DECIZIA (UE) 2021/259 A COMISIEI

din 10 februarie 2021

de stabilire a normelor de punere în aplicare privind securitatea industrială în ceea ce privește granturile clasificate

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 249,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 106,

având în vedere Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 ([1]),

având în vedere Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei ([2]),

având în vedere Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate ([3]),

având în vedere Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene ([4]),

După consultarea Grupului de experți în materie de securitate al Comisiei, în conformitate cu articolul 41 alineatul (5) din Decizia (UE, Euratom) 2015/444,

întrucât:

(1) Articolele 41, 42, 47 și 48 din Decizia (UE, Euratom) 2015/444 prevăd că, în completarea și în sprijinul capitolului 6 din decizia menționată, urmează să fie stabilite dispoziții mai detaliate în normele de punere în aplicare privind securitatea industrială, reglementând aspecte precum atribuirea de acorduri de grant clasificate, autorizările de securitate industrială, autorizările de securitate a personalului, vizitele, precum și transmiterea și transportul informațiilor clasificate al Uniunii Europene („IUEC").

(2) Decizia (UE, Euratom) 2015/444 prevede că acordurile de grant clasificate trebuie puse în aplicare în strânsă cooperare cu autoritatea națională de securitate, autoritatea de securitate desemnată sau orice altă autoritate competentă a statului membru respectiv. Statele membre au convenit să se asigure că orice entitate din jurisdicția lor care poate primi sau genera informații clasificate care provin de la Comisie este autorizată în mod corespunzător din punctul de vedere al securității și poate asigura o protecție adecvată, echivalentă celei asigurate de normele de securitate ale Consiliului Uniunii Europene pentru protecția informațiilor UE clasificate care poartă un marcaj de clasificare corespunzător, astfel cum se prevede în Acordul între statele membre ale Uniunii Europene, reunite în cadrul Consiliului, privind protecția informațiilor clasificate schimbate în interesul Uniunii Europene (2011/C 202/05) ([5]).

([1]) JO L 193, 30.7.2018, p. 1.
([2]) JO L 72, 17.3.2015, p. 41.
([3]) JO L 72, 17.3.2015, p. 53.
([4]) JO L 6, 11.1.2017, p. 40.
([5]) JO C 202, 8.7.2011, p. 13.

(3) Consiliul, Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au convenit să asigure o consecvență maximă în aplicarea normelor de securitate privind protecția IUEC, ținând seama, în același timp, de nevoile lor instituționale și organizatorice specifice, în conformitate cu declarațiile atașate la procesul-verbal al reuniunii Consiliului în cadrul căreia a fost adoptată Decizia 2013/488/UE a Consiliului ([6]) privind normele de securitate pentru protecția informațiilor UE clasificate.

(4) Normele de punere în aplicare ale Comisiei privind securitatea industrială în ceea ce privește granturile clasificate ar trebui, prin urmare, să asigure, de asemenea, o consecvență maximă și să țină seama de Orientările privind securitatea industrială, aprobate de Comitetul de securitate al Consiliului la 13 decembrie 2016.

(5) La 4 mai 2016, Comisia a adoptat o decizie ([7]) prin care membrul Comisiei responsabil de aspectele de securitate era abilitat să adopte, în numele Comisiei și sub responsabilitatea acesteia, normele de punere în aplicare prevăzute la articolul 60 din Decizia (UE, Euratom) 2015/444,

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Obiectul și domeniul de aplicare

(1) Prezenta decizie stabilește normele de punere în aplicare privind securitatea industrială referitoare la granturile clasificate, în sensul Deciziei (UE, Euratom) 2015/444 și, în special, al capitolului 6 din decizia menționată.

(2) Prezenta decizie stabilește cerințe specifice pentru a asigura protecția informațiilor UE clasificate (IUEC) în procesul de publicare a cererilor de propuneri și în momentul acordării granturilor și al punerii în aplicare a acordurilor de grant clasificate încheiate de Comisia Europeană.

(3) Prezenta decizie se aplică granturilor care implică informații clasificate la următoarele niveluri:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

(4) Prezenta decizie se aplică fără a aduce atingere normelor specifice prevăzute în alte acte juridice, cum ar fi cele privind Programul european de dezvoltare industrială în domeniul apărării.

Articolul 2

Responsabilități în cadrul Comisiei

(1) Ca parte a responsabilităților ordonatorului de credite al autorității care acordă grantul, menționate în Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului, ordonatorul de credite se asigură că grantul clasificat este conform cu Decizia (UE, Euratom) 2015/444 și cu normele sale de punere în aplicare.

([6]) Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).

([7]) Decizia Comisiei din 4 mai 2016 privind o abilitare legată de securitate [C(2016) 2797 final].

(2) În acest scop, ordonatorul de credite vizat trebuie să solicite, în toate etapele, consultanță din partea Autorității de securitate a Comisiei cu privire la aspecte legate de elementele de securitate ale unui acord de grant, program sau proiect clasificat și să îl informeze pe ofițerul local de securitate cu privire la acordurile de grant clasificate care au fost semnate. Decizia privind nivelul de clasificare a unor subiecte specifice revine autorității care acordă grantul și este luată ținând seama în mod corespunzător de ghidul clasificărilor de securitate.

(3) În cazul în care se aplică instrucțiunile privind securitatea programului sau a proiectului menționate la articolul 5 alineatul (3), autoritatea care acordă grantul și Autoritatea de securitate a Comisiei își îndeplinesc responsabilitățile care le-au fost atribuite în instrucțiunile respective.

(4) Pentru respectarea cerințelor prevăzute în prezentele norme de punere în aplicare, Autoritatea de securitate a Comisiei trebuie să coopereze îndeaproape cu autoritățile naționale de securitate („ANS") și cu autoritățile de securitate desemnate („ASD") din statele membre vizate, îndeosebi în ceea ce privește autorizările de securitate industrială („ASI"), autorizările de securitate a personalului („ASP"), procedurile privind vizitele și planurile de transport.

(5) În cazul în care granturile sunt gestionate de agenții executive ale UE sau de alte organisme de finanțare, iar normele specifice prevăzute în alte acte juridice menționate la articolul 1 alineatul (4) nu se aplică:

(a) departamentul Comisiei care deleagă este cel care exercită drepturile referitoare la emitentul IUEC generate în contextul granturilor, în cazul în care acordurile de delegare prevăd acest lucru;

(b) departamentul Comisiei care deleagă este cel care deține responsabilitatea stabilirii clasificării de securitate;

(c) cererile de informații privind autorizările de securitate și notificările către ANS și/sau ASD se transmit prin intermediul Autorității de securitate a Comisiei.

CAPITOLUL 2

GESTIONAREA CERERILOR DE PROPUNERI PENTRU GRANTURILE CLASIFICATE

Articolul 3

Principii de bază

(1) Părțile clasificate ale granturilor sunt puse în aplicare numai de beneficiari înregistrați într-un stat membru sau de beneficiari înregistrați într-o țară terță ori înființați de o organizație internațională în cazul în care țara terță sau organizația internațională respectivă a încheiat un acord privind securitatea informațiilor cu Uniunea sau un acord administrativ cu Comisia ([8]).

(2) Înainte de lansarea unei cereri de propuneri pentru un contract clasificat, autoritatea care acordă grantul stabilește clasificarea de securitate a tuturor informațiilor care ar putea fi furnizate solicitanților. Autoritatea care acordă grantul stabilește, de asemenea, clasificarea de securitate maximă a oricărei informații utilizate sau generate în executarea acordului de grant, a programului sau a proiectului ori, cel puțin, volumul anticipat și tipul de informații care urmează să fie produse sau gestionate, precum și necesitatea unui sistem informatic și de comunicații (SIC) clasificat.

(3) Autoritatea care acordă grantul se asigură că cererile de propuneri pentru granturi clasificate furnizează informații privind obligațiile speciale în materie de securitate legate de informațiile clasificate. Documentația cererii de propuneri trebuie să includă clarificări cu privire la calendarul pentru obținerea de către beneficiari a ASI, în cazul în care acestea sunt necesare. Anexele I și II conțin modele de formulare pentru informațiile referitoare la condițiile cererilor de propuneri.

([8]) Lista acordurilor încheiate de UE și a acordurilor administrative încheiate de Comisia Europeană, pe baza cărora pot fi schimbate informații UE clasificate cu țări terțe și cu organizații internaționale, poate fi consultată pe site-ul Comisiei.

(4) Autoritatea care acordă grantul se asigură că informațiile clasificate RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET sunt transmise solicitanților numai după ce aceștia au semnat un acord de confidențialitate, care îi obligă să gestioneze și să protejeze IUEC în conformitate cu Decizia (UE, Euratom) 2015/444, cu normele sale de punere în aplicare și cu normele naționale aplicabile.

(5) În cazul în care solicitanților li se furnizează informații RESTREINT UE/EU RESTRICTED, cerințele minime menționate la articolul 5 alineatul (7) din prezenta decizie trebuie incluse în cererea de propuneri sau în acordurile de confidențialitate încheiate în faza de propunere.

(6) Toți solicitanții și beneficiarii care trebuie să gestioneze sau să stocheze informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele lor, fie în faza de propunere, fie pe perioada executării propriu-zise a acordului de grant clasificat, trebuie să dețină o ASI la nivelul necesar, cu excepția cazurilor menționate la alineatul (9). Mai jos sunt identificate cele trei scenarii care pot apărea în faza de propunere pentru un grant clasificat care implică IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET:

(a) Nu se acordă acces la IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în faza de propunere:

În cazul în care cererea de propuneri privește un contract care va implica IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, dar care nu prevede gestionarea de către solicitant a unor astfel de informații în faza de propunere, solicitantul care nu deține o ASI la nivelul necesar nu trebuie să fie exclus din procesul de propunere pe motivul că nu deține autorizarea respectivă.

(b) Accesul la IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele autorității care acordă grantul faza de propunere:

Se acordă acces personalului solicitantului care deține o ASP la nivelul necesar și care are nevoie să cunoască informațiile respective.

(c) Gestionarea sau stocarea IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele solicitantului în faza de propunere:

În cazul în care cererea de propuneri le impune solicitanților să gestioneze sau să stocheze IUEC în incintele lor, solicitanții trebuie să dețină o ASI la nivelul necesar. În astfel de circumstanțe, înainte ca solicitantului să i se furnizeze orice IUEC, autoritatea care acordă grantul trebuie să obțină, prin intermediul Autorității de securitate a Comisiei, o asigurare din partea ANS sau ASD relevante, potrivit căreia solicitantului i s-a acordat o ASI adecvată. Se acordă acces personalului solicitantului care deține o ASP la nivelul necesar și care are nevoie să cunoască informațiile respective.

(7) În principiu, nu se impune obținerea unei ASI sau a unei ASP pentru accesul la informații RESTREINT UE/EU RESTRICTED nici în faza de propunere, nici pentru executarea acordului de grant. În cazul în care statele membre solicită o ASI sau o ASP pentru acorduri de grant sau subcontracte la nivelul RESTREINT UE/EU RESTRICTED în conformitate cu actele cu putere de lege și normele administrative naționale, astfel cum sunt enumerate în anexa IV, cerințele naționale respective nu trebuie să creeze obligații suplimentare pentru alte state membre și nu trebuie să excludă de la acorduri de grant sau subcontracte conexe solicitanții, beneficiarii sau subcontractanții din state membre care nu au astfel de cerințe privind ASI sau ASP în legătură cu accesul la informații clasificate RESTREINT UE/EU RESTRICTED și nici să îi pună în concurență în acest sens. Aceste acorduri de grant trebuie să fie executate în statele membre în conformitate cu actele cu putere de lege și cu normele administrative naționale ale acestora.

(8) În cazul în care este necesară o ASI pentru gestionarea unei cereri de propuneri și pentru punerea în aplicare a unui acord de grant clasificat, autoritatea care acordă grantul transmite, prin intermediul Autorității de securitate a Comisiei, o cerere către ANS sau ASD a beneficiarului, utilizând o fișă de informații privind autorizarea de securitate industrială („FIASI") sau orice formular electronic echivalent stabilit. Apendicele D la anexa III conține un exemplu de FIASI ([9]). Răspunsul la o FIASI este furnizat, în măsura posibilului, în termen de 10 zile lucrătoare de la data solicitării.

(9) În cazul în care instituțiile guvernamentale ale statelor membre sau instituțiile statelor membre aflate sub controlul guvernului acestora participă la granturi clasificate care necesită ASI și în cazul în care nu se eliberează ASI pentru respectivele instituții în temeiul legislației naționale, autoritatea care acordă grantul verifică împreună cu ANS sau ASD în cauză, prin intermediul Autorității de securitate a Comisiei, dacă respectivele instituții guvernamentale sunt capabile să gestioneze IUEC la nivelul solicitat.

