

DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE
DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ

**REGLEMENTAREA
ACCESULUI LA INFORMAȚII
CLASIFICATE ȘI OBȚINEREA
CERTIFICATELOR DE
SECURITATE**

studiu documentar

martie 2026

Lucrările elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților. Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă. Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:

<http://www.cdep.ro/infoparl/dip.studii?par1=2021>

Documentare și sinteză: Aurora Trănescu

Consilier parlamentar, Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

INTRODUCERE	4
AUSTRIA	5
FRANȚA	7
GERMANIA.....	9
IRLANDA	12
ITALIA.....	15
OLANDA (REGATUL ȚĂRILOR DE JOS)	17
POLONIA.....	19
PORTUGALIA	21
STATELE UNITE ALE AMERICII	23
UNGARIA	25
WEBOGRAFIE	27

INTRODUCERE

În Uniunea Europeană, autorizările sau certificatele de securitate sunt emise de statele membre. UE stabilește însă reguli comune minime, pentru a permite cooperarea și recunoașterea mutuală. Modelul UE prevede emitere națională, armonizare europeană și recunoaștere funcțională, nu automată.

[Decizia \(UE\) 2015/444 privind normele de securitate pentru protecția informațiilor clasificate ale UE \(EUCI\)](#) este actul normativ central în domeniu. Aceasta este documentul-cheie pentru toate instituțiile UE și proiectele finanțate sau coordonate la nivel UE. Decizia stabilește politica UE de securitate a informațiilor, impune obligativitatea autorizațiilor de securitate pentru acces la EUCI și reglementează cooperarea între statele membre. Decizia definește totodată cele patru niveluri de clasificare UE:

- **EU top secret** – informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii deosebit de grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- **EU secret** – informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- **EU confidential** – informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;
- **EU restricted** – informații și materiale a căror divulgare neautorizată ar putea fi în defavoarea intereselor Uniunii Europene sau ale unuia ori mai multor state membre.

Aceste niveluri de secretizare corespund, în linii mari, și cu cele existente la nivel NATO.

Dintre statele cuprinse în studiu, o serie precum Austria, Italia, Polonia și Portugalia au definite în legislație aceleași patru niveluri de clasificare ca în UE și NATO: top secret, secret, confidențial, restricționat. În cazul altor state există trei niveluri de clasificare și aici se încadrează Germania, Olanda, Ungaria, precum și Statele Unite ale Americii. Irlanda – care nu este membră NATO – se încadrează și ea în categoria țărilor cu trei niveluri de clasificare. Franța, pe de altă parte, are definite numai două niveluri de secretizare, anume *secret* și *très secret*.

Statele membre ale UE reglementează domeniul prin legi proprii precum și prin alte regulamente specifice și/sau acte normative de aplicare (există similarități între dispozițiile oficiale și modul de aplicare din țări diferite). Modul de procesare a certificatelor de securitate este foarte asemănător sistemului european și în Statele Unite ale Americii.

În toate statele prezentate în studiu, certificatele de securitate (*clearance*) nu pot fi solicitate de persoane fizice, ci numai de entități juridice, fie autorități publice, fie entități private cum ar fi firme specializate în tehnologie militară, care au nevoie de acces la informații clasificate pentru anumite persoane din structura lor. În cazul tuturor acestora, un aspect fundamental

care se analizează este necesitatea de a cunoaște respectivele informații (termenul consacrat în limba engleză fiind *need to know*).

Un alt aspect comun privește etapele care trebuie parcurse pentru a obține certificatul de securitate. În linii mari, acestea implică completarea de către candidat a unui chestionar detaliat, după care urmează etapa de investigații desfășurate de către serviciile de resort. De regulă, investigațiile sunt întreprinse de servicii diferite pentru domeniul civil de cel militar. Urmează etapa decizională în care organismul competent al statului emite avizul favorabil/nefavorabil. În caz de aviz favorabil, persoana în cauză semnează documentul de certificare și este instruită cu privire la responsabilitățile sale.

Cât privește durata etapelor de verificare ori a întregului proces în ansamblu, acestea nu sunt stabilite prin legi în majoritatea statelor. Ele sunt flexibile în general, pentru ca există o priorizare a calității investigațiilor versus viteza procesului¹. Ceea ce este definit totuși sunt ținte de performanță administrativă ale serviciilor care instrumentează procesul. În general, nici acestea nu sunt rigide. Ca exemplu, ele sunt formulate de felul „90% dintre cereri sunt procesate în X de zile”, sintagmă care permite tratarea diferită a cazurilor speciale.

Printre excepții sunt Olanda, Polonia și Ungaria, țări în care sunt definite prin articole de legi duratele prestabilite pentru procesare – de circa 2-3 luni. Există însă în aceleași legi și articole privind clauze de prelungire a termenelor fixe, ceea ce asigură gradul de flexibilitate necesar.

De asemenea, atunci când un stat solicită informații din alt stat, termenul de procesare se suspendă până la primirea documentelor de peste hotare.

Mai multe state europene prevăd în legislația lor de securitate posibilitatea acordării autorizațiilor temporare de securitate pentru acces la informații clasificate, până la finalizarea verificărilor complete. Acestea sunt utilizate în special pentru posturi urgente din apărare, la NATO (în structura administrativă) sau în industria/industriile de securitate.

ASPECTE COMPARATIVE

AUSTRIA

Ca și în alte țări, și în Austria este necesar un document oficial de securitate care să ateste dreptul unei persoane sau entități de a avea acces la informații clasificate. Accesul este condiționat de o verificare de securitate, urmată de autorizarea accesului la nivelul de clasificare solicitat.

¹ Sursele pentru durate de sunt obținute în general din rapoartele de activitate ale instituțiilor de resort. Răspunsurile guvernelor la interpelări parlamentare sunt o altă sursă de informații.

[Legea privind securitatea informațiilor](#) reglementează protecția informațiilor clasificate naționale și UE/NATO, stabilește condițiile de acces pentru persoane și entități și prevede obligativitatea autorizăției de securitate (*security clearance*).

Verificările și autorizările sunt centralizate la nivel de stat federal și sunt realizate de [Direcția pentru securitate a statului \(DSN\)](#) din cadrul Ministerului de Interne, în prezent structurile succesoare ale BVT² fostul Serviciu austriac de informații interne și combatere a terorismului, acum reorganizat.

Austria folosește niveluri de clasificare compatibile UE/NATO:

- *restricted*
- *confidential*
- *secret*
- *top secret*

Accesul este permis doar până la nivelul autorizat și doar pe principiul *need to know*.

Autorizația de securitate este obligatorie (în aceleași situații ca și în România) pentru funcționari publici, personal militar, contractori privați care lucrează cu statul, proiecte UE, NATO, apărare, infrastructură critică.

Firmele trebuie să fie certificate ca entitate, iar personalul lor este verificat individual.

Ca și în România, procedura de obținere a unui certificat de securitate este inițiată de o instituție publică, autoritate contractantă sau un angajator privat în calitate sa de contractor al statului, UE ori NATO. Aplicând strict principiul „need to know”, angajatorul stabilește nivelul de clasificare necesar.

Persoana vizată completează și furnizează, prin angajator documentele de bază, anume formular de verificare de securitate extins, copie act de identitate/ pașaport, CV detaliat, declarație pe propria răspundere privind antecedente penale, situația financiară, contacte externe relevante și cazier judiciar austriac iar dacă e cazul, și din alte state.

În funcție de nivelul de securitate solicitat, pot fi necesare documente suplimentare precum declarații privind șederi îndelungate în străinătate, informații despre membrii apropiați ai familiei, consimțământ scris pentru verificări extinse.

Verificările sunt realizate de structurile de securitate ale Ministerului de Interne și alte autorități precum poliție, registre financiare și altele, după caz.

² Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

Duratele aproximative de realizare a verificărilor depind de nivelul de acces solicitat:

Nivel de acces	Durata tipică
Restricted	3–6 săptămâni
Confidential	1–3 luni
Secret	3–6 luni
Top Secret	6–9 luni (uneori > 9 luni)

Termenele nu au o durată fixată prin lege, ci pot crește în caz de verificări internaționale, perioade petrecute în afara UE ori informații care necesită clarificări.

Autorizația de securitate are o valabilitate limitată în timp, de regulă 3–5 ani și este legată de funcție și angajator. Reînnoirea urmează o procedură similară, care de regulă este mai scurtă dacă nu au apărut riscuri noi.

FRANȚA

În Franța, cadrul legal pentru [protecția secretului apărării naționale](#) și acordarea certificatelor de securitate³ a fost profund reformat începând cu anul 2021.

Sistemul francez este centralizat și extrem de riguros, fiind coordonat de Secretariatul General al Apărării și Securității Naționale (SGDSN), care se află în subordinea primului ministru.

[Instrucțiunea generală interministerială nr. 1300 privind protecția secretului apărării naționale \(IGI 1300\)](#)⁴ este actul normativ principal în privința informațiilor clasificate în Franța. Acesta definește întreaga organizare a protecției secretului apărării naționale, reglementează nivelurile de clasificare, procedura de autorizare, măsurile de securitate fizică și informatică, precum și sancțiunile în caz de compromitere. Versiunea intrată în vigoare în 2021 a simplificat nivelurile de secretizare, Franța trecând de la un sistem cu trei niveluri la unul mai simplificat pentru a exista o mai buna corespondență cu standardele NATO și UE:

- secret (secret) - informații a căror divulgare ar putea afecta grav apărarea națională;
- foarte secret (très secret) - informații de o importanță vitală; adesea necesită compartimentări speciale (ex: nuclear, BURAN⁵).

³ Lb. fr.: *habilitations*

⁴ Lb. fr.: *Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale*

⁵ Bureau des enquêtes administratives de sécurité nationale

IGI 1300 conține reguli stricte pentru sistemele informatice care procesează date clasificate, incluzând măsuri de securitate fizică și logică (cifrare, control acces), punând un accent sporit pe securitatea informațiilor digitale și pe analiza riscurilor pentru site-urile care dețin ISC.

[Codul apărării](#) oferă baza legală superioară. Articolele relevante, în special L. 2311-1 și următoarele, respectiv R. 2311-1, stabilesc cadrul juridic pentru ceea ce constituie un secret al apărării naționale, responsabilitățile miniștrilor în protejarea acestor informații și categoriile de persoane care pot fi supuse verificărilor de securitate.

[Codul penal](#) stabilește pedepsele pentru încălcarea secretului de stat. Articolele 413-9 la 413-12 definesc infracțiunea de compromitere a secretului apărării naționale. Pedepsa poate ajunge la 7 ani de închisoare și 100.000 € amendă.

Spre deosebire de SUA de exemplu, unde procesul poate fi uneori mai transparent în ceea ce privește motivele de respingere, dreptul de apel fiind bine reglementat, în Franța, decizia de a refuza un certificat de securitate este un act administrativ care adesea invocă „motive de siguranță națională”, fiind mult mai dificil de contestat pe fond în instanțele civile.

În Franța, procesul de acordare a certificatului de securitate fiind unul dintre cele mai riguroase din Europa, este centrat pe conceptul de „investigație de integritate”. Procedura este reglementată de instrucțiunea [IGI 1300](#) și se desfășoară în patru etape principale, implicând atât angajatorul, cât și serviciile de informații:

- Candidatul completează un formular extrem de detaliat⁶, care include date despre starea civilă, reședințe anterioare, parcurs educațional și profesional, dar și detalii despre membrii familiei și contactele străine. Angajatorul transmite dosarul către autoritatea de securitate competentă ministerul de resort sau serviciul de informații.
- Investigația este partea critică a procesului. Verificările sunt efectuate de **DGSI** (Securitate Internă) – pentru civili și sectorul privat strategic și de **DRSD** (Informații de Apărare) – pentru personalul militar și contractanții apărării. Aceștia verifică antecedentele judiciare prin consultarea fișierelor de poliție și jandarmerie, vulnerabilitățile prin situația financiară (risc de corupție), anturajul, comportamentele care ar putea expune persoana la șantaj (dependențe, loialități duble). În caz de dubii sau pentru niveluri înalte (*très secret*), candidatul poate fi chemat la un interviu față în față cu un ofițer de informații.
- Etapa decizională: serviciul de informații emite un aviz favorabil sau nefavorabil, dar decizia finală aparține autorității de abilitare⁷. În caz de aviz favorabil se emite certificatul de securitate. În caz de aviz nefavorabil: accesul la informații clasificate este refuzat. În Franța, autoritatea nu este obligată să detalieze motivele refuzului dacă acestea țin de siguranța națională, protecția surselor sau a metodelor de investigație.

⁶ similar cu formularul SF-86 din SUA

⁷ Pentru nivelul secret aceasta este ministrul sau delegatul acestuia, iar pentru nivelul tres secret decizia este luată de premier sau SGDSN.

- Procesul-verbal de luare la cunoștință este semnat de persoana abilitată. Acesta confirmă că persoana a fost instruită cu privire la responsabilitățile sale legale și la sancțiunile penale în caz de divulgare. Abilitarea nu este permanentă; ea are o durată de validitate, de regulă 5 ani pentru nivelul *secret*, după care trebuie reînnoită.

Spre deosebire de alte proceduri administrative, duratele etapelor pentru obținerea unui certificat de securitate nu sunt reglementate prin termene legale stricte, adică nu există o lege care să spună că investigația *trebuie* să fie finalizată într-un termen fix. Sistemul francez prioritizează securitatea în fața celerității. Totuși, există **durate orientative de referință** stabilite prin directive interne ale serviciilor de informații (DGSI/DRSD) și prin obiectivele de performanță ale Ministerului Apărării.

Nivel	Durata totală a verificărilor
secret	2-4 luni
très secret	6-9 luni

De menționat că în dreptul administrativ francez general, lipsa unui răspuns timp de 2 luni echivalează cu un acord. Dar această regulă nu se aplică la certificatele de securitate.

În Franța nu se poate obține un acces temporar. Până la finalizarea investigației, accesul (la informații sensibile) este strict interzis. Dacă o companie privată lucrează pe un contract clasificat, nu doar angajații trebuie abilitați, ci și sediul firmei trebuie să obțină o *abilitare de persoană juridică*, care implică măsuri stricte de securitate fizică cum ar fi seifuri, zone de acces restricționat.

Utilizarea unui certificat de securitate obținut pentru o anumită misiune în scopuri personale sau la un alt loc de muncă este strict interzisă; abilitarea este legată de funcția specifică ocupată la momentul respectiv.

GERMANIA

În Germania, sistemul de verificare a securității este unul dintre cele mai bine reglementate și transparente din Europa, fiind guvernat de un act normativ central și de regulamentele de aplicare ale acestuia. În proces, se pune un accent deosebit pe echilibrul dintre securitatea statului și drepturile individuale (protecția datelor).

Spre deosebire de Franța – unde baza este instrucțiunea ministerială IGI 1300 – Germania are o lege federală votată prin procedură parlamentară, care oferă garanții juridice clare.

[Legea privind verificarea de securitate](#) (SÜG) este sursa juridică supremă și reglementează: cine trebuie verificat, ce date pot fi colectate și cum trebuie stocate precum și drepturile persoanei verificate (inclusiv dreptul la informare). De asemenea, stabilește cele trei niveluri de verificare:

- confidențial: verificare de bază: cazier, baze de date de poliție/intelligence;
- secret: include verificarea referințelor, a foștilor angajatori și a situației financiare;
- strict secret: investigație de teren: interviuri cu vecini, prieteni și verificarea detaliată a partenerului de viață.

