



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST

Direcția Generală Internă

Direcția Protecția Datelor Personale, Etică și Securitate Internă

Expert legal politici, standardizare de securitate cibernetică

#1177

1	Identificarea postului	2
1.1	Numele si prenumele titularului.....	2
1.2	Denumirea postului.....	2
1.3	Gradul profesional / treapta profesională	2
1.4	Poziția în COR (Clasificarea Ocupațiilor din Romania)	2
1.5	Compartimentul funcțional și locația.....	2
1.6	Nivelul postului	2
1.7	Sfera relațională internă și externă.....	2
1.7.1	Ierarhice	2
1.7.2	Funcționale	2
1.7.3	Reprezentare	3
1.7.4	Control	3
2	Descrierea postului	3
2.1	Scopul principal al postului	3
2.2	Descrierea sarcinilor / atribuțiilor / activităților postului	4
2.3	Delegarea de atribuții și competență.....	6
3	Condiții specifice de ocupare a postului	6
3.1	Studii de specialitate	6
3.2	Experiență profesională, competențe și aptitudini necesare	6
3.3	Instrumente și tehnologii de lucru	9
3.4	Certificări.....	9
3.5	Metodologii cunoscute	10
3.6	Cunoștințe de limba română și de limbi străine.....	10
3.7	Cerințe privind cetățenia.....	10
3.8	Autorizații speciale pentru exercitarea atribuțiilor	11
4	Indicatori de performanță.....	11

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME Prenume

1.2 Denumirea postului

- Expert legal politici, standardizare de securitate cibernetică
- *Notă: În cazul în care denumirea postului din DNSC nu se regăsește în COR, se va trece denumirea din COR cea mai apropiată din punct de vedere al sarcinilor și responsabilităților.*

1.3 Gradul profesional / treapta profesională

- superior

1.4 Poziția în COR (Clasificarea Ocupațiilor din Romania)

- Cod COR: expert în securitate cibernetică 252904 COR
- *Notă: În cazul în care poziția postului din DNSC nu se regăsește în COR, se va trece codul din COR pentru denumirea cea mai apropiată din punct de vedere al sarcinilor și responsabilităților.*

1.5 Compartimentul funcțional și locația

- Direcția Generală Internă - Direcția Protecția Datelor Personale, Etică și Securitate Internă
- Sediul DNSC / telemuncă
- Poziția #1177 în statul de funcții al DNSC

1.6 Nivelul postului

- Execuție

1.7 Sfera relațională internă și externă

1.7.1 Ierarhice

- Se subordonează pe următoarea linie ierarhică:
 - **Coordonator superior securitate cibernetică** - Direcția Protecția Datelor Personale, Etică și Securitate Internă
 - **Manager superior securitate cibernetică** - Direcția Protecția Datelor Personale, Etică și Securitate Internă
 - **Manager superior securitate cibernetică** - Conducere - Direcția Generală Internă
 - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Internă
 - **Directorul DNSC**
- Are în subordine: nu are în subordine alte posturi.

1.7.2 Funcționale

- Colaborează și cooperează cu toate funcțiile de conducere sau de execuție din compartimentele funcționale ale Directoratului Național de Securitate Cibernetică (DNSC sau Directoratul) în relaționarea cu:
 - Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS) și responsabili pentru protecția informațiilor clasificate din alte instituții competente, după caz
 - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
 - Secretariatul General al Guvernului (SGG)

- Agenția Națională de Integritate (ANI)
- Administrația Națională a Rezervelor de Stat și Probleme Speciale (ANRSPS)
- Regia Autonomă Administrația Patrimoniului Protocolului de Stat (RAAPPS)
- Colaborează și cooperează cu beneficiarii, partenerii instituționali, contractorii, subcontractorii și consultanții DNSC conform mandatului sau a instrucțiunilor primite din partea superiorilor ierarhici, pe domeniul de competență.
- Colaborează și cooperează cu managerii de proiect și cu membrii echipelor de proiect în care participă, inclusiv cu beneficiarii, partenerii instituționali, contractorii, subcontractorii și consultanții implicați în aceste proiecte.
- Colaborează și cooperează, după caz, pe domeniul de competență, cu toate funcțiile de conducere sau de execuție din compartimentele funcționale ale DNSC.
- Colaborează și cooperează cu Directorul DNSC și cu membrii cabinetului acestuia.
- Colaborează și cooperează cu Adjuncții Directorului DNSC și cu membrii cabinetelor acestora.