([9]) Alte formulare utilizate pot fi diferite – în ceea ce privește modul în care sunt concepute – de exemplul oferit în prezentele norme de punere în aplicare.

(10) În cazul în care este necesară o ASP pentru executarea unui acord de grant clasificat și în cazul în care, în conformitate cu normele naționale, este necesară o ASI înainte de acordarea unei ASP, autoritatea care acordă grantul verifică pe lângă ANS sau ASD a beneficiarului, prin intermediul Autorității de securitate a Comisiei, utilizând o FIASI, dacă beneficiarul deține o ASI sau dacă procesul de obținere a ASI este în desfășurare. În acest caz, Comisia nu emite cereri de ASP utilizând fișa de informații privind autorizarea de securitate a personalului („FIASP").

Articolul 4

Subcontractarea în cadrul granturilor clasificate

(1) Condițiile în care beneficiarii pot subcontracta sarcini care implică IUEC trebuie definite în cererea de propuneri și în acordul de grant. Aceste condiții includ cerința ca toate FIASI să fie transmise prin intermediul Autorității de securitate a Comisiei. Subcontractarea face obiectul unui acord prealabil scris din partea autorității care acordă grantul. După caz, subcontractarea trebuie să fie conformă cu actul de bază de instituire a programului.

(2) Părțile clasificate ale granturilor sunt subcontractate numai entităților înregistrate într-un stat membru sau entităților înregistrate într-o țară terță ori înființate de o organizație internațională în cazul în care țara terță sau organizația internațională respectivă a încheiat un acord privind securitatea informațiilor cu Uniunea sau un acord administrativ cu Comisia ([10]).

CAPITOLUL 3

GESTIONAREA GRANTURILOR CLASIFICATE

Articolul 5

Principii de bază

(1) La atribuirea unui grant clasificat, autoritatea care acordă grantul, împreună cu Autoritatea de securitate a Comisiei, se asigură că obligațiile beneficiarilor privind protecția IUEC utilizate sau generate în executarea acordului de grant fac parte integrantă din acordul de grant. Cerințele de securitate specifice grantului iau forma unei anexe de securitate („AS"). Un model de AS este prezentat în anexa III.

(2) Înainte de a semna un grant clasificat, autoritatea care acordă grantul aprobă un ghid al clasificărilor de securitate („GCS") pentru sarcinile care urmează să fie executate și informațiile generate în executarea grantului sau la nivel de program ori proiect, după caz. GCS face parte din AS.

(3) Cerințele de securitate specifice programului sau proiectului iau forma unor instrucțiuni de securitate pentru program (sau proiect) („ISP"). ISP pot fi elaborate pe baza dispozițiilor din modelul AS, astfel cum este prezentat în anexa III. ISP sunt elaborate de departamentul Comisiei care gestionează programul sau proiectul, în strânsă cooperare cu Autoritatea de securitate a Comisiei, și sunt transmise, în vederea acordării de consultanță, Grupului de experți în materie de securitate al Comisiei. În cazul în care un acord de grant face parte dintr-un program sau proiect cu propriile ISP, AS a acordului de grant trebuie să aibă o formă simplificată și să includă referințe la dispozițiile privind securitatea stabilite în ISP ale programului sau proiectului.

(4) Cu excepția cazurilor menționate la articolul 3 alineatul (9), acordul de grant clasificat nu se semnează până când ANS sau ASD a solicitantului nu confirmă ASI a solicitantului sau, în cazul în care acordul de grant clasificat este acordat unui consorțiu, până când ANS sau ASD a cel puțin unuia dintre solicitanți din cadrul consorțiului sau mai multora dintre aceștia, dacă este necesar, nu confirmă ASI a solicitantului respectiv.

(5) În principiu și cu excepția cazului în care se prevede altfel în alte norme relevante, autoritatea care acordă grantul este considerată emitentul IUEC generate în cursul executării acordului de grant.

([10]) Lista acordurilor încheiate de UE și a acordurilor administrative încheiate de Comisia Europeană, pe baza cărora pot fi schimbate informații UE clasificate cu țări terțe și cu organizații internaționale, poate fi consultată pe site-ul Comisiei.

(6) Autoritatea care acordă grantul notifică, prin intermediul Autorității de securitate a Comisiei, ANS și/sau ASD ale tuturor beneficiarilor și subcontractanților cu privire la semnarea acordurilor de grant sau a subcontractelor clasificate și la orice prelungire sau reziliere anticipată a respectivelor acorduri de grant ori subcontracte. O listă a cerințelor aferente fiecărei țări este furnizată în anexa IV.

(7) Acordurile de grant care implică informații clasificate RESTREINT UE/EU RESTRICTED trebuie să includă o clauză de securitate care să prevadă obligativitatea pentru beneficiari a dispozițiilor prevăzute în apendicele E la anexa III. Acordurile de grant respective trebuie să includă o AS care să prevadă, cel puțin, cerințele pentru gestionarea informațiilor RESTREINT UE/EU RESTRICTED, inclusiv aspectele legate de asigurarea informațiilor și cerințele specifice care trebuie îndeplinite de beneficiari în ceea ce privește acreditarea sistemului lor informatic și de comunicații (SIC) care gestionează informații RESTREINT UE/EU RESTRICTED.

(8) În cazul în care acest lucru este impus de actele cu putere de lege și normele administrative naționale ale statelor membre, ANS sau ASD se asigură că toți beneficiarii sau subcontractanții din jurisdicțiile lor respectă dispozițiile de securitate aplicabile pentru protecția informațiilor RESTREINT UE/EU RESTRICTED și efectuează vizite de verificare în clădirile beneficiarilor sau ale subcontractanților situate pe teritoriul lor. În cazul în care ANS sau ASD nu se află sub incidența unei astfel de obligații, autoritatea care acordă grantul trebuie să se asigure că beneficiarii pun în aplicare dispozițiile de securitate necesare, stabilite în apendicele E la anexa III.

Articolul 6

Accesul personalului beneficiarilor și al subcontractanților la IUEC

(1) Autoritatea care acordă grantul se asigură că acordurile de grant clasificate cuprind dispoziții care indică faptul că membrilor personalului beneficiarilor sau al subcontractanților care au nevoie de acces la IUEC pentru executarea acordului de grant sau a subcontractului clasificat li se poate acorda un astfel de acces numai dacă:

(a) s-a stabilit că este necesar ca aceștia să cunoască informațiile respective;

(b) pentru informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, acestora li s-a acordat o autorizare de securitate la nivelul relevant de către ANS sau ASD respectivă sau de orice altă autoritate de securitate competentă;

(c) aceștia au fost instruiți cu privire la normele de securitate aplicabile pentru protecția IUEC și au confirmat că au luat cunoștință de responsabilitățile care le revin în ceea ce privește protejarea acestor informații.

(2) După caz, accesul la IUEC trebuie să fie, de asemenea, conform cu actul de bază de instituire a programului și să țină seama de orice marcaje suplimentare definite în GCS.

(3) În cazul în care un beneficiar sau subcontractant dorește să angajeze un resortisant dintr-o țară din afara UE pe un post care necesită accesul la IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, beneficiarului sau subcontractantului respectiv îi revine responsabilitatea de a iniția procedura de acordare a autorizării de securitate pentru persoana în cauză, în conformitate cu actele cu putere de lege și normele administrative naționale aplicabile în locul în care urmează să fie acordat accesul la IUEC.

Articolul 7

Accesul la IUEC al experților care participă la verificări, revizuiri sau audituri

(1) În cazul în care persoane externe („experți”) sunt implicate în verificări, revizuiri sau audituri efectuate de autoritatea care acordă grantul sau în evaluări ale performanțelor beneficiarilor pentru care au nevoie de acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, acestor persoane li se furnizează un contract numai dacă au primit o autorizare de securitate la nivelul relevant din partea ANS sau ASD respective sau a oricărei alte autorități de securitate competente. Autoritatea care acordă grantul efectuează verificări, prin intermediul Autorității de securitate a Comisiei, și solicită, dacă este necesar, ANS sau ASD să inițieze procesul de verificare pentru experți cu cel puțin șase luni înainte de începerea contractelor acestora.

(2) Înainte de semnarea contractelor, experții trebuie să fie instruiți cu privire la normele de securitate aplicabile pentru protecția IUEC și să confirme că au luat cunoștință de responsabilitățile care le revin în ceea ce privește protejarea acestor informații.

CAPITOLUL 4

VIZITE LEGATE DE ACORDURILE DE GRANT CLASIFICATE

Articolul 8

Principii de bază

(1) În cazul în care autoritatea care acordă grantul, experții, beneficiarii sau subcontractanții au nevoie de acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele celeilalte părți în contextul punerii în aplicare a unui acord de grant clasificat, vizitele trebuie să fie organizate în colaborare cu ANS, cu ASD sau cu orice altă autoritate de securitate competentă implicată în proces.

(2) Vizitele menționate la alineatul (1) fac obiectul următoarelor cerințe:

(a) vizitele trebuie să aibă un scop oficial legat de grantul clasificat;

(b) orice vizitator trebuie să dețină o ASP la nivelul necesar și să aibă nevoie să cunoască informațiile respective pentru a avea acces la IUEC utilizate sau generate în executarea grantului clasificat.

Articolul 9

Cererile de vizită

(1) Vizitele efectuate de beneficiari sau subcontractanți în clădirile altor beneficiari sau subcontractanți sau în incintele autorității care acordă grantul care implică accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET trebuie să fie organizate în conformitate cu următoarea procedură:

(a) ofițerul de securitate al clădirii care trimite vizitatorul completează toate părțile relevante ale formularului de cerere de vizită și transmite cererea către ANS sau ASD a clădirii. Un model de formular de cerere de vizită este prezentat în apendicele C la anexa III;

(b) ANS sau ASD a clădirii care trimite vizitatorul trebuie să confirme ASP a vizitatorului înainte de a transmite cererea de vizită ANS sau ASD a clădirii-gazdă (sau Autorității de securitate a Comisiei în cazul în care vizita are loc în incintele unei autorități care acordă grantul);

(c) ofițerul de securitate al clădirii care trimite vizitatorul obține apoi de la propria ANS sau ASD răspunsul ANS sau al ASD a clădirii-gazdă (sau al Autorității de securitate a Comisiei), care fie autorizează, fie respinge cererea de vizită;

(d) o cerere de vizită este considerată aprobată în cazul în care nu sunt prezentate obiecțiuni până în momentul în care au mai rămas cinci zile lucrătoare până la data vizitei.

(2) Vizitele funcționarilor autorității care acordă grantul sau ale experților ori ale auditorilor în clădirile beneficiarilor sau ale subcontractanților care implică accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET trebuie să fie organizate în conformitate cu următoarea procedură:

(a) vizitatorul completează toate părțile relevante ale formularului de cerere de vizită și îl transmite Autorității de securitate a Comisiei;

(b) Autoritatea de securitate a Comisiei confirmă ASP a vizitatorului înainte de transmiterea cererii de vizită către ANS sau ASD a clădirii-gazdă;

(c) Autoritatea de securitate a Comisiei obține un răspuns din partea ANS sau a ASD a clădirii-gazdă prin care cererea de vizită este autorizată sau respinsă;

(d) o cerere de vizită este considerată aprobată în cazul în care nu sunt prezentate obiecțiuni până în momentul în care au mai rămas cinci zile lucrătoare până la data vizitei.

(3) O cerere de vizită poate acoperi fie o singură vizită, fie vizite recurente. În cazul vizitelor recurente, cererea de vizită poate fi valabilă timp de până la un an de la data de începere solicitată.

(4) Valabilitatea oricărei cereri de vizită nu trebuie să depășească valabilitatea ASP a vizitatorului.

(5) Ca regulă generală, ar trebui ca o cerere de vizită să fie transmisă autorității de securitate competente a clădirii-gazdă cu cel puțin 15 zile lucrătoare înainte de data vizitei.

Articolul 10

Procedurile privind vizitele

(1) Înainte de a le permite vizitatorilor accesul la IUEC, ofițerul de securitate al clădirii-gazdă trebuie să respecte toate procedurile și normele de securitate în legătură cu vizitele prevăzute de ANS sau ASD.

(2) La sosirea în clădirea-gazdă, vizitatorii fac dovada identității lor prin prezentarea unei cărți de identitate valabile sau a unui pașaport valabil. Informațiile de identificare trebuie să corespundă cu informațiile furnizate în cererea de vizită.