Legea prevede la art. 5 și alternativa ca în cazuri excepționale, persoanei în cauză să i se încredințeze o activitate sensibilă înainte de finalizarea autorizării de securitate, dacă autoritatea a evaluat informațiile din declarația de securitate sau dacă în cadrul autorizărilor nu au existat indicii privind un risc de securitate ca urmare a acestui fapt.

[Regulamentul de punere în aplicare a SÜG](#) detaliază aspectele tehnice și administrative cum ar fi formularele utilizate (chestionarele de securitate), procedurile specifice pentru verificarea soților sau partenerilor de viață, cooperarea dintre autoritățile federale și cele ale statelor federale (*Länder*).

[Instrucțiunile administrative generale \(SÜGVWV\)](#) sunt ghiduri interne pentru funcționari, care asigură că legea este aplicată unitar în toate ministerele și agențiile. Ele conțin criteriile de evaluare a riscurilor (de exemplu, ce sumă de datorii este considerată un risc de șantaj).

În Germania, verificarea este o colaborare între angajator și serviciul de informații interne:

- **BfV**⁸: Oficiul Federal pentru Protecția Constituției este agenția care efectuează investigația propriu-zisă la nivel federal.
- **LfV**⁹: Omologii de la nivel de stat (*Länder*), dacă persoana lucrează pentru o autoritate regională.
- **MAD**¹⁰: Serviciul de contrainformații militare, pentru personalul din cadrul armatei.

Cât privește protecția datelor (GDPR), Germania este extrem de strictă. SÜG prevede clar că datele colectate pentru clearance **nu pot fi folosite în alte scopuri** (de exemplu, pentru o anchetă penală separată), decât în condiții extrem de limitate.

Pentru nivelurile secret și strict secret, partenerul de viață (soț/soție sau partener coabitant) trebuie să își dea consimțământul scris pentru a fi verificat. Dacă partenerul refuză, solicitantul, de regulă, nu poate obține clearance-ul.

Înainte de a respinge un clearance, autoritatea este obligată de lege să ofere solicitantului posibilitatea de a clarifica personal suspiciunile (cu excepția cazului în care acest lucru ar periclita siguranța statului sau sursele).

⁸ Bundesamt für Verfassungsschutz

⁹ Landesämter für Verfassungsschutz

¹⁰ Militärischer Abschirmdienst

La fel ca în majoritatea sistemelor, un cetățean nu poate solicita un certificat în nume personal. Angajatorul, adică instituția publică sau compania privată implicată în proiecte clasificate, determină că postul respectiv necesită acces la informații de nivel confidențial, secret sau strict secret. O particularitate în Germania este **consimțământul scris** al persoanei care este obligatoriu pentru a începe verificarea. Apoi, candidatul primește un chestionar complex. Există două tipuri principale, în funcție de nivelul de verificare:

- nivel confidențial și secret: se solicită date personale, istoricul locuințelor, al locurilor de muncă și al călătoriilor;
- nivel strict secret: se solicită informații mult mai intime, inclusiv despre partenerul de viață care trebuie, de asemenea, să semneze formularul de consimțământ și referințe personale (prietenii, mentori).

Dosarul este trimis către **BfV** (Oficiul Federal de Protecție a Constituției) care verifică:

- bazele de date: cazierul judiciar, registrul central al străinilor, bazele de date ale poliției și ale altor servicii de informații;
- referințele (doar la Ü3): ofițerii BfV pot contacta persoanele indicate ca referințe pentru a verifica moralitatea și stilul de viață al candidatului;
- interviul de securitate: spre deosebire de SUA, unde interviul este aproape standard, în Germania acesta are loc de obicei doar dacă apar neconcordanțe sau „pete” în biografie care necesită clarificare.

BfV nu acordă certificatul, ci emite un aviz de securitate. Dacă nu există rezerve, serviciul transmite un aviz favorabil către „autoritatea de securitate” a angajatorului. Dacă există suspiciuni (ex: datorii mari, dependențe, legături cu organizații extremiste), se analizează dacă acestea constituie un risc de securitate.

Autoritatea administrativă (ministerul sau agenția) emite decizia de abilitare care poate fi pozitivă, ceea ce înseamnă că persoana primește acces și este instruită cu privire la manipularea documentelor; sau negativă caz în care persoana este informată despre refuz. În Germania, spre deosebire de Franța, autoritatea este obligată să motiveze refuzul, astfel încât persoana să se poată apăra – cu excepția cazului în care motivarea ar deconspira metode de intelligence.

Cât privește duratele de procesare, nu există termene legale stricte însă timpii medii sunt relativ predictibili:

- confidențial: 2-4 luni;
- secret: 4-6 luni;
- strict secret: 6-12 luni¹¹.

¹¹ Sursele pentru duratele de procesare sunt mult mai transparente în cazul Germaniei, deoarece **BfV** (Serviciul Federal de Protecție a Constituției) și Ministerul Federal de Interne (BMI) raportează periodic aceste date către Bundestag (Parlament). BfV publică anual un [Raport de activitate](#). În secțiunea dedicată „Protecției

În Germania, certificatele sunt supuse unei revizuii periodice. De regulă, la fiecare 10 ani se face o verificare completă. Între aceste intervale, se pot face verificări de actualizare dacă persoana își schimbă funcția sau apar indicatori de risc.

IRLANDA

Sistemul de verificare al securității din Irlanda¹² este ușor diferit față de modelele centralizate din alte țări. În Irlanda, nu există o singură lege a informațiilor clasificate care să acopere totul, ci reglementările sunt împărțite între protecția infrastructurii critice, verificările pentru personalul care lucrează cu persoane vulnerabile și procedurile administrative ale forțelor de apărare și poliției.

[Legile din 2012-2016 privind Biroul Național de Verificare \(copii și persoane vulnerabile\)](#), deși la bază se referă la protecția minorilor și a persoanelor vulnerabile, reprezintă **cea mai utilizată bază legală** pentru verificările de antecedente în Irlanda. Legile reglementează modul în care Poliția Națională furnizează informații despre cazier și așa numitele *informații de siguranță* angajatorilor. Procesul de verificare trebuie să fie întotdeauna inițiat de o entitate înregistrată, angajatorul sau o agenție guvernamentală, care va trimite un link prin e-mail persoanei verificate pentru a completa formularul online pe portalul [Biroului Național de Verificare](#) (NVB).

[Legea poliției naționale nr. 20/2005](#) oferă cadrul general pentru funcționarea poliției și îi conferă acesteia autoritatea de a efectua verificări de securitate în interesul siguranței statului. Pe baza acestei legi, Unitatea de informații a poliției¹³ efectuează ceea ce se numește *National Security Vetting (NSV)* pentru funcționarii publici sau angajații din sectoare strategice.

[Legea secretelor de stat nr. 1/1963](#) este legea care definește infracțiunile legate de divulgarea informațiilor oficiale și a secretelor de stat. Deși nu descrie procedura de *clearance* pas cu pas, ea stabilește obligația legală a oricărei persoane care ocupă o funcție publică sau un contract cu statul de a fi verificată și de a semna angajamente de confidențialitate.

Informațiilor și Securității Economice”, serviciul indică numărul de solicitări procesate și, periodic, timpii medii de răspuns.

Răspunsurile Guvernului Federal la [Interpelări Parlamentare](#) (Kleine Anfragen) sunt o altă sursă de informații, întrucât deputații din Bundestag adresează frecvent întrebări scrise guvernului cu privire la eficiența SÜG.