1.7.3 Reprezentare

- **Reprezintă DNSC și interesele DNSC**, pentru activitățile juridice pentru care este responsabil(ă) sau în care este implicat(ă), în raport cu părțile interne și externe relevante, astfel:
 - În raport cu personalul din cadrul autorităților naționale centrale și locale, după caz.
 - În raport cu furnizori de bunuri și servicii, contractori și consultanți implicați, după caz.
- **Reprezintă Direcția Protecția Datelor Personale, Etică și Securitate Internă din Direcția Generală Internă a DNSC**, conform mandatului primit din partea superiorilor ierarhici, atunci când participă la conferințe, seminarii, grupuri de lucru, prezentări sau alte evenimente ori activități profesionale în afara instituției.
- **Reprezintă DNSC și interesele DNSC** în raport cu experți individuali și organizații profesionale sau non-guvernamentale din domeniul juridic.

1.7.4 Control

- Are atribuții de monitorizare cu privire la securitatea informațiilor clasificate, a datelor cu caracter personal, în cadrul DNSC, precum și cu privire la respectarea legislației în vigoare referitoare la protecția informațiilor clasificate.
- Asigură activitatea de monitorizare și control cu privire la aplicarea prevederilor codului de etică și integritate la nivel instituțional.

2 Descrierea postului

2.1 Scopul principal al postului

- **Îndeplinește rolul de responsabil cu protecția datelor personale (Data Protection Officer - DPO) pentru Directorat.**
- **Îndeplinește rolul de punct de contact al DNSC în relația cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, inclusiv privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36 din Regulamentul UE nr.679/2016, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.
- **Asigură și desfășoară activități de consiliere juridică** a tuturor compartimentelor funcționale din cadrul DNSC, privind securitatea informațiilor clasificate, a datelor cu caracter personal, precum și aplicarea prevederilor codului de etică și integritate instituțional.
- **Avizează din punct de vedere juridic documente și acte administrative ale Directoratului** privind securitatea informațiilor clasificate, a datelor cu caracter personal, aplicarea prevederilor codului de etică și integritate instituțional.

- **Asigură reprezentarea juridică a Directoratului în fața persoanelor fizice sau juridice, în temeiul împuternicirilor date de conducerea DNSC pe linia securității informațiilor clasificate, a datelor cu caracter personal, aplicării prevederilor codului de etică și integritate instituțional.**

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- **Elaborează, analizează și evaluează, la nivelul Direcției Protecția Datelor Personale, Etică și Securitate Internă a DNSC documente specifice (rapoarte, analize, sinteze, decizii etc.) și le supune spre aprobare către conducerea Direcției;**
- **Pe bază de mandat, reprezintă și apără interesele legitime și poziția DNSC în fața autorităților publice, instanțelor, instituțiilor de orice natură, precum și în fața oricărei persoane juridice sau fizice, române sau străine.**
- **Redactează și depune în termen actele aferente procedurilor impuse de instituțiile cu care exercită competențele pe linia securității informațiilor clasificate, datelor cu caracter personal, aplicării prevederilor codului de etică și integritate instituțional aplicabile DNSC. Prezintă note de stadiu cu privire la procesele funcționale în curs de implementare în DNSC.**
- **Răspunde de redactarea, la cererea Conducerii Directoratului sau a superiorilor ierarhici, de proiecte de decizii, regulamente, contracte și orice alte documente referitoare la desfășurarea activității instituției, în conformitate cu legislația în vigoare.**
- **Răspunde de redactarea, la cererea Conducerii Directoratului sau a superiorilor ierarhici, de opinii juridice coerente și fundamentate în fapt și în drept cu privire la evenimente curente pe linia securității informațiilor clasificate, datelor cu caracter personal, aplicării prevederilor codului de etică și integritate instituțional.**
- **Răspunde de informarea și consilierea Conducerii Directoratului, precum și a angajaților care se ocupă de prelucrarea datelor la nivelul DNSC, cu privire la obligațiile care le revin în temeiul Regulamentului UE nr.679/2016 și a altor dispoziții de drept al Uniunii Europene sau drept intern referitoare la protecția datelor cu caracter personal.**
- **Efectuează și răspunde de monitorizarea respectării prevederilor Regulamentului UE nr.679/2016, a altor dispoziții de drept al Uniunii Europene sau de drept intern referitoare la protecția datelor și a politicilor instituției în ceea ce privește protecția datelor cu caracter personal, inclusiv:**
 - Colectarea de informații pentru a identifica operațiunile de prelucrare a datelor.
 - Analiza și verificarea conformitatea operațiunilor de prelucrare a datelor.
 - Propunerea de alocare a responsabilităților și de acțiuni de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente.
 - Evaluarea și documentarea impactului asupra protecției datelor (Data Protection Impact Assessment DPIA) pentru procesele și platformele DNSC.
 - Semnalarea, pe cale ierarhică, în scris, argumentat juridic și asumat, a elementelor de neconformitate cu prevederile legale privind prelucrarea și protecția datelor cu caracter personal.
- **Răspunde de semnalarea, pe cale ierarhică, în scris, argumentat juridic și asumat, a elementelor de neconformitate cu prevederile legale, pe linia securității informațiilor clasificate, a aplicării prevederilor codului de etică și integritate instituțional din DNSC în ansamblu sau a compartimentelor funcționale ale DNSC și face recomandări de acțiuni concrete în vederea soluționării neconformităților.**
- **La cerere, efectuează și răspunde de analiza, evaluarea, verificarea și/sau avizarea din punct de vedere juridic (dar nu se pronunță asupra aspectelor economice, tehnice sau de altă natură cuprinse în documentele vizate ori semnate) de:**
 - Protocoale, convenții, acorduri de colaborare, acorduri de parteneriat, contracte de muncă, contracte de achiziții încheiate de Directorat în domeniul său de activitate.
 - Acte cu caracter juridic și administrative pe linia securității informațiilor clasificate, a datelor cu caracter personal, a aplicării prevederilor codului de etică și integritate instituțional.