(3) Clădirea-gazdă asigură păstrarea evidenței tuturor vizitatorilor, inclusiv numele acestora, organizația pe care o reprezintă, data expirării ASP, data vizitei și numele persoanelor vizitate. Aceste evidențe sunt păstrate pe o perioadă de cel puțin cinci ani sau mai mult, în cazul în care normele și reglementările naționale din țara în care este situată clădirea-gazdă impun acest lucru.

Articolul 11

Vizite organizate direct

(1) În contextul unor proiecte specifice, ANS sau ASD relevante și Autoritatea de securitate a Comisiei pot conveni asupra unei proceduri prin care vizitele pentru un acord de grant clasificat specific să poată fi organizate direct de ofițerul de securitate al vizitatorului împreună cu ofițerul de securitate al clădirii care urmează să fie vizitată. Un model al formularului care trebuie folosit în acest scop este prezentat în apendicele C la anexa III. O astfel de procedură excepțională trebuie să fie stabilită în ISP sau în alte acorduri specifice. În aceste cazuri, procedurile prevăzute la articolul 9 și la articolul 10 alineatul (1) nu se aplică.

(2) Vizitele care implică accesul la informații clasificate RESTREINT UE/EU RESTRICTED trebuie să fie organizate direct de entitatea care trimite vizitatorul împreună cu entitatea care primește vizitatorul, fără a fi necesară parcurgerea procedurilor stabilite la articolul 9 și la articolul 10 alineatul (1).

CAPITOLUL 5

TRANSMITEREA ȘI TRANSPORTUL IUEC ÎN CADRUL EXECUTĂRII ACORDURILOR DE GRANT CLASIFICATE

Articolul 12

Principii de bază

Autoritatea care acordă grantul se asigură că toate deciziile legate de transferul și transportul IUEC respectă Decizia (UE, Euratom) 2015/444 și normele sale de punere în aplicare, precum și condițiile prevăzute în acordul de grant clasificat, inclusiv consimțământul emitentului.

Articolul 13

Gestionarea electronică

(1) Gestionarea și transmiterea electronică a IUEC au loc în conformitate cu capitolele 5 și 6 din Decizia (UE, Euratom) 2015/444 și cu normele sale de punere în aplicare.

Sistemele informatice și de comunicații deținute de un beneficiar și utilizate pentru gestionarea IUEC în scopul executării acordului de grant („SIC ale beneficiarului") trebuie să facă obiectul acreditării de către autoritatea de acreditare în materie de securitate („AAS") responsabilă. Orice transmitere electronică a IUEC trebuie să fie protejată prin intermediul unor produse criptografice aprobate în conformitate cu articolul 36 alineatul (4) din Decizia (UE, Euratom) 2015/444. Măsurile de securitate TEMPEST trebuie să fie puse în aplicare în conformitate cu articolul 36 alineatul (6) din decizia menționată.

(2) Acreditarea în materie de securitate a SIC ale beneficiarului care gestionează IUEC la nivel RESTREINT UE/EU RESTRICTED și orice interconexiune în acest sens pot fi delegate ofițerului de securitate al beneficiarului în cazul în care actele cu putere de lege și normele administrative naționale permit acest lucru. În cazul în care respectiva sarcină este delegată, beneficiarul este responsabil de punerea în aplicare a cerințelor de securitate minime descrise în anexa de securitate atunci când gestionează informații RESTREINT UE/EU RESTRICTED în cadrul sistemului său informatic și de comunicații. Totuși, ANS sau ASD relevante și AAS păstrează responsabilitatea pentru protecția informațiilor RESTREINT UE/EU RESTRICTED gestionate de beneficiar, precum și dreptul de a inspecta măsurile de securitate luate de acesta. În plus, beneficiarul oferă autorității care acordă grantul și, atunci când acest lucru este impus prin actele cu putere de lege și normele administrative naționale, AAS naționale competente, o declarație de conformitate care certifică faptul că SIC ale beneficiarului și interconexiunile aferente au fost acreditate pentru gestionarea IUEC la nivel RESTREINT UE/EU RESTRICTED ([11]).

Articolul 14

Transportul prin intermediul curierilor comerciali

Transportul IUEC prin intermediul curierilor comerciali trebuie să se desfășoare în conformitate cu dispozițiile relevante ale Deciziei (UE, Euratom) 2019/1962 a Comisiei ([12]) privind normele de punere în aplicare pentru gestionarea informațiilor RESTREINT UE/EU RESTRICTED și ale Deciziei (UE, Euratom) 2019/1961 a Comisiei ([13]) privind normele de punere în aplicare pentru gestionarea informațiilor CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET.

Articolul 15

Transportul personal

(1) Transportul personal al informațiilor clasificate trebuie să facă obiectul unor cerințe de securitate stricte.

(2) Informațiile RESTREINT UE/EU RESTRICTED pot fi transportate personal de membrii personalului beneficiarului în cadrul Uniunii, cu condiția îndeplinirii următoarelor cerințe:

(a) plicul sau ambalajul folosit să fie opac și să nu poarte nicio indicație privind clasificarea conținutului său;

(b) informațiile clasificate să nu iasă din posesia persoanei care le transportă;

(c) plicul sau ambalajul să nu fie deschis pe drum.

(3) În cazul informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET, transportul personal de către membrii personalului beneficiarului în cadrul unui stat membru este organizat în prealabil de către entitățile expeditoare împreună cu entitățile destinatare. Autoritatea sau clădirea expeditoare informează autoritatea sau clădirea destinatară cu privire la detaliile transportului, inclusiv referința, clasificarea, ora estimată a sosirii și numele curierului. Transportul personal de acest tip este permis cu condiția îndeplinirii următoarelor cerințe:

(a) informațiile clasificate să fie transportate într-un plic sau ambalaj dublu;

(b) plicul sau ambalajul exterior să fie securizat și să nu poarte nicio indicație a clasificării conținutului său, iar plicul interior să poarte indicația nivelului de clasificare;

(c) IUEC să nu iasă din posesia persoanei care le transportă;

(d) plicul sau ambalajul să nu fie deschis pe drum;

(e) plicul sau ambalajul să fie transportat într-o servietă care poate fi încuiată sau într-un recipient similar aprobat, având o dimensiune și greutate care îi permit persoanei care efectuează transportul să o (îl) păstreze în permanență asupra sa și să nu o (îl) depoziteze într-un spațiu pentru bagaje;

(f) curierul să dețină un certificat de curier eliberat de autoritatea sa de securitate competentă, prin care este autorizat să transporte pachetul clasificat astfel cum este identificat.

([11]) Cerințele minime pentru sistemele informatice și de comunicații care gestionează IUEC la nivelul RESTREINT UE/EU RESTRICTED sunt prevăzute în apendicele E la anexa III.

([12]) Decizia (UE, Euratom) 2019/1962 a Comisiei din 17 octombrie 2019 privind normele de punere în aplicare pentru gestionarea informațiilor RESTREINT UE/EU RESTRICTED (JO L 311, 2.12.2019, p. 21).

([13]) Decizia (UE, Euratom) 2019/1961 a Comisiei din 17 octombrie 2019 privind normele de punere în aplicare pentru gestionarea informațiilor CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET (JO L 311, 2.12.2019, p. 1).

(4) În cazul în care membrii personalului beneficiarului transportă personal informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET dintr-un stat membru în altul, se aplică următoarele norme suplimentare:

(a) curierul trebuie să fie responsabil de păstrarea în siguranță a materialului clasificat transportat, până la momentul în care acesta este înmânat destinatarului;

(b) în eventualitatea unei încălcări a securității, ANS sau ASD a expeditorului poate solicita ca autoritățile din țara în care a avut loc încălcarea să desfășoare o anchetă, să raporteze constatările în urma acesteia și să ia măsurile legale sau alte măsuri adecvate;

(c) curierul trebuie să fie informat în prealabil cu privire la toate obligațiile de securitate care trebuie respectate în timpul transportului și trebuie să semneze un document corespunzător de luare la cunoștință;

(d) instrucțiunile destinate curierului trebuie să fie atașate la certificatul curierului;

(e) curierului trebuie să i se furnizeze o descriere a transportului și itinerarul;

(f) documentele trebuie să fie returnate ANS sau ASD emitente la finalizarea călătoriei (călătoriilor) sau să fie păstrate de către destinatar, rămânând disponibile în scopuri de monitorizare;

(g) în cazul în care autoritățile vamale, autoritățile de imigrație sau poliția de frontieră solicită examinarea și inspectarea transportului, acestora trebuie să li se permită să deschidă și să observe părți suficiente din acesta, astfel încât să stabilească faptul că nu conține alte materiale decât cele declarate;

(h) autoritățile vamale ar trebui îndemnate să respecte autoritatea oficială a documentelor de transport și a documentelor de autorizare transportate de curier.

În cazul în care un transport este deschis de autoritățile vamale, acest lucru ar trebui realizat la distanță de persoane neautorizate și, pe cât posibil, în prezența curierului. Curierul trebuie să solicite ca transportul să fie reambalat și să le ceară autorităților care efectuează inspecția să resigileze transportul și să confirme în scris că acesta a fost deschis de ele.

(5) Transportul personal al informațiilor clasificate RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET de către membrii personalului beneficiarului către o țară terță sau o organizație internațională va face obiectul dispozițiilor din acordul privind securitatea informațiilor sau din acordul administrativ încheiat între Uniune sau Comisie, pe de o parte, și țara terță sau organizația internațională respectivă, pe de altă parte.

CAPITOLUL 6

PLANIFICAREA CONTINUITĂȚII ACTIVITĂȚII

Articolul 16

Planuri de urgență și măsuri de recuperare

Autoritatea care acordă grantul se asigură că acordul de grant clasificat le impune beneficiarilor să stabilească planuri de asigurare a continuității activității pentru protejarea IUEC gestionate în contextul acordului de grant în situații de urgență, precum și să instituie măsuri preventive și de recuperare în contextul planificării continuității activității, astfel încât să reducă la minimum impactul incidentelor legate de gestionarea și stocarea IUEC. Beneficiarii confirmă autorității care acordă grantul faptul că și-au adoptat planurile de asigurare a continuității activității.

Articolul 17

Intrarea în vigoare

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 10 februarie 2021.

Pentru Comisie,
Pentru Președinte,
Johannes HAHN
Membru al Comisiei

ANEXA I

INFORMAȚII STANDARD ÎN CEREREA DE PROPUNERI

(a se adapta în funcție de cererea de propuneri utilizată)

Securitate

Proiectele care implică informații UE clasificate trebuie să facă obiectul unui control de securitate pentru a autoriza finanțarea și pot face obiectul unor norme de securitate specifice [detaliate într-o anexă de securitate (AS) care însoțește acordul de grant].

Aceste norme (aflate sub incidența Deciziei (UE, Euratom) 2015/444 a Comisiei ([1]) și/sau a reglementărilor naționale) prevăd, de exemplu, următoarele:

— proiectele care implică informații clasificate TRÈS SECRET UE/EU TOP SECRET (sau informații echivalente) **NU** pot fi finanțate;

— informațiile clasificate trebuie marcate în conformitate cu instrucțiunile de securitate aplicabile din AS;

— informațiile cu nivelul de clasificare CONFIDENTIEL UE/EU CONFIDENTIAL sau superior (precum și RESTREINT UE/EU RESTRICTED, dacă normele naționale impun acest lucru) pot fi:

  — create sau accesate numai în incinte care dispun de o autorizare de securitate industrială acordată de autoritatea națională de securitate (ANS) competentă, în conformitate cu normele naționale;

  — gestionate numai într-o zonă securizată acreditată de ANS competentă;

  — accesate și gestionate numai de persoanele care dețin o autorizare de securitate a personalului (ASP) valabilă și care au nevoie să cunoască informațiile respective;

— la sfârșitul grantului, informațiile clasificate trebuie să fie returnate sau să fie protejate în continuare în conformitate cu normele aplicabile;

— sarcinile care implică informații UE clasificate (IUEC) pot fi subcontractate numai cu aprobarea scrisă prealabilă din partea autorității care acordă grantul și numai unor entități stabilite într-un stat membru al UE sau într-o țară din afara UE care a încheiat un acord privind securitatea informațiilor cu UE (sau un acord administrativ cu Comisia);

— divulgarea IUEC către părți terțe face obiectul unei aprobări scrise prealabile din partea autorității care acordă grantul.

