor clasificate

pe care le gestionează; sunt considerate **riscuri de securitate**:

- (1) derularea unor activități ce contravin intereselor de siguranță națională;
 - (2) relațiile cu persoane fizice sau juridice străine ce ar putea aduce prejudicii intereselor statului român;
 - (3) asociațiile, persoane fizice și juridice, care pot reprezenta factori de risc pentru interesele de stat ale României (art. 220);
- (d) să fi **respectat obligațiile de securitate** din cadrul contractelor clasificate derulate anterior;
 - (e) **personalul** implicat în derularea contractului să dețină autorizație/certificat de securitate de nivel egal celui al informațiilor din contractului clasificat (art. 218).
-



Avizul de securitate industrială, condiții

- (a) agentul economic nu prezintă riscuri de securitate;
- (b) sunt aplicate în mod corespunzător măsurile de securitate fizică și normele privind accesul persoanelor la informații clasificate;
- (c) obiectivul industrial este solvabil din punct de vedere financiar;
- (d) obiectivul industrial nu a fost și nu este implicat sub nici o formă în activitatea unor organizații, asociații, mișcări, grupări de persoane străine sau autohtone care au adoptat sau adoptă o politică de sprijinire sau aprobare a comiterii de acte de sabotaj, subversive sau teroriste (art. 223)

Verificări de securitate pentru eliberarea avizului necesar ASI

- (a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială (anexa nr. 25);
 - (b) verificarea modului de aplicare a prevederilor PPSIC;
 - (c) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie:
 - (a) asociați/acționari, administratori, persoanele din comitetul director și structura de securitate;
 - (b) persoane executive implicate în negocierea contractului clasificat;
 - (d) verificarea datelor minime referitoare la bonitatea și stabilitatea economică a obiectivului industrial (domeniu și obiect de activitate, statut juridic, acționari, garanții bancare)
-

Verificări de securitate pentru eliberarea avizului necesar CSI

I. Nivel secret:

- (a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială (anexa nr. 26);
- (b) 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 derularea contractului clasificat;
- (c) verificarea unor date minime referitoare la bonitatea și stabilitatea economică a obiectivului industrial - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare;
- (d) verificarea modului de implementare și de aplicare a normelor și măsurilor de securitate fizică, de securitate a personalului și a documentelor, prevăzute pentru nivelul secret.

II. Nivelurile strict secret și strict secret de importanță deosebită

- (a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 27;
 - (b) 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 derularea contractului clasificat, precum și a celor desemnate să participe la activitățile de negociere a acestuia;
 - (c) verificarea datelor și informațiilor detaliate referitoare la bonitatea și stabilitatea economică a agentului economic - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare - incluzând și aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
 - (d) verificarea existenței autorizării sistemului informatic și de comunicații propriu, pentru nivelurile strict secret, respectiv strict secret de importanță deosebită;
 - (e) verificarea modului de implementare și de aplicare a normelor și măsurilor de securitate fizică, de securitate a personalului și a documentelor, prevăzute pentru nivelurile strict secret, respectiv strict secret de importanță deosebită;
 - (f) discuții cu proprietarii, membrii consiliului director, funcționarii de securitate, angajații, în vederea clarificării datelor rezultate din chestionar, după caz.
-

ELIBERAREA ȘI TERMENELE ASI ȘI CSI

Condiții și termene

ORNISS **eliberează** și transmite sau nu operatorului economic ASI sau CSI în următoarele condiții:

- (a) în urma verificării de securitate se constată că sunt îndeplinite cerințele de securitate necesare asigurării protecției la nivelul de clasificare corespunzător informațiilor vehiculate în cadrul contractului clasificat;
- (b) dacă se constată că obiectivul industrial nu îndeplinește condițiile de securitate necesare, ORNISS nu eliberează ASI/CSI și informează obiectivul industrial în acest sens. ORNISS nu este obligat să prezinte motivele refuzului. Refuzul eliberării ASI/CSI va fi comunicat și la ADS care a efectuat verificările de securitate;
- (c) când sunt semnalate elemente care nu constituie riscuri, dar sunt relevante din punct de vedere al securității, în luarea deciziei de eliberare a ASI/CSI vor avea prioritate interesele de securitate (art.229).

Termenele pentru eliberarea ASI/CSI sunt:

- (1) pentru ASI - 60 de zile lucrătoare;
- (2) pentru CSI de nivel secret - 90 de zile lucrătoare;
- (3) pentru CSI de nivel strict secret - 120 de zile lucrătoare;
- (4) pentru CSI de nivel strict secret de importanță deosebită - 180 de zile lucrătoare.