¹² *Garda Vetting* sau *National Security Vetting*

¹³ *Garda National Crime & Security Intelligence Service*

Spre deosebire de sistemele NATO standardizate, Irlanda nefiind membră NATO, utilizează un sistem propriu, adesea coordonat de [Biroul National de Verificare](#) din cadrul Poliției naționale:

- *Garda Vetting*: verificarea standard a cazierului este cea mai comună;
- *National Security Vetting (NSV)*: un proces mult mai riguros, utilizat pentru: personalul din forțele de apărare, angajații din biroul prim-ministrului și Departamentul de Afaceri Externe, accesul la infrastructura critică (aeroporturi, securitate cibernetică guvernamentală).

În Irlanda, pentru contractele ce implică instituții UE – precum Eurofound, care are sediul la Dublin – se pot aplica reglementările europene, dar verificarea de teren este efectuată tot de autoritățile irlandeze sub egida legislației naționale menționate mai sus.

National Security Vetting (NSV) este un proces mult mai intruziv și riguros, destinat protejării intereselor vitale ale statului irlandez. NSV este conceput pentru a identifica persoanele care ar putea reprezenta un risc de spionaj, sabotaj, terorism sau care ar putea fi vulnerabile la presiuni externe (șantaj). Unitatea de informații privind criminalitatea și securitatea (*Crime & Security Intelligence Service*) este responsabilă pentru civili, funcționari guvernamentali și contractori privați. Forțele de Apărare (*J2 Intelligence Section*) este responsabilă pentru personalul militar și angajații Departamentului Apărării.

National Security Vetting (NSV) este echivalentul certificatului de securitate (*clearance*) pentru acces la informații secrete, infrastructură critică sau posturi în cadrul guvernului. Termenul estimat al verificărilor poate fi de la **3 luni la 12 luni**, întrucât legislația irlandeză nu impune un termen limită Unității de informații a poliției *Garda National Crime & Security Intelligence Service*; aceștia efectuează verificări amănunțite care includ:

- verificarea rezidenței în ultimii 10 ani;
- interviuri de securitate – pentru niveluri înalte;
- cooperarea cu agenții externe cum ar fi Interpol, Europol sau servicii naționale din alte țări.

Irlanda utilizează, în general, trei niveluri principale de NSV, în funcție de sensibilitatea informațiilor accesate:

Nivel	Destinație Tipică	Obiectul și profunzimea verificării
Level 1	Personal de aeroport, securitate cibernetică de bază.	Cazier, baze de date ale poliției, verificare istoric rezidență.

Nivel	Destinație Tipică	Obiectul și profunzimea verificării
Level 2	Funcționari în Departamente cheie (Justiție, Externe).	Include verificări financiare și ale stilului de viață.
Level 3	Acces la informații "Top Secret", Cabinetul Prim-ministrului.	Investigație de teren, interviuri cu terți, evaluare psihologică/poligraf (rar).

Procedura este mult mai complexă decât o simplă verificare de cazier:

- Solicitantul completează un formular mult mai detaliat decât cel standard, acoperind istoricul personal, adresele din ultimii 10 ani, istoricul călătoriilor și interesele financiare.
- Se verifică nu doar condamnările, ci și orice contact cu poliția sau serviciile de informații care nu s-a soldat cu proces (așa-numitul *intelligence check*).
- Pentru nivelurile superioare, se analizează solvabilitatea. Un nivel mare de îndatorare este considerat un risc major de șantaj sau corupție.
- În cazurile de nivel înalt, un ofițer de securitate va purta o discuție față în față cu candidatul pentru a clarifica eventuale neconcordanțe sau zone de risc din trecutul acestuia.

Spre deosebire de vetting-ul civil, unde se pot vedea motivele refuzului, în cazul **NSV**, dacă avizul este negativ, autoritățile pot refuza să detalieze motivele exacte din motive de siguranță națională. Există însă un mecanism de apel administrativ, dar succesul acestuia este limitat dacă informațiile provin din surse de inteligență clasificate.

Deși nu sunt precizate în lege, pentru un **NSV Level 1**, termenul realist este de **3-6 luni**, iar pentru nivelurile superioare, acesta depășește adesea **9-12 luni**.

Sistemul de [eVetting](#) prezent pe pagina web a Poliției naționale a fost conceput special pentru a asigura procesarea rapidă a cererilor de verificare. Serviciul eVetting asigură un termen de 5 zile pentru 80 % din cererile primite prin intermediul sistemului, conform țintei de performanță administrativă asumate. Procesarea electronică a solicitărilor de *clearing* poate fi urmărită [online](#) introducând numărul de înregistrare a cererii.

Un factor care suspendă termenele este rezidența în străinătate pentru persoanele care au locuit în afara Irlandei pentru o perioadă mai mare de 6 luni. Prin NSV se solicită adesea persoanei să obțină singură un cazier judiciar din țara respectivă. În consecință, procesul este pus în pauză până când documentul străin este tradus și prezentat autorităților irlandeze.

ITALIA

În Italia, sistemul de protecție a informațiilor clasificate și acordarea certificatelor de securitate (NOS¹⁴) este extrem de centralizat și bine structurat din punct de vedere juridic. Cadrul normativ italian a fost modernizat semnificativ prin legi care au vizat reforma serviciilor de informații și securitate.

[Legea nr. 124/ 2007 privind sistemul informatic pentru securitatea Republicii și noile reglementări privind secretul](#) este actul normativ fundamental care a reorganizat serviciile de informații și securitate din Italia. Această lege a fost adoptată pentru a moderniza structurile de informații, înlocuind legislația veche din 1977, într-un context internațional schimbat post-9 septembrie 2001. Legea stabilește organizarea întregului sistem de securitate națională și definește atribuțiile Departamentului de Informații de Securitate (DIS). Articolul 9 al acestei legi reglementează direct protecția secretului de stat și mecanismele de acordare a autorizațiilor de securitate. Între altele, legea a reformat comisia parlamentară de supraveghere, cunoscută acum sub numele de **COPASIR**¹⁵, oferindu-i puteri mai mari de control asupra serviciilor.

[Decretul Președintelui Consiliului de Miniștri nr. 5/ 2015](#) (DPCM) reprezintă regulamentul tehnic principal care detaliază procedurile administrative pentru obținerea, reînnoirea și revocarea certificatelor de securitate (NOS). Acesta definește clar cele patru niveluri de clasificare italiene: strict secret, secret, strict confidențial și confidențial¹⁶.

În Italia, certificatul de securitate se acordă în funcție de nivelul de acces necesar:

Nivel	Corespondent internațional	Validitate standard
Segretissimo	Top Secret	5 ani
Segreto	Secret	10 ani
Riservatissimo	Confidential	10 ani
Riservato	Restricted	10 ani

¹⁴ Lb. it.: nulla osta di sicurezza - NOS

¹⁵ Lb. It.: Comitato parlamentare per la sicurezza della Repubblica

¹⁶ Lb. it.: segretissimo, segreto, riservatissimo și riservato

[Decretul legislativ nr. 159 din 2011 \(Codul antimafia\)](#) are relevanță întrucât verificările pentru certificatele de securitate includ obligatoriu consultarea bazelor de date antimafia pentru a exclude orice tentativă de infiltrare a crimei organizate în structurile care gestionează secrete de stat.

Spre deosebire de alte țări unde fiecare minister are o autonomie mai mare, în Italia totul trece prin Departamentul de Informații de Securitate (DIS) din subordinea premierului. UCSe (Ufficio Centrale per la Segretezza) este organul tehnic din cadrul DIS care gestionează efectiv eliberarea certificatelor de securitate.