Vă rugăm să rețineți că, în funcție de tipul de activitate, este posibil să fie necesară furnizarea autorizării de securitate industrială înainte de semnarea grantului. Autoritatea care acordă grantul va evalua necesitatea autorizărilor în fiecare caz și va stabili data de eliberare a acestora în timpul pregătirii grantului. Vă atragem atenția asupra faptului că nu putem semna **în niciun caz** un acord de grant până când cel puțin unul dintre beneficiarii unui consorțiu nu dispune de o autorizare de securitate industrială.

Alte recomandări în materie de securitate pot fi adăugate la acordul de grant sub forma unor prestații în materie de securitate (*de exemplu crearea unui grup consultativ în materie de securitate, limitarea nivelului de detaliere, utilizarea unui scenariu fals, excluderea utilizării informațiilor clasificate etc.*).

Beneficiarii trebuie să se asigure că proiectele lor nu fac obiectul unor cerințe de securitate naționale/ale țărilor terțe care ar putea afecta punerea în aplicare sau ar putea pune sub semnul întrebării acordarea grantului (*de exemplu restricții tehnologice, clasificări naționale de securitate etc.*). Autoritatea care acordă grantul trebuie să fie informată imediat cu privire la orice eventuale probleme de securitate.

[OPȚIUNE suplimentară pentru acordurile-cadru de parteneriat: În ceea ce privește parteneriatele-cadru, este posibil ca atât cererile de parteneriat-cadru, cât și cererile de grant să fie supuse controlului de securitate.]

([1]) A se vedea Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

ANEXA II

CLAUZE STANDARD ALE ACORDULUI DE GRANT

(a se adapta în funcție de acordul de grant utilizat)

13.2. Securitate – Informații clasificate

Părțile trebuie să gestioneze informațiile clasificate (UE sau naționale) în conformitate cu legislația UE sau națională aplicabilă privind informațiile clasificate [în special Decizia (UE, Euratom) 2015/444 a Comisiei ([1]) și normele sale de punere în aplicare].

Normele specifice de securitate (dacă există) sunt prevăzute în anexa 5.

ANEXA 5

Securitate – Informații UE clasificate

[OPȚIUNE pentru acțiuni cu informații UE clasificate (standard): În cazul în care sunt utilizate sau generate de către acțiunea propriu-zisă, informațiile UE clasificate trebuie tratate în conformitate cu ghidul clasificărilor de securitate (GCS) și cu anexa de securitate (AS), astfel cum se prevede în anexa 1, precum și cu Decizia (UE, Euratom) 2015/444 și cu normele sale de punere în aplicare, până la declasificarea lor.

Prestațiile care conțin informații UE clasificate trebuie transmise în conformitate cu procedurile speciale convenite cu autoritatea care acordă grantul.

Sarcinile care implică informații UE clasificate pot fi subcontractate numai cu aprobarea prealabilă explicită, în scris, din partea autorității care acordă grantul și numai unor entități stabilite într-un stat membru al UE sau într-o țară din afara UE care a încheiat un acord privind securitatea informațiilor cu UE (sau un acord administrativ cu Comisia).

Informațiile UE clasificate nu pot fi divulgate niciunei părți terțe (inclusiv participanților implicați în punerea în aplicare a acțiunii) fără aprobarea prealabilă explicită, în scris, a autorității care acordă grantul.]

([1]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

ANEXA III

[Anexa IV (la ……)]

ANEXA DE SECURITATE (AS) [1]

[Model]

[1] Prezentul model de AS se aplică în cazul în care Comisia este considerată emitentul informațiilor clasificate create și gestionate în vederea executării acordului de grant. În cazul în care emitentul informațiilor clasificate create și gestionate în vederea executării acordului de grant nu este Comisia și în cazul în care statele membre care participă la grant instituie un cadru de securitate specific, se pot aplica și alte modele de AS.

Apendicele A

CERINȚE DE SECURITATE

Autoritatea care acordă grantul trebuie să includă în anexa de securitate (AS) cerințele de securitate de mai jos. Este posibil ca unele clauze să nu se aplice acordului de grant. Acestea sunt indicate între paranteze pătrate.

Lista clauzelor nu este exhaustivă. Pot fi adăugate și alte clauze, în funcție de natura grantului clasificat.

CONDIȚII GENERALE [*NB: aplicabile tuturor acordurilor de grant clasificate*]

1. Prezenta anexă de securitate (AS) face parte integrantă din acordul de grant [sau subcontractul] clasificat și descrie cerințele de securitate specifice acordului de grant. Neîndeplinirea acestor cerințe poate constitui un motiv suficient pentru rezilierea acordului de grant.

2. Beneficiarii grantului fac obiectul tuturor obligațiilor prevăzute în Decizia (UE, Euratom) 2015/444 a Comisiei ([2]) (denumită în continuare „DC 2015/444") și în normele sale de punere în aplicare ([3]). În cazul în care se confruntă cu o problemă în ceea ce privește aplicarea cadrului juridic în vigoare într-un stat membru, beneficiarul grantului trebuie să se adreseze Autorității de securitate a Comisiei și autorității naționale de securitate (ANS) sau autorității de securitate desemnate (ASD).

3. Informațiile clasificate generate în executarea acordului de grant trebuie marcate ca informații UE clasificate (IUEC) la nivelul de clasificare de securitate astfel cum este stabilit în ghidul clasificărilor de securitate (GCS) din apendicele B la prezenta anexă. Abaterea de la nivelul de clasificare de securitate stipulat în GCS poate fi permisă numai cu autorizarea scrisă a autorității care acordă grantul.

4. Drepturile care îi revin emitentului oricărei IUEC create și gestionate în scopul executării acordului de grant clasificat sunt exercitate de Comisie, în calitate de autoritate care acordă grantul.

5. Fără consimțământul scris al autorității care acordă grantul, beneficiarul sau subcontractantul nu trebuie să utilizeze nicio informație și niciun material furnizat de autoritatea care acordă grantul sau elaborat în numele autorității respective în orice alt scop decât cel al acordului de grant.

6. În cazul în care este necesară o autorizare de securitate industrială (ASI) pentru executarea unui acord de grant, beneficiarul trebuie să solicite autorității care acordă grantul să dea curs solicitării ASI.

7. Beneficiarul trebuie să investigheze toate încălcările securității legate de IUEC și să le raporteze autorității care acordă grantul cât mai curând posibil. Beneficiarul sau subcontractantul trebuie să raporteze imediat autorității sale naționale de securitate sau autorității sale de securitate desemnate și, în cazul în care actele cu putere de lege și normele administrative naționale permit acest lucru, Autorității de securitate a Comisiei, toate cazurile în care se cunoaște sau există motive să se suspecteze că IUEC furnizate sau generate în temeiul acordului de grant au fost pierdute sau divulgate unor persoane neautorizate.

([2]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

([3]) Autoritatea care acordă grantul ar trebui să introducă referințele după ce au fost adoptate respectivele norme de punere în aplicare.

8. La sfârșitul acordului de grant, beneficiarul sau subcontractantul trebuie să returneze cât mai curând posibil autorității care acordă grantul orice IUEC pe care le deține. Atunci când este posibil, beneficiarul sau subcontractantul poate distruge IUEC în loc să le returneze. Acest lucru trebuie realizat în conformitate cu actele cu putere de lege și normele administrative naționale din țara în care își are sediul beneficiarul, cu acordul prealabil al Autorității de securitate a Comisiei și conform instrucțiunilor acesteia. IUEC trebuie distruse în așa fel încât să nu poată fi reconstituite nici integral, nici parțial.

9. În cazul în care beneficiarul sau subcontractantul este autorizat să păstreze IUEC după rezilierea sau finalizarea acordului de grant, IUEC trebuie să fie în continuare protejate în conformitate cu DC 2015/444 și cu normele sale de punere în aplicare ([4]).

10. Orice gestionare, prelucrare și transmitere electronică a IUEC trebuie să respecte dispozițiile prevăzute în capitolele 5 și 6 din DC 2015/444. Acestea includ, printre altele, cerința ca sistemele informatice și de comunicații deținute de beneficiar și utilizate pentru gestionarea IUEC în scopul executării acordului de grant (denumite în continuare „SIC ale beneficiarului") să facă obiectul acreditării ([5]), ca orice transmitere electronică a IUEC să fie protejată prin intermediul unor produse criptografice aprobate în conformitate cu articolul 36 alineatul (4) din DC 2015/444 și ca măsurile de securitate TEMPEST să fie puse în aplicare în conformitate cu articolul 36 alineatul (6) din DC 2015/444.

11. Beneficiarul sau subcontractantul trebuie să dispună de planuri de asigurare a continuității activității pentru a proteja orice IUEC gestionate în executarea acordului de grant clasificat în situații de urgență, precum și să instituie măsuri preventive și de recuperare pentru a reduce la minimum impactul incidentelor asociate cu gestionarea și stocarea IUEC. Beneficiarul sau subcontractantul trebuie să informeze autoritatea care acordă grantul cu privire la planurile sale de asigurare a continuității activității.

ACORDURI DE GRANT CARE NECESITĂ ACCES LA INFORMAȚII CLASIFICATE RESTREINT UE/EU RESTRICTED

12. În principiu, nu este necesară autorizarea de securitate a personalului (ASP) în scopul conformității cu acordul de grant ([6]). Totuși, informațiile sau materialele clasificate RESTREINT UE/EU RESTRICTED trebuie să fie accesibile numai membrilor personalului beneficiarului care au nevoie de aceste informații pentru executarea acordului de grant (*principiul necesității de a cunoaște*), care au fost informați de ofițerul de securitate al beneficiarului cu privire la responsabilitățile lor și la consecințele oricărei compromiteri sau încălcări a securității cu privire la informațiile respective și care au confirmat în scris faptul că au luat cunoștință de consecințele neasigurării protecției IUEC.

13. Cu excepția situației în care autoritatea care acordă ajutorul și-a dat acordul în scris, beneficiarul sau subcontractantul nu trebuie să acorde acces la informații sau materiale clasificate RESTREINT UE/EU RESTRICTED niciunei alte entități sau persoane în afara membrilor personalului său care au nevoie să cunoască informațiile respective.

14. Beneficiarul sau subcontractantul trebuie să păstreze marcajele de clasificare de securitate pentru informațiile clasificate generate sau furnizate în cadrul executării unui acord de grant și nu trebuie să declasifice informațiile fără acordul scris al autorității care acordă grantul.

15. Atunci când nu sunt utilizate, informațiile sau materialele clasificate RESTREINT UE/EU RESTRICTED trebuie depozitate în mobilier de birou încuiat. În tranzit, documentele trebuie transportate într-un plic opac. Documentele nu trebuie să iasă din posesia persoanei care le transportă și nu trebuie deschise pe drum.

([4]) Autoritatea care acordă grantul ar trebui să introducă referințele după ce au fost adoptate respectivele norme de punere în aplicare.

([5]) Partea care este acreditată va trebui să prezinte autorității care acordă grantul o declarație de conformitate, prin intermediul Autorității de securitate a Comisiei și în coordonare cu autoritatea națională relevantă de acreditare în materie de securitate (AAS).

([6]) În cazul în care beneficiarii provin din state membre care solicită ASP și/sau ASI pentru granturi clasificate RESTREINT UE/EU RESTRICTED, autoritatea care acordă grantul enumeră în cadrul AS aceste cerințe privind ASP și ASI pentru beneficiarii în cauză.

16. Beneficiarul sau subcontractantul poate transmite autorității care acordă grantul documentele clasificate RESTREINT UE/EU RESTRICTED folosind societăți comerciale de curierat, servicii poștale, transportul personal sau mijloace electronice. În acest scop, beneficiarul sau subcontractantul trebuie să respecte instrucțiunile de securitate ale programului (proiectului) (ISP) emise de Comisie și/sau normele de punere în aplicare ale Comisiei privind securitatea industrială referitoare la granturile clasificate ([7]).

17. Atunci când nu mai sunt necesare, documentele clasificate RESTREINT UE/EU RESTRICTED trebuie distruse în așa fel încât să nu poată fi reconstituite nici integral, nici parțial.

18. Acreditarea în materie de securitate a SIC ale beneficiarului care gestionează IUEC la nivelul RESTREINT UE/EU RESTRICTED și orice interconexiune în acest sens pot fi delegate ofițerului de securitate al beneficiarului în cazul în care actele cu putere de lege și normele administrative naționale permit acest lucru. În cazul în care acreditarea este delegată astfel, ANS, ASD sau autoritățile de acreditare în materie de securitate (AAS) păstrează responsabilitatea pentru protecția informațiilor RESTREINT UE/EU RESTRICTED gestionate de beneficiar, precum și dreptul de a inspecta măsurile de securitate luate de acesta. În plus, beneficiarul oferă autorității care acordă grantul și, atunci când acest lucru este impus prin actele cu putere de lege și normele administrative naționale, AAS naționale competente, o declarație de conformitate care certifică faptul că SIC ale beneficiarului și interconexiunile aferente au fost acreditate pentru gestionarea IUEC la nivelul RESTREINT UE/EU RESTRICTED.