ORNISS va elibera ASI/CSI ori, după caz, va comunica obiectivului industrial refuzul eliberării acestora, în termen de șapte zile lucrătoare de la primirea avizului de securitate de la ADS.

VALABILITATEA ȘI RETRAGEREA ASI ȘI CSI

Valabilitatea ASI/CSI:

- (1) ASI are valabilitate până la încheierea contractului sau până la retragerea de la negocieri;
- (2) contractantul este obligat să solicite la ORNISS eliberarea certificatului de securitate industrială, în condițiile în care contractul negociat este adjudecat
- (3) termenul de valabilitate al CSI nu poate fi mai mare de trei ani, după care contractantul este obligat să solicite revalidarea acestuia, sau este determinat de perioada derulării contractului clasificat.

Retragerea ASI/CSI:

ORNISS retrage ASI/CSI în următoarele cazuri:

- (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 certificare acordat inițial ².
-

AUTORIZAREA DE SECURITATE INDUSTRIALĂ UE

VERIFICAREA DE SECURITATE

Decizia Consiliului UE nr.2013/488

Autoritatea Națională de Securitate (ANS), Autoritatea Desemnată de Securitate (ADS) și oricare altă autoritate competentă din statele membre se asigură, în derularea contractelor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, în măsura permisă de actele cu putere de lege și reglementările **naționale**, că:

- (a) atât contractanții, cât și subcontractanții iau toate măsurile necesare pentru **protecția informațiilor UE clasificate (IUEC)** în cursul negocierilor premergătoare contractului, precum și pe parcursul executării contractelor clasificate;
 - (b) atât contractanții, cât și subcontractanții înregistrați în respectivul stat membru și care participă la contracte sau subcontracte necesitând accesul, în obiectivele lor, la informații clasificate, fie în cursul executării contractelor respective, fie în etapa precontractuală, trebuie **să dețină autorizare de securitate industrială (ASI)**, la nivelul de clasificare necesar.
 - (c) personalului contractantului sau al subcontractantului ale cărui atribuții pot necesita accesul la informații clasificate în scopul executării unui contract clasificat i se acordă o **autorizare de securitate a personalului (ASP)**.
-

AUTORIZAREA DE SECURITATE INDUSTRIALĂ

ASI se acordă de către ANS/ADS sau de către orice altă autoritate de securitate competentă a unui stat membru pentru a atesta că o entitate industrială sau de altă natură **poate proteja IUEC la nivelul de clasificare adecvat** în interiorul obiectivelor sale.

La **eliberarea** unei ASI, ANS sau ADS relevantă asigură cel puțin:

- (a) **evaluarea integrității** entității industriale sau de altă natură;
- (b) evaluarea regimului de proprietate, a controlului sau a potențialului de exersare a unei influențe necuvenite care ar putea fi considerată un **risc de securitate**;
- (c) verificarea faptului că entitatea industrială sau orice altă entitate a instituit un **sistem de securitate în incintă**, care include toate măsurile de securitate adecvate necesare pentru protecția informațiilor sau a materialelor clasificate, în conformitate cu cerințele prevăzute de prezenta decizie;
- (d) verificarea faptului că **statutul în ceea ce privește securitatea** a fost stabilit pentru personalul de conducere, proprietarii și angajații care necesită acces la informații clasificate, în conformitate cu cerințele prevăzute de prezenta decizie; și
- (e) verificarea faptului că entitatea industrială sau orice altă entitate a numit un **agent de securitate al obiectivului**, care este responsabil cu gestionarea acesteia în vederea aplicării obligațiilor de securitate în cadrul entității respective.

Retragerea ASI:

- de către ANS/ADS este temei suficient pentru SGC să înceteze un contract clasificat sau să excludă un ofertant din competiție.



CONTRACTE ȘI SUBCONTRACTE CLASIFICATE

Secretariatul General al Consiliului UE

Secretariatul General al Consiliului (SGC) este autoritate contractantă a UE pentru contracte clasificate.