Procesul de obținere a certificării gestionat de UCSe din DIS implică etape similare cu cele din alte state:

- Candidatul completează un chestionar biografic detaliat dar spre deosebire de Germania, unde consimțământul este punctul central, în Italia procesul este declanșat exclusiv de „nevoia de a cunoaște” a administrației sau a firmei angajatoare.
- UCSe delegă verificările către serviciile de informații interne și, adesea, către carabinieri sau guardia di finanza pentru verificări de teren. sunt verificate cazierul, profilul psihologic, situația patrimonială și, foarte important în Italia, legăturile de rudenie sau asociere pentru a evita riscurile legate de criminalitatea organizată.
- Dacă investigația este pozitivă, UCSe eliberează certificatul fizic. În Italia, certificatul este transmisibil într-o anumită măsură între agenții ale aceluiași minister, dar trebuie actualizat la schimbarea angajatorului.

Dacă o companie italiană vrea să participe la licitații clasificate, aceasta trebuie să obțină Certificatul de siguranță industrială (ASI), un proces reglementat tot prin DPCM 5/2015, care implică verificarea nu doar a personalului, ci și a sediului, a sistemelor informatice și a acționariatului.

Interviul de securitate este obligatoriu pentru nivelul *top secret* și se desfășoară adesea la sediul DIS sau prin intermediul carabinieri/poliției dacă este necesară o investigație de teren mai amplă.

Italia nu publică rapoarte parlamentare la fel de detaliate precum Germania (cu tabele de zile exacte), dar conform directivelor UCSe și practicii administrative, termenele sunt:

Nivel NOS	Durata Medie	Sursa de referință
Riservato / Riservatissimo	2 - 4 luni	Practica administrativă UCSe
Segreto	4 - 7 luni	Ghidurile de Securitate Industrială
Segretissimo	6 - 12 luni	Standarde NATO/UE aplicate de DIS

Deciziile de refuz ale NOS sunt acte administrative. Ele pot fi atacate la tribunalele administrative regionale (TAR) din Lazio, însă instanțele italiene acordă o "discreționaritate tehnică" foarte largă serviciilor de informații în aceste cazuri.

OLANDA (REGATUL ȚĂRILOR DE JOS)

În Olanda, sistemul de verificare a securității și eliberarea certificatelor de securitate este unul dintre cele mai bine reglementate și transparente din Uniunea Europeană. Cadrul legal principal a suferit modificări recente, cu o nouă reformă programată să intre în vigoare la începutul anului 2026.

[Legea privind investigațiile de securitate \(1996\)](#) este pilonul central și a fost modificată pentru a oferi mai multă flexibilitate investigațiilor de securitate în sectoarele în care angajații schimbă frecvent angajatorii. Se preconizează că legea va intra în vigoare treptat, începând cu începutul anului 2026, și va fi introdusă în practică în urma consultării cu toți contribuabilii.

Legea definește ce este o „funcție confidențială”, cine trebuie verificat și care sunt criteriile de evaluare. În Olanda, autorizația de securitate nu se numește doar „clearance”, ci VGB¹⁷ adică *Declarație de fără obiecții*. Varianta amendată a acestei legi introduce un „Registru al deținătorilor de funcții confidențiale” și un certificat „legat de locație” pentru a permite angajaților din sectoare precum aviația să schimbe angajatorul fără a relua de la zero întregul proces de screening.

[Legea serviciilor de informații și securitate \(2017\)](#) reglementează competențele de investigare ale serviciilor olandeze de informații (AIVD și MIVD) și stabilește cadrul în care serviciile pot accesa bazele de date (cazier, taxe, poliție) pentru a efectua screening-ul de securitate.

[Cerințe generale de securitate pentru contracte de apărare \(ABDO 2019\)](#) reprezintă regulamentul specific pentru contractele de apărare. Acesta stabilește cerințele de securitate pentru companiile private care lucrează cu ministerul apărării. Versiunea curentă, ABDO 2019, detaliază cum trebuie protejate informațiile clasificate și ce nivel al autorizației de securitate este necesar pentru personalul industrial.

Olanda folosește un sistem designat prin litere pentru nivelurile de clasificare. Conform Legii privind investigațiile de securitate, art.6, termenul standard de procesare este de 8 săptămâni. Deși art. 6 stabilește un termen general de 8 săptămâni, în practică, complexitatea verificării variază. De regulă, Serviciul de Informații și Securitate Generală (AIVD) reușește să respecte termenul de 8 săptămâni pentru nivelurile B și C. Însă pentru nivelul A (cel mai înalt), din cauza investigațiilor aprofundate de teren și a interviurilor, se folosește aproape întotdeauna clauza de prelungire, ajungându-se la 16 săptămâni.

¹⁷ Lb. olandeza: *Verklaring van geen bezwaar*

Nivel VGB	Nivel de Clasificare	Durata Investigării (Țintă)
Nivel A	Top Secret (Staatsgeheim zeer geheim)	12 - 16 săptămâni ¹⁸
Nivel B	Secret (geheim)	8 săptămâni
Nivel C	Confidențial (vertrouwelijk)	8 săptămâni

Companiile externe trebuie să respecte Cerințele generale de securitate pentru contractele de apărare 2019 (ABDO 2019) pentru contractele de apărare clasificate și/sau vitale. ABDO 2019 se aplică numai contractelor în curs. Pentru contractele noi, se aplică, de la 1 ianuarie 2026, [Cerințele generale de securitate pentru achizițiile publice guvernamentale \(ABRO\)](#). Organizațiile au la dispoziție 2 ani pentru a introduce ABRO. Prin urmare, data intrării în vigoare diferă de la o organizație la alta. În 2026 și 2027, ABRO va fi introdus în poliție, ministere, serviciile și agențiile acestora. Ministerul Apărării utilizează ABRO pentru contractele noi. Datorită ABRO, aceleași cerințe se aplică în întregime și uniform în administrația centrală. ABRO reduce riscurile pentru securitatea națională, cum ar fi atacurile cibernetice și spionajul.

Există cerințe suplimentare de securitate pentru companiile care execută contracte publice care prezintă riscuri pentru securitatea națională. Acestea sunt incluse în ABRO. Cu ABRO, companiile beneficiază de mai multă claritate în sensul că acestea lucrează întotdeauna cu aceleași cerințe de securitate la diferite organizații guvernamentale. Nu contează dacă îndeplinesc o misiune pentru, de exemplu, un minister, o agenție sau poliție. ABRO vizează ministerele civile, agențiile guvernamentale și modul în care funcționarii publici manipulează informațiile în interiorul guvernului.

Ministerul de Interne (BZK) stabilește normele ABRO, dar nu verifică fiecare firmă în parte. El delegă această responsabilitate către ministerul care acordă contractul.

Dacă o firmă încheie un contract civil cu un minister (de exemplu, ministerul justiției sau ministerul infrastructurii), biroul de securitate sau ofițerul de securitate al acelui minister este responsabil să verifice dacă firma respectă ABRO. Ei pot face audituri la sediul firmei și verifică dacă personalul firmei are certificatele VGB necesare.

¹⁸ Din cauza reînarmării și a contractelor masive de apărare, investigațiile de nivel A (militar) pot tinde și spre limita superioară de 16-20 de săptămâni.

Serviciul de Informații și Securitate Generală (AIVD) intervine în două moduri sub umbrela ABRO:

- prin verificarea persoanelor: efectuează investigațiile pentru angajații firmei care au nevoie de acces la informații clasificate;
- prin consultanță tehnică: dacă informațiile sunt de nivel înalt, AIVD poate oferi consultanță ministerului pentru a audita sistemele IT ale firmei respective.

Spre deosebire de prevederile ABDO, unde exista o autoritatea centrală de verificare, în cazul ABRO, responsabilitatea este descentralizată. Fiecare minister este propriul său verificador pentru contractele pe care le semnează cu firmele private.