GESTIONAREA INFORMAȚIILOR CLASIFICATE RESTREINT UE/EU RESTRICTED ÎN CADRUL SISTEMELOR INFORMATICE ȘI DE COMUNICAȚII (SIC)

19. Cerințele minime pentru SIC care gestionează informații clasificate RESTREINT UE/EU RESTRICTED sunt prevăzute în apendicele E la prezenta AS.

CONDIȚIILE ÎN CARE BENEFICIARUL POATE SUBCONTRACTA

20. Beneficiarul trebuie să obțină permisiunea autorității care acordă grantul înainte de a subcontracta orice parte a unui acord de grant clasificat.

21. Niciun subcontract nu poate fi atribuit unei entități înregistrate într-o țară din afara UE sau unei entități care aparține unei organizații internaționale în cazul în care respectiva țară din afara UE sau organizație internațională nu a încheiat un acord privind securitatea informațiilor cu UE sau un acord administrativ cu Comisia.

22. În cazul în care beneficiarul a atribuit un subcontract, dispozițiile de securitate din acordul de grant se aplică *mutatis mutandis* subcontractantului (subcontractanților) și personalului acestuia (acestora). Într-un astfel de caz, beneficiarului îi revine responsabilitatea de a se asigura că toți subcontractanții aplică, la rândul lor, aceste principii acordurilor de subcontractare pe care le încheie. Pentru a se asigura monitorizarea adecvată a securității, ANS și/sau ASD ale beneficiarului și ale subcontractantului trebuie să fie notificate de către Autoritatea de securitate a Comisiei cu privire la atribuirea tuturor subcontractelor clasificate conexe de la nivelurile CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET. Dacă este cazul, ANS și/sau ASD ale beneficiarului și ale subcontractantului primesc o copie a dispozițiilor de securitate specifice subcontractului. ANS și ASD care trebuie notificate cu privire la dispozițiile de securitate din acordurile de grant clasificate la nivelul RESTREINT UE/EU RESTRICTED sunt enumerate în anexa la normele de punere în aplicare ale Comisiei privind securitatea industrială referitoare la acordurile de grant clasificate ([8]).

23. Beneficiarul nu poate transmite IUEC unui subcontractant fără aprobarea în scris prealabilă a autorității care acordă grantul. Dacă IUEC trebuie transmise subcontractanților frecvent sau în mod sistematic, autoritatea care acordă grantul își poate da acordul pentru o anumită perioadă (de exemplu 12 luni) sau pentru întreaga durată a subcontractului.

([7]) Autoritatea care acordă grantul ar trebui să introducă referințele după ce au fost adoptate respectivele norme de punere în aplicare.
([8]) Autoritatea care acordă grantul ar trebui să introducă referințele după ce au fost adoptate respectivele norme de punere în aplicare.

VIZITE

În cazul în care procedura standard pentru cererile de vizită trebuie aplicată vizitelor care implică informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, autoritatea care acordă grantul trebuie să includă punctele 24, 25 și 26 și să elimine punctul 27. În cazul în care sunt organizate vizite care implică informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET direct de unitatea care trimite vizitatorul împreună cu unitatea care primește vizitatorul, autoritatea care acordă grantul trebuie să elimine punctele 25 și 26 și să includă numai punctul 27.

24. Vizitele care implică accesul sau accesul potențial la informații clasificate RESTREINT UE/EU RESTRICTED trebuie să fie organizate direct de unitatea care trimite vizitatorul împreună cu unitatea care primește vizitatorul, fără a fi necesară parcurgerea procedurii descrise la punctele 25-27 de mai jos.

[25. Vizitele care implică accesul sau accesul potențial la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET fac obiectul următoarei proceduri:

(a) ofițerul de securitate al clădirii care trimite vizitatorul completează toate părțile relevante ale formularului de cerere de vizită (apendicele C) și transmite cererea către ANS sau ASD a clădirii;

(b) ANS sau ASD a clădirii care trimite vizitatorul trebuie să confirme ASP a vizitatorului înainte de a transmite cererea de vizită ANS sau ASD a clădirii-gazdă (sau Autorității de securitate a Comisiei în cazul în care vizita are loc în incintele autorității care acordă grantul);

(c) ofițerul de securitate al clădirii care trimite vizitatorul obține apoi de la propria ANS sau ASD răspunsul ANS sau al ASD a clădirii-gazdă (sau al Autorității de securitate a Comisiei), care fie autorizează, fie respinge cererea de vizită;

(d) cerere de vizită este considerată aprobată în cazul în care nu sunt prezentate obiecțiuni până în momentul în care au mai rămas cinci zile lucrătoare până la data vizitei.]

[26. Înainte de a acorda vizitatorului (vizitatorilor) acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, clădirea-gazdă trebuie să primească autorizarea din partea propriei ANS sau ASD.]

[27. Vizitele care implică accesul sau accesul potențial la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET trebuie să fie organizate direct de unitatea care trimite vizitatorul împreună cu unitatea care primește vizitatorul (un exemplu al formularului care poate fi folosit în acest scop este furnizat în apendicele C).]

28. La sosirea în clădirea-gazdă, vizitatorii trebuie să facă dovada identității lor prin prezentarea unei cărți de identitate valabile sau a unui pașaport valabil.

29. Clădirea care găzduiește vizita trebuie să se asigure că sunt păstrate evidențe ale tuturor vizitatorilor. Acestea trebuie să includă numele lor, organizația pe care o reprezintă, data expirării ASP (dacă este cazul), data vizitei și numele persoanei (persoanelor) vizitate. Fără a aduce atingere normelor europene privind protecția datelor, aceste evidențe trebuie păstrate o perioadă de cel puțin cinci ani sau în conformitate cu normele și reglementările naționale, după caz.

VIZITE DE EVALUARE

30. Autoritatea de securitate a Comisiei poate, în cooperare cu ANS sau ASD relevantă, să desfășoare vizite în clădirile beneficiarilor sau ale subcontractanților pentru a verifica respectarea cerințelor de securitate pentru gestionarea IUEC.

GHIDUL CLASIFICĂRILOR DE SECURITATE

31. O listă a tuturor elementelor din acordul de grant care sunt clasificate sau care urmează să fie clasificate pe parcursul executării acordului de grant, normele necesare în acest scop și specificarea nivelurilor de clasificare de securitate aplicabile sunt incluse în ghidul clasificărilor de securitate (GCS). GCS face parte integrantă din acordul de grant și poate fi consultat în apendicele B la prezenta anexă.

Apendicele B

GHIDUL CLASIFICĂRILOR DE SECURITATE

[text specific care urmează să fie ajustat în funcție de obiectul acordului de grant]

Apendicele C

CERERE DE VIZITĂ (MODEL)

INSTRUCȚIUNI DETALIATE PRIVIND COMPLETAREA CERERII DE VIZITĂ

(Solicitarea trebuie depusă numai în limba engleză)

TITLU	A se bifa casetele privind tipul vizitei și tipul de informații și a se indica câte locuri urmează să fie vizitate și numărul vizitatorilor.
4. **DATE ADMINISTRATIVE**	A se completa de către ANS/ASD solicitantă.
5. **ORGANIZAȚIA SAU CLĂDIREA INDUSTRIALĂ SOLICITANTĂ**	Indicați denumirea completă și adresa poștală. A se include orașul, statul și codul poștal, după caz.
6. **ORGANIZAȚIA SAU CLĂDIREA INDUSTRIALĂ CARE URMEAZĂ SĂ FIE VIZITATĂ**	Indicați denumirea completă și adresa poștală. A se include orașul, statul, codul poștal, numărul de telex sau de fax (dacă există), numărul de telefon și adresa de e-mail. A se indica numele și numărul de telefon/fax și adresa de e-mail ale punctului dumneavoastră principal de contact sau ale persoanei cu care ați programat vizita. Observații: 1. Indicarea codului poștal corect este importantă deoarece o societate poate deține mai multe clădiri diferite. 2. În cazul în care cererea se depune manual, anexa 1 poate fi utilizată atunci când trebuie vizitate două sau mai multe clădiri în legătură cu același subiect. În cazul în care se folosește o anexă, punctul 3 ar trebui să indice: „A SE VEDEA ANEXA 1, NUMĂR DE CLĂDIRI…” (indicați numărul de clădiri).
7. **DATELE VIZITEI**	Indicați data sau perioada efectivă (de la prima la ultima zi) a vizitei în formatul „zi-lună-an”. Dacă este cazul, indicați o dată sau o perioadă alternativă între paranteze.
8. **TIPUL DE INIȚIATIVĂ**	Specificați dacă vizita a fost inițiată de organizația sau clădirea solicitantă sau la invitația clădirii care urmează să fie vizitată.
9. **VIZITA PRIVEȘTE:**	Indicați denumirea completă a proiectului, a contractului sau a licitației, folosind numai abrevierile utilizate în mod obișnuit.
10. **SUBIECTUL DE DISCUTAT/ JUSTIFICARE**	Prezentați o scurtă descriere a motivului (motivelor) vizitei. Nu utilizați abrevieri care nu au fost explicate. Observații: În cazul vizitelor recurente, acest punct ar trebui să indice „Vizite recurente” ca prime cuvinte în elementul de date (de exemplu, Vizite recurente pentru a discuta_____).
11. **NIVELUL ANTICIPAT AL INFORMAȚIILOR CLASIFICATE CARE URMEAZĂ SĂ FIE IMPLICATE**	Indicați SECRET UE/EU SECRET (S-UE/EU-S) sau CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), după caz.

12. **DATE PRIVIND VIZITATORUL**	Observație: atunci când în vizită sunt implicați mai mult de doi vizitatori, ar trebui să se utilizeze anexa 2.
13. **OFIȚERUL DE SECURITATE AL ENTITĂȚII SOLICITANTE**	La acest punct trebuie indicate numele, numărul de telefon, numărul de fax și adresa de e-mail ale ofițerului de securitate al clădirii solicitante.
14. **CERTIFICAREA AUTORIZĂRII DE SECURITATE**	Acest câmp trebuie completat de autoritatea de certificare. Note pentru autoritatea de certificare: (a) indicați numele, adresa, numărul de telefon, numărul de fax și adresa de e-mail (pot fi imprimate în prealabil); (b) acest punct trebuie semnat și ștampilat (după caz).
15. **AUTORITATE DE SECURITATE SOLICITANTĂ**	Acest câmp trebuie completat de ANS/ASD. Notă pentru ANS/ASD: (a) indicați numele, adresa, numărul de telefon, numărul de fax și adresa de e-mail (pot fi imprimate în prealabil); (b) acest punct trebuie semnat și ștampilat (după caz).

Toate câmpurile trebuie completate, iar formularul trebuie transmis prin intermediul canalelor dintre administrațiile guvernamentale ([9]).

CERERE DE VIZITĂ

(MODEL)

CĂTRE: _____

1. **TIPUL DE CERERE DE VIZITĂ**	2. **TIPUL DE INFORMAȚII**	3. **CUPRINS**
☐ Vizită unică ☐ Vizită recurentă ☐ Vizită de urgență ☐ Modificare ☐ Date ☐ Vizitatori ☐ Clădire În cazul unei modificări, introduceți numărul de referință inițial al cererii de vizită alocat de ANS/ASD Nr. _____	☐ C-UE/EU-C ☐ S-UE/EU-S	Nr. de locuri: _____ Nr. de vizitatori: _____

4. **DATE ADMINISTRATIVE:**	
Solicitant: Către:	Nr. de referință al cererii de vizită alocat de ANS/ASD Nr. _____ Data *(zz/ll/aaaa)*: _____/_____/_____

([9]) În cazul în care s-a convenit că vizitele care implică accesul sau accesul potențial la IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET pot fi organizate direct, formularul completat poate fi transmis direct ofițerului de securitate al unității care urmează să fie vizitată.

5. **ORGANIZAȚIA SAU CLĂDIREA INDUSTRIALĂ SOLICITANTĂ**

DENUMIRE:

ADRESA POȘTALĂ:

E-MAIL:

FAX TEL.