Reguli aplicabile:

- (a) SGC notifică ANS/ADS corespunzătoare contractantului sau subcontractantului dispozițiile în materie de securitate ale contractului clasificat, după atribuire;
 - (b) SGC notifică de îndată ANS/ADS sau orice altă autoritate de securitate competentă a statului membru în care este înregistrat contractantul sau subcontractantul în cazul în care un astfel de contract încetează;
 - (c) contractantului sau subcontractantului i se solicită să înapoieze autorității contractante, la încheierea contractului sau subcontractului clasificat, orice IUEC pe care le deține;
 - (d) în cazul în care contractantul sau subcontractantul este autorizat să rețină IUEC după încheierea unui contract, confidențialitatea IUEC este protejată de către contractant sau subcontractant;
 - (e) condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta sunt menționate în procedura de ofertare și în contract;
 - (f) un contractant obține permisiunea SGC înainte de a subcontracta părți ale unui contract clasificat. Nu se atribuie subcontracte entităților industriale sau de altă natură înregistrate într-un stat care nu este membru al UE care nu a încheiat cu Uniunea un acord privind securitatea informațiilor.
 - (g) contractantul este responsabil pentru asigurarea faptului că toate activitățile de subcontractare sunt întreprinse în conformitate cu standardele minime prevăzute în prezenta decizie și nu furnizează IUEC unui subcontractant fără consimțământul prealabil scris al autorității contractante;
 - (h) vizitele personalului SGC, contractanților sau al subcontractanților care necesită acces la informații clasificate în incintele celeilalte părți sunt organizate în colaborare cu ANS/ADS, iar accesul se acordă pe baza unui ASP corespunzător și a respectării principiului necesității de a cunoaște¹⁰.
-

Note bibliografice

- ¹ Hotărârea Guvernului nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, în: Monitorul Oficial cu numărul 485 din data de 5 iulie 2002, disponibilă la: <https://legislatie.just.ro/Public/DetaliiDocument/37319> (accesat la: 15 martie 2024)
- ² Marius Petrescu, Anca-Gabriela Petrescu, Florentina-Raluca Bîlcan, Vasile-Adrian Cămărășan, *Managementul securității informațiilor, Note de curs*, Editura Bibliotheca, 2018, p.112
- ³ Vasile-Adrian Cămărășan, Anca-Gabriela Petrescu, Marius Petrescu, Florentina-Raluca Bîlcan, *Instrumente și mecanisme privind managementul informațiilor clasificate - de la teorie la practică*, Editura Bibliotheca, 2017, p.137
- ⁴ Constantin Raicu, *Protecția informațiilor clasificate*, Editura Academiei Naționale de Informații „Mihai Viteazul”, 2009, p.91
- ⁵ Decizia Consiliului Uniunii Europene din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (2013/488/UE), disponibilă la: <https://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX:32013D0488> (accesat la: 15 martie 2024)
- ⁶ Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS) nr.491 din 21 noiembrie 2003 pentru aprobarea Normelor metodologice privind protecția informațiilor clasificate în cadrul activităților contractuale NATO, publicat în Monitorul Oficial, nr.885 din 12 decembrie 2003,

disponibil la: <https://legislatie.just.ro/Public/DetaliiDocument/48386>; https://orniss.ro/ro/legislatie/pdf/ordine/securitate_industrial/O491_2003/Ordin_NATO_491_2003.pdf (accesate la: 15 martie 2024); Anexa cuprinzând Normele metodologice nu este publicată, fiind comunicată unităților și instituțiilor de drept public și privat îndreptățite

⁷ Marius Petrescu et al, *op.cit.*, pp.112-115

⁸ Hotărârea Guvernului nr. 353 din 15 aprilie 2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, publicată în Monitorul Oficial cu numărul 315 din data de 13 mai 2002, disponibilă la: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/35978>; https://orniss.ro/ro/legislatie/pdf/HG_353.pdf (accesate la: 15 martie 2024)

⁹ Hotărârea Guvernului nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, în: Monitorul Oficial cu numărul 485 din data de 5 iulie 2002, disponibilă la: <https://legislatie.just.ro/Public/DetaliiDocument/37319> (accesat la: 18 martie 2024)

¹⁰ Decizia Consiliului Uniunii Europene din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (2013/488/UE), disponibilă la: <https://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX:32013D0488> (accesat la: 18 martie 2024)

Credit foto: consilium.europa.eu; nato.int; orniss.ro

EMSAPHIR - EXPERTIZĂ
ÎN PROTECȚIA DATELOR
PERSONALE ȘI
SECURITATEA
INFORMAȚIILOR

DATE DE CONTACT

- **telefon: 0755 544 575**
- **e-mail: contact@emsaphir.ro**