[Serviciul de Audit al Statului \(ADR\)](#) este organismul care auditează periodic ministerele. În cadrul acestor controale, ADR verifică dacă ministerele și-au monitorizat corect furnizorii privați în raport cu normele de securitate ABRO.

POLONIA

În Polonia, sistemul de protecție a informațiilor clasificate și procedura de obținere a certificatului de securitate sunt reglementate unitar, procedurile fiind mult mai centralizate decât în alte state.

[Legea privind protecția informațiilor clasificate nr.5/ 2010](#) este actul normativ fundamental care guvernează acest domeniu. Legea reglementează cele patru niveluri de clasificare: strict secret, secret, confidențial și restricționat, de asemenea legea definește Agenția de Securitate Internă (ABW) drept autoritate de control pentru sectorul civil, Serviciul de Contrainformații Militare (SKW) pentru sectorul militar și detaliază procedura de verificare a persoanelor și a companiilor.

Legea de mai sus este completată de o serie de regulamente emise de prim-ministru sau miniștrii de resort, care stabilesc detaliile tehnice. Astfel, [Regulamentul privind securitatea industrială](#) detaliază modul în care firmele pot obține certificatul de securitate industrială.

În Polonia responsabilitatea este împărțită clar între Agenția de Securitate Internă (ABW) care supraveghează instituțiile civile, companiile de stat și contractanții privați civili și Serviciul de Contrainformații Militare (SKW) care se ocupă exclusiv de structurile Ministerului Apărării Naționale și de companiile care lucrează pentru armată.

Adâncimea verificării depinde de nivelul solicitat:

- nivelul restricționat implică o verificare simplificată, efectuată de obicei de către ofițerul de securitate al instituției angajatoare, fără implicarea directă a serviciilor secrete;
- nivelul confidențial implică o procedură de verificare obișnuită;

- nivelurile secret și strict secret necesită o procedură de verificare extinsă, care include investigații amănunțite despre viața privată, situația financiară și anturaj.

Termenele legale pentru finalizarea procedurilor de verificare a securității sunt reglementate prin Articolul 24 din Legea privind protecția informațiilor clasificate nr. 5/2010. Astfel, articolul 24 alineatul (6) reglementează în mod clar termenul general de **3 luni** în care trebuie finalizată procedura obișnuită de verificare de la data depunerii unei cereri de proceduri de verificare împreună cu chestionarul completat.

Totuși, în cazul în care termenul nu este respectat, autoritatea care efectuează procedura informează cu privire la data preconizată de finalizare, la cererea persoanei verificate și, dacă acest lucru nu prejudiciază protecția informațiilor clasificate, cu privire la motivele prelungirii.

Practica, ghidurile juridice și reglementările secundare stabilesc termene procedurale preconizate pentru verificarea/controlul antecedentelor în funcție de tipul și amploarea controlului:

Nivel de clasificare	Tipul procedurii	Termen legal (Zile/Luni)
Restricționat	Procedură simplificată	Până la 30 de zile
Confidențial	Procedură obișnuită	Până la 3 luni
Secret	Procedură extinsă	Până la 6 luni
Strict Secret	Procedură extinsă	Până la 6 luni

Pentru cazurile complexe sau verificările extinse, unele surse estimează că este nevoie de câteva luni până la aproximativ un an pentru finalizare, în special pentru verificările *secret* sau *strict secret*.

Legea poloneză privind informațiile clasificate impune verificarea antecedentelor înainte de acordarea unei autorizații de securitate. În practică, verificările standard sunt concepute pentru a fi finalizate în câteva luni, verificările extinse (pentru un nivel mai ridicat de confidențialitate) pot dura puțin mai mult, iar verificările de control sau de reverificare pot dura până la șase luni sau mai mult în circumstanțe speciale.

Desfășurarea procedurii de verificare necesită consimțământul scris al persoanei care face obiectul verificării, iar în cursul verificării, ABW sau SKW au dreptul să conducă un interviu cu persoana verificată, în scopul eliminării oricăror inexactități sau contradicții conținute în informațiile obținute.

Articolul 29 din Legea 5/2010 specifică că autorizația de securitate are o perioadă de valabilitate care diferă în funcție de nivelul de clasificare:

- 10 ani pentru nivelul confidențial,
- 7 ani pentru secret,
- 5 ani pentru strict secret.

Autorizația precizează, de asemenea, tipul de verificare efectuată și confirmă obligația persoanei de a păstra secretul.

PORTUGALIA

În Portugalia, sistemul de protecție a informațiilor clasificate și obținerea certificatului de securitate¹⁹ sunt reglementate printr-un cadru legislativ consolidat, aliniat la standardele NATO și ale Uniunii Europene. Autoritatea centrală responsabilă este Biroul Național de Securitate (GNS²⁰).

[Decretul-Lege nr. 62/2011](#) este actul normativ de bază care reglementează GNS, stabilind misiunea, atribuțiile și organizarea GNS. Decretul definește rolul directorului general al GNS ca fiind Autoritatea Națională de Securitate, singura entitate care are competența de a elibera certificate de securitate în Portugalia.

[Legea nr. 49/2008 de organizare a investigării criminale](#), deși este o lege generală, aceasta oferă cadrul în care serviciile de informații și poliția pot colabora pentru verificarea antecedentelor în scopul securității naționale.

Sistemul portughez utilizează patru niveluri, identice cu cele din majoritatea statelor NATO:

- strict secret
- secret
- confidențial
- restricționat

Procesul de autorizare este inițiat de entitatea angajatoare publică sau privată și transmis către GNS. Verificarea este realizată de Serviciile de informații (SIRP). Legislația nu impune un termen limită dar procesul este recunoscut ca fiind unul de durată. Pentru nivelul restricționat, verificarea este rapidă (câteva săptămâni). Pentru nivelul secret sau strict secret, procesul durează de obicei între **4 și 8 luni**, deoarece implică investigații amănunțite asupra loialității, caracterului și situației financiare.

GNS emite certificatul dar investigația de teren este delegată către Serviciul de informații de securitate (**SIS**) pentru civili și Serviciul de informații privind strategia de apărare (**SIED**)

¹⁹ Lb. portugheză: *Credenciação de Segurança*

²⁰ Lb. portugheză: *Gabinete Nacional de Segurança*

pentru context militar/extern. De menționat că SIS și SIED sunt ambele servicii de informații distincte și autonome, care funcționează sub cupola de coordonare a Serviciilor de Informații portugheze **SIRP**

Procedura de acordare a certificatului de securitate în Portugalia este un proces administrativ și de investigație riguros, centralizat de Biroul Național de Securitate (GNS).

Iată etapele procedurii și duratele estimate pentru fiecare nivel, bazate pe [Reglementările naționale privind siguranța - siguranța personalului \(RNS 1\)](#):

- Solicitarea trebuie inițiată de entitatea angajatoare instituție publică sau companie privată care deține deja un certificat de securitate industrială.
- Candidatul completează un formular detaliat care acoperă date personale, rezidențe anterioare, educație, experiență profesională, situație financiară și călătorii în străinătate.
- SIRP (prin serviciile sale operative SIS sau SIED) efectuează verificarea antecedentelor. Pentru nivelurile inferioare, se verifică bazele de date (cazier, poliție, informații). Pentru nivelurile superioare, se fac investigații de teren și interviuri.
- Evaluarea Riscului are loc la nivelul GNS care primește raportul de la serviciile de informații și decide dacă există factori de risc: vulnerabilitate la șantaj, loialitate îndoielnică etc.
- Directorul GNS semnează decizia de acreditare pe baza celor de mai sus. Certificatul este valabil, de regulă, **5 ani**.