6. **ORGANIZAȚIA (ORGANIZAȚIILE) SAU CLĂDIREA INDUSTRIALĂ (CLĂDIRILE INDUSTRIALE) CARE URMEAZĂ SĂ FIE VIZITATĂ (VIZITATE)** ***(a se completa anexa 1)***

7. **DATA VIZITEI** ***(zz/ll/aaaa)*****: DE LA _____/_____/_____ LA _____/_____/_____**

8. **TIPUL DE INIȚIATIVĂ:**

□ Inițiată de organizația sau clădirea solicitantă

□ La invitația clădirii care urmează să fie vizitată

9. **VIZITA PRIVEȘTE CONTRACTUL:**

10. **SUBIECTUL DE DISCUTAT/MOTIVE/SCOP (a se include detalii privind entitatea-gazdă și orice alte informații relevante. Abrevierile ar trebui evitate):**

11. **CEL MAI ÎNALT NIVEL DE CLASIFICARE ANTICIPAT PENTRU INFORMAȚIILE/ MATERIALELE SAU ACCESUL LA LOCUL VIZITEI CARE URMEAZĂ SĂ FIE IMPLICATE:**

12. **DATE PRIVIND VIZITATORUL (VIZITATORII)** ***(a se completa anexa 2)***

13. **OFIȚERUL DE SECURITATE AL ORGANIZAȚIEI SAU CLĂDIRII INDUSTRIALE SOLICITANTE:**

NUME:

TEL.

E-MAIL:

SEMNĂTURĂ:

14. CERTIFICAREA NIVELULUI AUTORIZĂRII DE SECURITATE:

NUME:

ADRESĂ:

TEL.

E-MAIL:

SEMNĂTURĂ:

ȘTAMPILĂ

DATA *(zz/ll/aaaa)*:
_____/_____/_____

15. **AUTORITATEA NAȚIONALĂ DE SECURITATE/AUTORITATEA DE SECURITATE DESEMNATĂ SOLICITANTĂ:**

NUME:

ADRESĂ:

TEL.

E-MAIL:

ȘTAMPILĂ

SEMNĂTURĂ:

DATA *(zz/ll/aaaa)*:
_____/_____/_____

16. **OBSERVAȚII *(Justificare obligatorie în cazul unei vizite de urgență)*:**

<Spațiu rezervat pentru trimiterea la legislația aplicabilă privind datele cu caracter personal și linkul către informațiile obligatorii pentru persoana vizată, de exemplu modul în care este pus în aplicare articolul 13 din Regulamentul general privind protecția datelor ([10]).>

([10]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

ANEXA 1 la FORMULARUL DE CERERE DE VIZITĂ

ORGANIZAȚIA (ORGANIZAȚIILE) SAU CLĂDIREA INDUSTRIALĂ (CLĂDIRILE INDUSTRIALE) CARE URMEAZĂ SĂ FIE VIZITATĂ (VIZITATE)
1. DENUMIRE: ADRESĂ: TEL. FAX NUMELE PUNCTULUI DE CONTACT: E-MAIL: TEL. NUMELE OFIȚERULUI DE SECURITATE SAU NUMELE CELUI DE AL DOILEA PUNCT DE CONTACT: E-MAIL: TEL.
2. DENUMIRE: ADRESĂ: TEL. FAX NUMELE PUNCTULUI DE CONTACT: E-MAIL: TEL. NUMELE OFIȚERULUI DE SECURITATE SAU NUMELE CELUI DE AL DOILEA PUNCT DE CONTACT: E-MAIL: TEL. ***(Se completează în continuare în funcție de necesități)***

<Spațiu rezervat pentru trimiterea la legislația aplicabilă privind datele cu caracter personal și linkul către informațiile obligatorii pentru persoana vizată, de exemplu modul în care este pus în aplicare articolul 13 din Regulamentul general privind protecția datelor ([11]).>

([11]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

ANEXA 2 la FORMULARUL DE CERERE DE VIZITĂ

DATE PRIVIND VIZITATORUL (VIZITATORII)
1. NUME: PRENUME (conform pașaportului): DATA NAȘTERII *(zz/ll/aaaa)*:____/____/____ LOCUL NAȘTERII: CETĂȚENIE: NIVELUL AUTORIZĂRII DE SECURITATE: NUMĂR PAȘAPORT/CARTE DE IDENTITATE: POZIȚIE: SOCIETATE/ORGANIZAȚIE:
2. NUME: PRENUME *(conform pașaportului)*: DATA NAȘTERII *(zz/ll/aaaa)*:____/____/____ LOCUL NAȘTERII: CETĂȚENIE: NIVELUL AUTORIZĂRII DE SECURITATE: NUMĂR PAȘAPORT/CARTE DE IDENTITATE: POZIȚIE: SOCIETATE/ORGANIZAȚIE: ***(Se completează în continuare în funcție de necesități)***

<Spațiu rezervat pentru trimiterea la legislația aplicabilă privind datele cu caracter personal și linkul către informațiile obligatorii pentru persoana vizată, de exemplu modul în care este pus în aplicare articolul 13 din Regulamentul general privind protecția datelor ([12]).>

([12]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

Apendicele D

FIȘA INFORMATIVĂ PRIVIND AUTORIZAREA DE SECURITATE INDUSTRIALĂ (FIASI) (MODEL)

1. **INTRODUCERE**

1.1. Se regăsește atașat un model de fișă informativă privind autorizarea de securitate industrială (FIASI) pentru schimbul rapid de informații între autoritatea națională de securitate (ANS) sau autoritatea de securitate desemnată (ASD), alte autorități naționale de securitate competente și Autoritatea de securitate a Comisiei (care acționează în numele autorităților care acordă grantul) cu privire la autorizarea de securitate industrială (ASI) a unei clădiri implicate în cererile de granturi sau de subcontracte clasificate și în punerea în aplicare a acestora.

1.2. FIASI este valabilă numai dacă este ștampilată de ANS relevantă, de ASD relevantă sau de altă autoritate competentă.

1.3. FIASI este compusă dintr-o secțiune pentru cerere și o secțiune pentru răspuns și poate fi utilizată în scopurile identificate mai sus sau în orice alte scopuri pentru care este necesar statutul ASI pentru o anumită clădire. Motivul solicitării trebuie identificat de ANS sau ASD solicitantă în câmpul 7 din secțiunea pentru cerere.

1.4. Detaliile conținute în FIASI nu sunt, de regulă, clasificate; în consecință, atunci când o FIASI urmează să fie transmisă între ANS/ASD/Comisie, aceasta ar trebui realizată, de preferință, prin intermediul mijloacelor electronice.

1.5. ANS/ASD ar trebui să depună toate eforturile pentru a răspunde unei cereri de FIASI în termen de 10 zile lucrătoare.

1.6. În cazul în care sunt transferate informații clasificate sau un grant ori subcontract este atribuit în legătură cu această asigurare, ANS sau ASD emitentă trebuie informată.

Proceduri și instrucțiuni pentru utilizarea fișei informative privind autorizarea de securitate industrială (FIASI)

Prezentele instrucțiuni detaliate sunt destinate ANS sau ASD ori autorității care acordă grantul și Autorității de securitate a Comisiei, care completează FIASI. Solicitarea ar trebui, de preferință, să fie scrisă cu litere majuscule.

ANTET	Solicitantul introduce denumirea completă a ANS/ASD și a țării.
1. **TIPUL CERERII**	Autoritatea solicitantă care acordă grantul selectează casetele adecvate pentru tipul cererii de FIASI. A se include nivelul de autorizare de securitate solicitat. Trebuie utilizate următoarele abrevieri: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C SIC = sisteme informatice și de comunicații pentru prelucrarea informațiilor clasificate.
2. **DETALII PRIVIND SUBIECTUL**	Câmpurile 1-6 sunt evidente. În câmpul 4 ar trebui utilizat un cod de țară standard, format din două litere. Câmpul 5 este opțional.
3. **MOTIVUL CERERII**	A se indica motivul specific al cererii, indicatorii de proiect, numărul cererii de propuneri sau al grantului. A se specifica nevoia de capacitate de stocare, nivelul de clasificare a SIC etc. Ar trebui inclus(ă) orice termen-limită/dată a expirării/dată a atribuirii care poate avea o influență asupra completării unei ASI.

4. **ANS/ASD SOLICITANTĂ**	Indicați numele solicitantului efectiv (în numele ANS/ASD) și data cererii în format numeric (zz/ll/aaaa).
5. **SECȚIUNEA PENTRU RĂSPUNS**	Câmpurile 1-5: selectați câmpurile adecvate. Câmpul 2: în cazul în care o ASI este în curs, se recomandă să se ofere solicitantului o indicație privind durata necesară pentru prelucrare (dacă se cunoaște). Câmpul 6: (a) deși validarea diferă în funcție de țară sau chiar de clădire, se recomandă ca data expirării ASI să fie menționată. (b) în cazul în care data expirării asigurării ASI este nedefinită, acest câmp poate fi tăiat cu o linie. (c) în conformitate cu normele și reglementările naționale respective, solicitantul sau fie beneficiarul, fie subcontractantul este responsabil de solicitarea reînnoirii ASI.
6. **OBSERVAȚII**	Pot fi folosite pentru informații suplimentare privind ASI, clădirea sau elementele de mai sus.
7. **ANS/ASD EMITENTĂ**	Indicați denumirea autorității emitente (în numele ANS/ASD) și data răspunsului în format numeric (zz/ll/aaaa).

FIȘA INFORMATIVĂ PRIVIND AUTORIZAREA DE SECURITATE INDUSTRIALĂ (FIASI) (MODEL)

Toate câmpurile trebuie completate, iar formularul trebuie transmis prin intermediul canalelor dintre administrațiile guvernamentale sau al canalelor dintre administrația guvernamentală și organizația internațională.

CERERE DE ASIGURARE A AUTORIZĂRII DE SECURITATE INDUSTRIALĂ

CĂTRE: _____

(Denumirea țării ANS/ASD)

Completați casetele de răspuns, după caz:

[ ] Furnizați o asigurare ASI la nivelul: [ ] S-UE/EU-S [ ] C-UE/EU-C

pentru clădirea indicată mai jos

[ ] inclusiv protejarea informațiilor/materialelor clasificate

[ ] inclusiv sisteme informatice și de comunicații (SIC) pentru prelucrarea informațiilor clasificate

[ ] Inițiați, direct sau la cererea corespunzătoare a unui beneficiar sau subcontractant, procesul obținerii unei ASI până la și incluzând nivelul ..... cu nivelul de protecție ..... și nivelul ..... pentru SIC, în cazul în care clădirea nu deține, în prezent, nivelurile respective de capabilități.

Confirmați exactitatea detaliilor de mai jos privind clădirea și furnizați corecturi/informații suplimentare după caz.

1. Denumirea completă a clădirii: Corecturi/informații suplimentare:

....

2. Adresa completă a clădirii:

....

3. Adresa poștală (dacă diferă de 2)

....

4. Codul poștal al orașului/al țării

....

5. Numele ofițerului de securitate

.....
.....

6. Nr. de telefon/fax/adresa de e-mail ale ofițerului de securitate

....

7. Cererea este efectuată din motivul (motivele) următor (următoare): [furnizați detalii privind etapa precontractuală (selectarea propunerii), grantul sau subcontractul, programul/proiectul etc.]

.....

ANS solicitantă/ ASD solicitantă/ autoritatea solicitantă care acordă grantul: Denumire: .....

Data (zz/ll/aaaa) : .....

RĂSPUNS (în termen de 10 zile lucrătoare)

Prin prezenta se certifică următoarele:

1. [ ] clădirea menționată mai sus deține ASI până la nivelul [ ] S-UE/EU-S inclusiv

   [ ] C-UE/EU-C.

2. clădirea menționată mai sus deține capabilitatea de a proteja informații/materiale clasificate:

   [ ] da, nivelul: ..... [ ] nu.

3. clădirea menționată mai sus deține un SIC acreditat/autorizat:

   [ ] da, nivelul: ..... [ ] nu.

4. [ ] în legătură cu cererea menționată mai sus, a fost inițiat procesul privind ASI. Veți fi informat cu privire la acordarea sau refuzarea acordării ASI.

5. [ ] clădirea menționată mai sus nu deține o ASI.

6. Această asigurare ASI expiră la: ..... (*zz/ll/aaaa*) sau după cum recomandă ANS/ASD. Veți fi informat în cazul unei invalidări anticipate sau al oricăror modificări aduse informațiilor enumerate mai sus.

7. Observații:
   .....

*ANS/ASD emitentă*Denumire: ..... *Data: (zz/ll/aaaa)* .....