Nivel de clasificare	Tip de investigație	Durată estimată
restricționat (reservado)	Verificare de bază (bazele de date)	30 - 60 zile
confidențial (confidencial)	Verificare standard (bazele de date + istoric)	3 - 5 luni
secret (secreto)	Investigație aprofundată (stil de viață, finanțe)	6 - 9 luni
strict secret (muito secreto)	Investigație completă (inclusiv interviuri)	9 - 12 luni+

Portugalia nu are termene de finalizare a verificărilor stricte înscrise în lege, însă termenele de procesare practicate de GNS și SIRP sunt estimative.

STATELE UNITE ALE AMERICII

Procedura de acordare a autorizațiilor de securitate în SUA este guvernată de un ansamblu de acte normative dar actul fundamental privind accesul la informații clasificate este [Ordinul executiv privind accesul la informațiile clasificate nr. 12968 \(1995\)](#). Acesta este baza legală a întregului sistem de *security clearance*, se aplică tuturor agențiilor federale; stabilește criteriile de eligibilitate, principiul *need to know*, drepturile persoanei investigate și procedura de revocare/ contestare.

[Ordinul executiv 13526 \(2009\)](#) stabilește cine poate clasifica informații, cât timp rămân clasificate, regulile de declasificare și definește nivelurile de clasificare:

- confidential;
- secret;
- top secret.

[Biroul Directorului Serviciului Național de Informații](#)²¹ emite [Linii directoare judiciare pentru determinarea eligibilității pentru accesul la informații clasificate](#) care stabilesc criteriile concrete de evaluare a persoanei. Sunt analizate mai multe categorii de risc precum: loialitate față de SUA, influență străină, situație financiară, consum de substanțe, comportament personal, utilizarea tehnologiei informației etc.

La nivel federal, Congresul a adoptat [Legea privind reforma serviciilor de informații și prevenirea terorismului \(IRTPA\) – 2004](#) care standardizează investigațiile de background și schimbul de informații între agenții și stă la baza sistemului actual de verificări.

În timp ce verificările sunt făcute de către agenția care a solicitat autorizarea, investigațiile concrete sunt, în principal, realizate de [Agenția de Contrainformații și Securitate a Apărării](#) pentru majoritatea cazurilor. În situații speciale, Biroul Federal de Investigații (FBI) desfășoară ancheta. Pentru nivelul *top secret*, investigația este mult mai aprofundată și include un interviu de securitate unde se clarifică riscuri de șantaj, legături externe, comportamente problematice etc.

Ca și în țările europene, în SUA, autorizația de securitate pentru acces la informații clasificate nu se solicită individual ca un permis obișnuit, ci este **inițiată de un angajator** (instituție guvernamentală sau firmă contractoare) atunci când postul o cere.

Procesul presupune completarea formularului electronic SF-86 *Questionnaire for National Security Positions*, unde se declară: date personale, istoricul locurilor de muncă, educația, adresele anterioare, călătorii în străinătate, contacte cu cetățeni străini, situația financiară, consum de droguri/ alcool, antecedente penale.

În funcție de nivelul de autorizației solicitate, au loc apoi verificările descrise mai sus. Duratele verificărilor de securitate nu sunt stabilite strict în legi, ci apar în politici executive,

²¹ *Office of the Director of National Intelligence*

directive și standarde administrative. Există repere oficiale privind duratele „*timeliness goals*” impuse la nivel federal.

[Legea privind reforma serviciilor de informații și prevenirea terorismului \(IRTPA\) – 2004](#), deși nu impune termene fixe de verificare, obligă executivul să măsoare, raporteze și să optimizeze procesul de *clearance*. Secțiunea 3001(g) stipulează:

„(1) șeful entității desemnate elaborează un plan pentru reducerea duratei procesului de verificare a securității personalului;

(2) (...) acest plan să prevadă luarea unei decizii cu privire la cel puțin 90 % din toate cererile de verificare a securității în termen de **60 de zile**; și

(3) punerea în aplicare a acestui plan în termen de cinci ani de la intrarea în vigoare a prezentei legi.”

[Directiva agentului executiv de securitate \(SEAD\) nr 5](#) emisă de Serviciul Național de Informații, face trecerea de la investigații periodice la verificări continue în sensul că atunci când apare un indicator de risc, verificarea se declanșează imediat, indiferent de timpul scurs de la ultima investigație.

[Agencia de Contrainformații și Securitate a Apărării](#) aplică ținte interne de procesare, raportate anual Congresului. Sunt categorisite inclusive cazurile simple versus cazurile complexe.

Legile cer ca procesul să fie eficient și monitorizat, fără să impună termene fixe, având în vedere necesitatea flexibilității executive, iar duratele apar doar ca obiective administrative. Trebuie precizat că termenele de realizare a investigațiilor sunt mai degrabă obiective de performanță administrativă decât termene legale rigide.

Din punct de vedere juridic, acest lucru înseamnă că solicitanții de autorizații nu pot da în judecată statul pentru depășirea duratei verificărilor iar întârzierile nu sunt motiv automat de aprobare.

Pe de altă parte, dreptul de a contesta respingerea sau revocarea unui certificat de securitate este mult mai structurat și mai transparent decât în multe alte țări. Acest proces este reglementat în principal de **Ordinul executiv 12968** și de directivele specifice ale agențiilor, cum ar fi SEAD 4 pentru criteriile de verificare.

Sistemul american se bazează pe principiul că, deși nimeni nu are un drept constituțional la un *clearance*, orice persoană are dreptul la un proces echitabil înainte ca accesul să îi fie refuzat.

UNGARIA

În Ungaria, sistemul de verificare și eliberare a certificatelor de securitate, atât pentru persoane fizice, cât și pentru firme, este reglementat în principal de două acte normative fundamentale.

[Legea nr. CLV din 2009 privind protecția informațiilor clasificate](#) este legea-cadru care definește: nivelurile de clasificare (strict secret, secret, confidențial și restricționat), instituția responsabilă de supravegherea protecției datelor și de eliberarea certificatelor pentru mediul industrial/contractori, anume Autoritatea Națională de Securitate (NBF)²² și condițiile deținerii unui certificat de securitate valid și a principiului „nevoii de a cunoaște”.

[Legea nr. CXXV din 1995 privind serviciile de securitate națională](#) stabilește procedura propriu-zisă de verificare, mai exact:

- entitatea care efectuează verificarea: de regulă, Oficiul pentru Protecția Constituției în cazul civililor sau Serviciul de Securitate Națională Militară pentru domeniul apărării;
- detaliază etapele controlului de securitate, chestionarele care trebuie completate și criteriile de risc (loialitate, vulnerabilități financiare, conexiuni străine etc.);
- definește controalele de tip „A”, „B” sau „C” în funcție de nivelul de acces solicitat.

Pe scurt, verificarea se face conform Legii 125/1995, dar dreptul de acces și formatul certificatului sunt stabilite de Legea 155/2009.

[Hotărârea de Guvern nr. 90/2010 \(III. 26.\)](#) este actul normativ care reglementează funcționarea Autorității Naționale de Securitate (NBF) și procedurile de gestionare a datelor clasificate. Aceasta detaliază procedurile pentru verificarea personalului (ca persoane fizice) care are acces la date clasificate și instituie reguli pentru siguranța fizică a spațiilor în care se prelucrează informații secrete și supravegherea locală a securității.

Procedura de obținere a certificatului de securitate în Ungaria este structurată în funcție de nivelul de acces solicitat (restricționat, confidențial, secret sau strict secret). Aceasta implică atât angajatorul, cât și serviciile de informații. Ca și în alte state, procedura nu poate fi începută de persoana fizică individual, ci trebuie inițiată de angajator sau de autoritatea contractantă: angajatorul stabilește că postul respectiv necesită acces la informații clasificate. Se verifică dacă persoana deține deja un certificat valid. Dacă nu, se înaintează o cerere către autoritatea de verificare competentă, pentru civili Oficiul pentru Protecția Constituției. Candidatul primește un chestionar detaliat existent în variante pentru tipurile de control „A” (nivelul cel mai scăzut), „B” sau „C”.

²² Lb. maghiară: NBF - [Nemzeti Biztonsági Felügyelet](#)

De menționat că în Ungaria, pentru nivelurile superioare, serviciile pot solicita utilizarea poligrafului în anumite condiții specifice, dacă există suspiciuni sau neconcordanțe în declarații.

După finalizarea investigației, serviciul de informații emite un aviz de securitate: favorabil sau nefavorabil. Dacă avizul este favorabil, Autoritatea Națională de Securitate (NBF) sau instituția abilitată emite certificatul fizic. Acesta are o valabilitate limitată, de regulă **5 ani**, după care procedura trebuie reluată.

Termenele maxime pentru efectuarea verificărilor de securitate națională erau reglementate strict prin lege în Ungaria. Actul normativ principal care stabilea aceste durate era Legea nr. CXXV din 1995 privind serviciile de securitate națională:

Nivel de Clasificare	Tip Control	Durată Aproximativă	Termen legal de finalizare
Confidențial	Tip A	30 - 45 zile	45 zile
Secret	Tip B	45 - 60 zile	60 zile
Strict secret	Tip C	60 - 90 zile	90 zile

În 2025 și la începutul anului 2026, sistemul de *clearance* din Ungaria a fost simplificat, eliminând vechile categorii stricte (A, B, C) pentru marea majoritate a verificărilor civile și unificând termenele. În prezent se aplică:

Art. 71/B. § (1) „Directorul general al serviciului național de securitate în exercițiu dispune efectuarea unui control de securitate națională în termen de 15 zile de la primirea solicitării. Controlul de securitate națională trebuie efectuat în termen de 60 de zile de la dispunere, termen care poate fi prelungit cu 30 de zile o singură dată.”

Așadar, totalul maxim teoretic din prezent este de 15 zile (eliberare ordin) + 60 zile (investigație) + 30 zile (prelungire) = 105 zile calendaristice.

Este important de reținut că termenul de 60 de zile se referă strict la durata investigației efectuate de serviciul de informații. După expirarea acestui termen și emiterea avizului favorabil, mai poate exista o perioadă administrativă scurtă până când Autoritatea Națională de Securitate (NBF) emite efectiv certificatul fizic.

În contextul modificării recente a Legii CXXV/1995, a fost introdusă verificarea simplificată de siguranță națională (art. 72), afirmându-se că scopul nu este o investigație exhaustivă a vieții private, ci una axată strict pe *angajabilitate*. Statul vrea să determine dacă persoana respectivă prezintă riscuri care ar putea afecta funcționarea legală a instituțiilor statului sau stabilitatea economiei naționale. Angajatorul are discreția de a decide dacă ocuparea postului se poate face fie fără nicio verificare (în anumite condiții) sau înainte de finalizarea verificării (angajare provizorie sub rezerva rezultatului ulterior).

Verificarea simplificată este un filtru de integritate rapid. Astfel, dacă serviciile găsesc ceva care face angajatul vulnerabil la influențe externe, angajatorul primește o așa numită „informație care afectează angajarea”, ceea ce duce fie la refuzul angajării, fie la concedierea imediată dacă persoana a fost deja instalată pe post.

Nivelul „restricționat” este cel mai redus prag de clasificare în Ungaria. Din acest motiv, procedura veche era considerabil mai simplă și mai rapidă decât în cazul nivelurilor superioare confidențial, secret sau strict secret în versiunea anterioară a legii, când nu se efectua o investigație de securitate națională completă de către serviciile de informații. În vechea formă a legii, nivelul restricționat era adesea gestionat intern de ofițerul de securitate al angajatorului, fără implicarea directă a serviciilor de informații (AH). În prezent, legea unifică aceste verificări sub umbrela verificării simplificate.

WEBOGRAFIE

[Legea privind securitatea informațiilor](#), Austria

[Instrucțiunea generală interministerială nr. 1300 privind protecția secretului apărării naționale \(IGI 1300\)](#), Franța

[Codul apărării](#), Franța

[Codul penal](#), Franța

[Legea privind verificarea de securitate](#) (SÜG), Germania

[Regulamentul de punere în aplicare a SÜG](#), Germania

[Instrucțiuni administrative generale \(SÜGVWV\)](#), Germania

[Raport de activitate](#) Oficiul Federal de Protecție a Constituției (BfV), Germania

[Interpelări Parlamentare](#) (Kleine Anfragen), Germania

[Legile din 2012-2016 privind Biroul Național de Verificare \(copii și persoane vulnerabile\)](#), Irlanda

[Legea poliției naționale nr. 20/2005](#), Irlanda

[Legea secretelor de stat nr. 1/1963](#), Irlanda

[Legea nr. 124/ 2007 privind sistemul informatic pentru securitatea Republicii și noile reglementări privind secretul](#), Italia

[Decretul Președintelui Consiliului de Miniștri nr. 5/ 2015](#) (DPCM), Italia

[Decretul legislativ nr. 159 din 2011 \(Codul antimafia\)](#), Italia

[Legea privind investigațiile de securitate \(1996\)](#), Olanda

[Legea serviciilor de informații și securitate \(2017\)](#), Olanda

[Cerințe generale de securitate pentru contracte de apărare \(ABDO 2019\)](#), Olanda

[Cerințele generale de securitate pentru achizițiile publice guvernamentale \(ABRO\)](#), Olanda

[Legea privind protecția informațiilor clasificate nr.5/ 2010](#), Polonia

[Regulamentul privind securitatea industrială](#), Polonia

[Decretul-Lege nr. 62/2011](#) Portugalia

[Legea nr. 49/2008 de organizare a investigării criminale](#), Portugalia

[Reglementările naționale privind siguranța - siguranța personalului \(RNS 1\)](#), Portugalia

[Ordinul executiv privind accesul la informațiile clasificate nr. 12968 \(1995\)](#), Statele Unite ale Americii

[Ordinul executiv 13526 \(2009\)](#), Statele Unite ale Americii

[Linii directoare judiciare pentru determinarea eligibilității pentru accesul la informații clasificate](#), Statele Unite ale Americii

[Legea privind reforma serviciilor de informații și prevenirea terorismului \(IRTPA\) – 2004](#), Statele Unite ale Americii

[Directiva agentului executiv de securitate \(SEAD\) nr 5](#), Statele Unite ale Americii

[Legea nr. CLV din 2009 privind protecția informațiilor clasificate](#), Ungaria

[Legea nr. CXXV din 1995 privind serviciile de securitate națională](#), Ungaria

[Hotărârea de Guvern nr. 90/2010 \(III. 26.\)](#), Ungaria

Alte surse bibliografice orientative:

Procedures for granting access to NATO classified information

<https://orniss.ro/procedures/access-to-nato-classified-information/?lang=en>

EDPS Security clearance procedures https://www.edps.europa.eu/system/files/2023-12/59_EDPS_data_protection_notice_Security_clearance_procedures_EN.pdf â

Clearance for NATO, EU and ESA <https://english.aivd.nl/topics/s/security-screening/clearance-for-nato-eu-and-esa> (Olanda)

EEAS Privacy Statement - PSC e-Clearance

https://www.eeas.europa.eu/sites/default/files/eeas_privacy_statement_personal_security_clearance_psc_e-clearance_climb.pdf

USA, Facility Security Clearance <https://www.state.gov/facility-security-clearance-fcl-faq> , <https://www.congress.gov/crs-product/R43216> ; **The Complete Security Clearance Guide for Government Contractors** - <https://fedbizaccess.com/the-complete-security-clearance-guide-for-government-contractors-2025/>