<Spațiu rezervat pentru trimiterea la legislația aplicabilă privind datele cu caracter personal și linkul către informațiile obligatorii pentru persoana vizată, de exemplu modul în care este pus în aplicare articolul 13 din Regulamentul general privind protecția datelor ([13]).>

([13]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

Apendicele E

Cerințe minime pentru protecția IUEC în format electronic la nivelul RESTREINT UE/EU RESTRICTED gestionate în SIC al beneficiarului

Aspecte generale

1. Beneficiarul trebuie să fie responsabil de asigurarea faptului că protecția informațiilor clasificate RESTREINT UE/EU RESTRICTED respectă cerințele minime de securitate astfel cum sunt prevăzute în prezenta clauză de securitate și orice alte cerințe suplimentare recomandate de autoritatea care acordă grantul sau, dacă este cazul, de autoritatea națională de securitate (ANS) sau autoritatea de securitate desemnată (ASD).

2. Beneficiarul este responsabil de punerea în aplicare a cerințelor de securitate identificate în prezentul document.

3. În scopul prezentului document, un sistem informatic și de comunicații (SIC) acoperă toate echipamentele utilizate pentru gestionarea, stocarea și transmiterea IUEC, inclusiv stații de lucru, imprimante, copiatoare, faxuri, servere, sisteme de gestionare a rețelei, dispozitive de control al rețelei și dispozitive de control al comunicațiilor, laptopuri, notebookuri, tablete, telefoane inteligente și dispozitive de stocare mobile, precum unități flash pentru USB, CD-uri, carduri SD etc.

4. Echipamentele speciale, precum produsele criptografice, trebuie protejate în conformitate cu procedurile sale operaționale de securitate specifice (SecOP).

5. Beneficiarii trebuie să stabilească o structură responsabilă de gestionarea, din punctul de vedere al securității, a SIC care gestionează informații clasificate RESTREINT UE/EU RESTRICTED și să numească un ofițer de securitate responsabil de clădirea vizată.

6. Utilizarea soluțiilor informatice (hardware, software sau servicii) deținute în privat de personalul beneficiarului pentru stocarea sau prelucrarea informațiilor RESTREINT UE/EU RESTRICTED nu este permisă.

7. Acreditarea SIC al beneficiarului prin care se gestionează informații clasificate RESTREINT UE/EU RESTRICTED trebuie să fie aprobată de autoritatea de acreditare în materie de securitate (AAS) din statul membru vizat sau trebuie să fie delegată ofițerului de securitate al beneficiarului, astfel cum este permis prin actele cu putere de lege și normele administrative naționale.

8. Numai informațiile clasificate RESTREINT UE/EU RESTRICTED care sunt criptate cu ajutorul produselor criptografice aprobate pot fi gestionate, stocate sau transmise (prin mijloace tehnice cu fir sau fără fir) la fel ca orice alte informații neclasificate din cadrul acordului de grant. Aceste produse criptografice trebuie să fie aprobate de UE sau de un stat membru.

9. Clădirile externe implicate în activitățile de întreținere/reparație trebuie să fie obligate contractual să respecte dispozițiile aplicabile pentru gestionarea informațiilor clasificate RESTREINT UE/EU RESTRICTED, astfel cum se prevede în prezentul document.

10. La solicitarea autorității care acordă grantul sau a ANS, ASD ori AAS relevante, beneficiarul trebuie să furnizeze dovezi ale conformității cu clauza de securitate din acordul de grant. În cazul în care un audit și o inspecție a proceselor și clădirilor beneficiarului sunt, de asemenea, necesare, pentru a asigura conformitatea cu aceste cerințe, beneficiarii permit reprezentanților autorității care acordă grantul, ANS, ASD sau AAS ori autorității relevante în materie de securitate din UE să efectueze auditul și inspecția respectivă.

Securitatea fizică

11. Zonele în care SIC sunt utilizate pentru a afișa, a stoca, a prelucra sau a transmite informații RESTREINT UE/EU RESTRICTED sau zonele în care se află serverele, sistemele de gestionare a rețelei, dispozitivele de control al rețelei și al comunicațiilor pentru SIC respectiv ar trebui stabilite ca zone separate și controlate, cu un sistem adecvat de control al accesului. Accesul la aceste zone separate și controlate ar trebui restricționat la persoanele cu autorizare specifică. Fără a aduce atingere punctului 8, echipamentele descrise la punctul 3 trebuie stocate în astfel de zone separate și controlate.

12. Trebuie puse în aplicare mecanisme și/sau proceduri de securitate pentru a reglementa introducerea sau conectarea unor suporturi informatice de stocare mobile (precum unități flash pentru USB, dispozitive de stocare în masă sau CD-RW) la componentele SIC.

Accesul la SIC

13. Accesul la SIC al beneficiarului prin care se gestionează IUEC este permis pe baza unei nevoi stricte de a cunoaște informațiile respective și a unei autorizări a personalului.

14. Toate SIC trebuie să conțină liste actualizate ale utilizatorilor autorizați. Toți utilizatorii trebuie autentificați la începutul fiecărei sesiuni de prelucrare.

15. Parolele, care fac parte din majoritatea măsurilor de securitate bazate pe identificare și autentificare, trebuie să aibă o lungime de cel puțin nouă caractere și să includă caractere numerice și „speciale” (dacă sistemul le acceptă), precum și caractere alfabetice. Parolele trebuie schimbate cel puțin la 180 de zile. Acestea trebuie schimbate cât de curând posibil în cazul în care au fost compromise sau divulgate unei persoane neautorizate sau dacă se suspectează o astfel de compromitere sau divulgare.

16. Toate SIC trebuie să dispună de elemente de control al accesului intern pentru a preveni ca utilizatori neautorizați să acceseze sau să modifice informațiile clasificate RESTREINT UE/EU RESTRICTED și să modifice elementele de control al sistemului și al securității. Utilizatorii trebuie să fie deconectați automat din SIC în cazul în care terminalele acestora au fost inactive o perioadă prestabilită sau SIC trebuie să activeze un economizor de ecran protejat de o parolă după 15 minute de inactivitate.

17. Fiecărui utilizator al SIC i se alocă un cont de utilizator și un nume de utilizator unice. Conturile de utilizator trebuie blocate automat în cazul a cel puțin cinci încercări succesive de autentificare nereușite.

18. Toți utilizatorii SIC trebuie să cunoască responsabilitățile care le revin și procedurile care trebuie urmate pentru protejarea informațiilor clasificate RESTREINT UE/EU RESTRICTED în cadrul SIC. Responsabilitățile și procedurile care trebuie urmate trebuie documentate, iar utilizatorii trebuie să confirme în scris faptul că au luat cunoștință de ele.

19. SecOP trebuie să fie disponibile pentru utilizatori și administratori și trebuie să includă descrieri ale rolurilor în materie de securitate și lista de sarcini, instrucțiuni și planuri aferentă.

Contabilitate, audit și răspuns la incidente

20. Orice acces la SIC trebuie înregistrat.

21. Următoarele evenimente trebuie înregistrate:

    (a) toate încercările de autentificare, reușite sau nereușite;

    (b) deconectarea (inclusiv sesiuni expirate, după caz);

    (c) crearea, eliminarea sau modificarea drepturilor și privilegiilor de acces;

    (d) crearea, ștergerea sau modificarea parolelor.

22. În cazul tuturor evenimentelor enumerate mai sus, trebuie comunicate cel puțin următoarele informații:

    (a) tipul evenimentului;

    (b) identificatorul utilizatorului;

    (c) data și ora;

    (d) codul de identificare al dispozitivului.

23. Registrele contabile ar trebui să ajute un ofițer de securitate să examineze eventualele incidente de securitate. Acestea pot fi utilizate, de asemenea, pentru a sprijini orice investigații legale în eventualitatea unui incident de securitate. Toate registrele de securitate ar trebui verificate periodic pentru a identifica eventuale incidente de securitate. Registrele contabile trebuie protejate împotriva ștergerii sau modificării neautorizate.

24. Beneficiarul trebuie să dispună de o strategie de răspuns stabilită, pentru a trata incidentele de securitate. Utilizatorii și administratorii trebuie instruiți cu privire la modalitatea de răspuns la incidente, de raportare a acestora și de reacție în cazul unei urgențe.

25. Compromiterea sau suspiciunea de compromitere a informațiilor clasificate RESTREINT UE/EU RESTRICTED trebuie raportată autorității care acordă grantul. Raportul trebuie să conțină o descriere a informațiilor implicate și o descriere a circumstanțelor compromiterii sau suspiciunii de compromitere. Toți utilizatorii SIC trebuie să ia cunoștință de modul în care trebuie raportat ofițerului de securitate orice incident de securitate efectiv sau suspectat.

Crearea de rețele și interconectarea

26. În cazul în care SIC al unui beneficiar prin care se gestionează informații clasificate RESTREINT UE/EU RESTRICTED este interconectat cu un SIC care nu este acreditat, crește în mod semnificativ amenințarea atât la adresa securității SIC, cât și a informațiilor RESTREINT UE/EU RESTRICTED gestionate de acel SIC. Sunt incluse aici internetul și orice alt SIC public sau privat, de exemplu alt SIC deținut de beneficiar sau subcontractant. În acest caz, beneficiarul trebuie să efectueze o evaluare a riscurilor, pentru a identifica cerințele de securitate suplimentare care trebuie puse în aplicare ca parte a procesului de acreditare în materie de securitate. Beneficiarul oferă autorității care acordă grantul și, atunci când se impune prin actele cu putere de lege și normele administrative naționale, AAS competente, o declarație de conformitate care certifică faptul că SIC al beneficiarului și interconexiunile aferente au fost acreditate pentru gestionarea IUEC la nivelul RESTREINT UE/EU RESTRICTED.

27. Accesul la distanță de la alte sisteme la servicii LAN (de exemplu, acces la distanță la e-mail și asistență la distanță pentru sistem) este interzis, cu excepția cazului în care măsuri de securitate speciale sunt puse în aplicare și acceptate de autoritatea care acordă grantul și, atunci când acest lucru se impune prin actele cu putere de lege și normele administrative naționale, aprobate de AAS competentă.

Gestionarea configurației

28. O configurație detaliată a elementelor hardware și software, astfel cum se prevede în documentația de acreditare/aprobare (inclusiv diagrame ale sistemului și rețelei) trebuie să fie disponibilă și verificată periodic.

29. Ofițerul de securitate al beneficiarului trebuie să efectueze controale ale configurației cu privire la elementele hardware și software, pentru a se asigura că nu au fost introduse elemente hardware sau software neautorizate.

30. Modificările aduse configurației SIC al beneficiarului trebuie evaluate din punctul de vedere al implicațiilor lor pentru securitate și trebuie aprobate de ofițerul de securitate și, atunci când acest lucru se impune prin actele cu putere de lege și normele administrative naționale, de AAS.

31. Sistemul trebuie scanat cel puțin trimestrial pentru a fi detectate eventuale vulnerabilități la nivelul securității. Trebuie instalat și actualizat un software de detectare a programelor malware. Dacă este posibil, acest software ar trebui să dețină o aprobare națională sau o aprobare internațională recunoscută ori ar trebui să fie un standard industrial acceptat la scară largă.

32. Beneficiarul trebuie să elaboreze un plan de asigurare a continuității activității. Trebuie stabilite proceduri de rezervă pentru a aborda următoarele aspecte:

(a) frecvența creării copiilor de rezervă;

(b) cerințele de stocare la fața locului (containere ignifuge) sau în exterior;

(c) controlul accesului autorizat la copii de rezervă.

Sanitizare și distrugere

33. În cazul SIC sau al mediilor de stocare a datelor care au deținut în orice moment informații RESTREINT UE/EU RESTRICTED trebuie efectuată următoarea sanitizare a întregului sistem sau a mediului de stocare înainte de eliminare:

    (a) memoria flash (de exemplu, unități flash pentru USB, carduri SD, unități solid state, harddiskuri hibride) trebuie suprascrise de cel puțin trei ori și, ulterior, verificate pentru a se asigura că respectivul conținut inițial nu poate fi recuperat sau trebuie șterse folosind un software de ștergere aprobat;

    (b) mediile magnetice (de exemplu, harddiskurile) trebuie suprascrise sau demagnetizate;

    (c) mediile optice (de exemplu, CD-uri sau DVD-uri) trebuie distruse sau dezintegrate;

    (d) pentru orice alt mediu de stocare, autoritatea care acordă grantul sau, după caz, ANS, ASD sau AAS ar trebui consultată cu privire la cerințele de securitate care trebuie respectate.

34. Informațiile clasificate RESTREINT UE/EU RESTRICTED trebuie sanitizate pe orice mediu de stocare a datelor înainte de transmiterea către orice entitate care nu este autorizată să acceseze informații clasificate RESTREINT UE/EU RESTRICTED (de exemplu, pentru lucrări de întreținere).

ANEXA IV

Autorizarea de securitate industrială și autorizarea de securitate a personalului care sunt acordate beneficiarilor sau subcontractanților și care implică informații RESTREINT UE/EU RESTRICTED și ANS/ASD care trebuie notificate cu privire la acordurile de grant clasificate la nivelul RESTREINT UE/EU RESTRICTED ([1])

Statul membru	ASI		Notificarea ANS și/sau ASD privind un acord de grant sau un subcontract care implică informații clasificate R-UE/EU-R		ASP	
	DA	NU	DA	NU	DA	NU
Belgia		**X**		**X**		**X**
Bulgaria		**X**		**X**		**X**
Cehia		**X**		**X**		**X**
Danemarca	**X**		**X**		**X**	
Germania		**X**		**X**		**X**
Estonia	**X**		**X**			**X**
Irlanda		**X**		**X**		**X**
Grecia	**X**			**X**	**X**	
Spania		**X**	**X**			**X**
Franța		**X**		**X**		**X**
Croația		**X**	**X**			**X**
Italia		**X**	**X**			**X**
Cipru		**X**	**X**			**X**
Letonia		**X**		**X**		**X**
Lituania	**X**		**X**			**X**
Luxemburg	**X**		**X**		**X**	
Ungaria		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Țările de Jos	**X** (numai pentru acordurile de grant și subcontractele din domeniul apărării)		**X** (numai pentru acordurile de grant și subcontractele din domeniul apărării)			**X**
Austria		**X**		**X**		**X**
Polonia		**X**		**X**		**X**

([1]) Aceste cerințe naționale privind ASI/ASP și notificările acordurilor de grant care implică informații RESTREINT UE/EU RESTRICTED nu trebuie să creeze nicio obligație suplimentară pentru alte state membre sau pentru beneficiarii și subcontractanții aflați în jurisdicția lor.
NB:Notificările privind acordurile de grant care implică informații CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET sunt obligatorii.

Portugalia		**X**		**X**		**X**
România		**X**		**X**		**X**
Slovenia	**X**		**X**			**X**
Slovacia	**X**		**X**			**X**
Finlanda		**X**		**X**		**X**
Suedia		**X**		**X**		**X**

ANEXA V

LISTA DEPARTAMENTELOR DIN CADRUL AUTORITĂȚII NAȚIONALE DE SECURITATE/AUTORITĂȚII DE SECURITATE DESEMNATE, RESPONSABILE DE PROCEDURILE DE GESTIONARE ASOCIATE CU SECURITATEA INDUSTRIALĂ

BELGIA

Autoritatea națională de securitate
Serviciul public federal Afaceri externe
Rue des Petits Carmes 15
1000 Bruxelles

Tel. +32 25014542 (Secretariat)

Fax +32 25014596

E-mail: nvo-ans@diplobel.fed.be

BULGARIA

1. Comisia de stat privind securitatea informațiilor – Autoritatea națională de securitate
   4 Kozloduy Street
   1202 Sofia
   Tel. +359 29835775
   Fax +359 29873750
   E-mail: dksi@government.bg

2. Serviciul de informații în materie de apărare din cadrul Ministerului Apărării (serviciu de securitate)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel. +359 29227002
   Fax +359 29885211
   E-mail: office@iksbg.org

3. Agenția Națională de Informații (serviciu de securitate)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel. +359 29813221
   Fax +359 29862706
   E-mail: office@dar.bg

4. Agenția de stat pentru operațiuni tehnice (serviciu de securitate)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel. +359 29824971
   Fax +359 29461339
   E-mail: dato@dato.bg

(Autoritățile competente enumerate mai sus desfășoară procedurile de verificare pentru eliberarea de ASI pentru entitățile juridice care le solicită în vederea încheierii unui contract clasificat și de ASP pentru persoane fizice care pun în aplicare un contract clasificat pentru a răspunde nevoilor autorităților respective.)

5. Agenția națională de securitate (serviciu de securitate)

   45 Cherni Vrah Blvd.
   1407 Sofia

   Tel. +359 28147109

   Fax +359 29632188, +359 28147441

   E-mail: dans@dans.bg

(Serviciul de securitate menționat mai sus desfășoară procedurile de verificare pentru eliberarea de ASI și ASP pentru toate celelalte entități juridice și persoane fizice din țară, care solicită autorizările respective pentru a încheia un contract clasificat sau un acord de grant clasificat sau care pun în aplicare un contract clasificat sau un acord de grant clasificat.)

CEHIA

Autoritatea națională de securitate
Departamentul de securitate industrială
PO BOX 49
150 06 Praha 56

Tel. +420 257283129

E-mail: sbr@nbu.cz

DANEMARCA

1. Politiets Efterretningstjeneste
   (Serviciul Danez de Informații de Securitate)

   Klausdalsbrovej 1

   2860 Søborg

   Tel. +45 33148888

   Fax +45 33430190

2. Forsvarets Efterretningstjeneste
   (Serviciul Danez de Informații de Apărare)
   Kastellet 30
   2100 Copenhagen Ø

   Tel. +45 33325566

   Fax +45 33931320

GERMANIA

1. Pentru aspecte care privesc politica de securitate industrială, ASI, planurile de transport (cu excepția elementelor criptografice/CCI):
   Ministerul Federal al Afacerilor Economice și Energiei

   Departamentul de securitate industrială - RS3

   Villemombler Str. 76

   53123 Bonn

   Tel. +49 228996154028

   Fax +49 228996152676

   E-mail: dsagermany-rs3@bmwi.bund.de (adresa de e-mail a biroului)

2. Pentru cereri de vizită standard din partea societăților germane/la societăți germane:

Ministerul Federal al Afacerilor Economice și Energiei

Departamentul de securitate industrială – RS2
Villemombler Str. 76
53123 Bonn

Tel. +49 228996152401

Fax +49 228996152603

E-mail: rs2-international@bmwi.bund.de (adresa de e-mail a biroului)

3. Planuri de transport pentru materiale criptografice:

Biroul federal pentru securitatea informațiilor (BSI)
Agenția Națională de Distribuție/NDA-EU DEU
Mainzer Str. 84
53179 Bonn

Tel. +49 2289995826052

Fax +49 228991095826052

E-mail: NDAEU@bsi.bund.de

ESTONIA

Departamentul Autorității Naționale de Securitate
Serviciul eston de informații externe
Rahumäe tee 4B
11316 Tallinn

Tel. +372 6939211

Fax +372 6935001

E-mail: nsa@fis.gov.ee

IRLANDA

Autoritatea națională de securitate din Irlanda
Departamentul de Afaceri Externe și Comerț
76-78 Harcourt Street
Dublin 2
D02 DX45

Tel. +353 14082724

E-mail: nsa@dfa.ie

GRECIA

Personalul general de apărare națională a Greciei
Unitatea E' (Security INTEL, CI BRANCH)
Direcția E3
Biroul de securitate industrială
227-231 Mesogeion Avenue
15561 Holargos, Atena

Tel. +30 2106572022, +30 2106572178

Fax +30 2106527612

E-mail: daa.industrial@hndgs.mil.gr

SPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tel. +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

E-mail: nsa-sp@areatec.com

Pentru informații privind programele clasificate: programas.ons@areatec.com

Pentru chestiuni legate de autorizările de securitate ale personalului: hps.ons@areatec.com

Pentru planuri de transport și vizite internaționale: sp-ivtco@areatec.com

FRANȚA

Autoritatea națională de securitate (ANS) (pentru politici și pentru punere în aplicare în alte domenii decât industria de apărare)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel. +33 171758193

Fax +33 171758200

E-mail: ANSFrance@sgdsn.gouv.fr

Autoritatea de securitate desemnată (pentru punere în aplicare în industria de apărare)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15

Tel. +33 988670421

E-mail: pentru formulare și pentru cereri de vizită trimise: dga-ssdi.ai.fct@intradef.gouv.fr

pentru cereri de vizită primite: dga-ssdi.visit.fct@intradef.gouv.fr

CROAȚIA

Biroul Consiliului Național de Securitate
ANS din Croația
Jurjevska 34
10000 Zagreb

Tel. +385 14681222

Fax +385 14686049

E-mail: NSACroatia@uvns.hr

ITALIA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna 15
00187 Roma

Tel. +39 0661174266

Fax +39 064885273

CIPRU

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

E-mail: cynsa@mod.gov.cy

Ministerul Apărării
Autoritatea națională de securitate (ANS)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Tel. +357 22807569, +357 22807764

Fax +357 22302351

E-mail: cynsa@mod.gov.cy

LETONIA

Autoritatea națională de securitate
Biroul de protecție a Constituției din Republica Letonia
P.O. Box 286
Riga LV-1001

Tel. +371 67025418, +371 67025463

Fax +371 67025454

E-mail: ndi@sab.gov.lv, ndi@zd.gov.lv

LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Comisia de coordonare a protecției secretelor din Republica Lituania)
Autoritatea națională de securitate
Pilaitės pr. 19
LT-06264 Vilnius

Tel. +370 70666128

E-mail: nsa@vsd.lt

LUXEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxemburg

Tel. +352 24782210

E-mail: ans@me.etat.lu

UNGARIA

Autoritatea națională de securitate din Ungaria
H-1399 Budapesta P.O. Box 710/50
H-1024 Budapesta, Szilágyi Erzsébet fasor 11/B

Tel. +36 13911862

Fax +36 13911889

E-mail: nbf@nbf.hu

MALTA

Direcția de standardizare
Autoritatea de securitate desemnată pentru securitatea industrială
Institutul de standarde și metrologie
Autoritatea pentru aspecte legate de concurență și consumatori din Malta
Mizzi House
National Road
Blata I-Bajda HMR9010

Tel. +356 23952000

Fax +356 21242406

E-mail: certification@mccaa.org.mt

ȚĂRILE DE JOS

1. Ministerul de Interne și Relații ale Regatului

   PO Box 20010
   2500 EA Haga

   Tel. +31 703204400

   Fax +31 703200733

   E-mail: nsa-nl-industry@minbzk.nl

2. Ministerul Apărării

   Departamentul de securitate industrială

   PO Box 20701
   2500 ES Haga

   Tel. +31 704419407

   Fax +31 703459189

   E-mail: indussec@mindef.nl

AUSTRIA

1. Cancelaria Federală a Austriei

   Departamentul I/10, Biroul federal pentru securitatea informațiilor

   Ballhausplatz 2
   10104 Viena

   Tel. +43 153115202594

   E-mail: isk@bka.gv.at

2. ASD în sfera militară:

   BMLV/Abwehramt

   Postfach 2000
   1030 Viena

   E-mail: abwa@bmlvs.gv.at

POLONIA

Agenția de Securitate Internă
Departamentul pentru protecția informațiilor clasificate
Rakowiecka 2A
00-993 Varșovia

Tel. +48 225857944

Fax +48 225857443

E-mail: nsa@abw.gov.pl

PORTUGALIA

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisabona

Tel. +351 213031710

Fax +351 213031711

E-mail: sind@gns.gov.pt, franco@gns.gov.pt

ROMÂNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
ANS din România – ORNISS – Oficiul Registrului Național al Informațiilor Secrete de Stat
Str. Mureș nr. 4
012275 București

Tel. +40 212075115

Fax +40 212245830

E-mail: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel. +386 14781390

Fax +386 14781399

E-mail: gp.uvtp@gov.si

SLOVACIA

Národný bezpečnostný úrad
(Autoritatea națională de securitate)
Departamentul pentru autorizări de securitate
Budatínska 30
851 06 Bratislava

Tel. +421 268691111

Fax +421 268691700

E-mail: podatelna@nbu.gov.sk

FINLANDA

Autoritatea națională de securitate
Ministerul Afacerilor Externe
P.O. Box 453
FI-00023 Government

E-mail: NSA@formin.fi

SUEDIA

1. Autoritatea națională de securitate

   Utrikesdepartementet (Ministerul Afacerilor Externe)
   UD SÄK / NSA
   SE-103 39 Stockholm
   Tel. +46 84051000
   Fax +46 87231176
   E-mail: ud-nsa@gov.se

2. ASD

   Försvarets Materielverk (Administrația materialelor de apărare din Suedia)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel. +46 87824000
   Fax +46 87826900
   E-mail: security@fmv.se