- Acte administrative și/sau documente privind actele de numire, definitivare sau eliberare din funcție.
- Acte administrative și/sau documente privind procedurile de achiziție publică derulate de DNSC, inclusiv cele ce implică finanțare internațională.
- **Asigură executarea la timp și la un nivel de calitate adecvat** profesiei juridice a activităților de consiliere juridică pe linia securității informațiilor clasificate, a datelor cu caracter personal, a aplicării prevederilor codului de etică și integritate instituțional, cu identificarea resurselor necesare pentru atingerea obiectivelor acestora, precum și identificarea și gestionarea riscurilor aferente.
- Întocmește răspunsuri din punct de vedere juridic la adrese și sesizări înregistrate la sediul instituției, dacă este cazul.
- Răspunde de publicarea pe site-ul web al DNSC a unei secțiuni **pe linia securității informațiilor clasificate, a datelor cu caracter personal, a aplicării prevederilor codului de etică și integritate al DNSC** și cooperează cu **Direcția Comunicare, Media și Marketing** și respectiv cu **Direcția Infrastructură Tehnică** în vederea modernizării și actualizării formei și conținutului site-ului web / paginii.
- În colaborare cu **Serviciul Secretariat**, întocmește, completează și actualizează permanent lista de contacte instituționale a DNSC (instituții, persoane de contact, adresa poștală, numere de telefon, adrese de email) care fac obiectul direct sau incidental al activității proprii.
- Are obligația de a organiza și păstra toate documentele primite / transmise, inclusiv cele întocmite pentru uz intern.
- **Identifică voluntari (elevi, studenți, absolvenți, etc.)** în vederea colaborării cu DNSC și propune superiorilor ierarhici modalități de implicare a acestora în activitățile Directoratului.
- Efectuează coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) care îi sunt asigurați, în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Monitorizare Reglementări Interne și Internaționale**.
- Îndeplinește, în conformitate cu art.81-82 din HG 1336/2022, **rolul de îndrumător** pentru unul sau mai mulți salariați debutanți.
- **Participă, după caz, ca membru sau președinte** al comisiei, în comisiile de concurs sau examen pentru posturile scoase la concurs de către DNSC.
- **Participă, după caz, ca membru sau președinte** al comisiei, în comisiile de inventariere înființate la nivelul DNSC.
- Participă, la nevoie, în comisiile de evaluare/contestații/negociere a contractelor de achiziție publică, **în calitate de consilier juridic**.
- **Răspunde de confidențialitatea datelor și informațiilor DNSC** la care are acces, în conformitate cu prevederile legale, normele interne ale DNSC și cu instrucțiunile primite.
- Furnizează expertiză, efectuează analize, pregătește clarificări și face propuneri de îmbunătățire privind activitățile specifice ale **Direcției Protecția Datelor Personale, Etică și Securitate Internă**.
- Participă activ la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Protecția Datelor Personale, Etică și Securitate Internă sau ale Direcției Juridice**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- Participă activ la **ședințele interne organizate lunar la nivelul Direcției Protecția Datelor Personale, Etică și Securitate Internă**.
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul **Direcției Protecția Datelor Personale, Etică și Securitate Internă** precum și cu alte compartimente din cadrul DNSC și/sau partenerii instituționali.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Pregătește datele și informațiile necesare și întocmește raportarea periodică pentru **indicatorii de performanță (KPIs - Key Performance Indicators)** ai activităților proprii

- **Facilitează cooperarea și lucrul în echipă la nivelul Direcției** prin comunicare verbală și scrisă cu personalul acesteia; și efectuează diseminarea permanentă a tuturor informațiilor relevante precum și urmărirea folosirii de către personalul Direcției a informațiilor furnizate.
- **Face propuneri concrete de îmbunătățire a metodelor de lucru la nivelul Direcției Protecția Datelor Personale, Etică și Securitate Internă**, atât direct în cadrul Direcției sau la nivelele ierarhice superioare, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor în atingerii obiectivelor instituționale.
- **Asigură identificarea și rezolvarea cu celeritate a problemelor apărute** în derularea activităților curente în care este implicat(ă) și informează la timp superiorii ierarhici despre problemele apărute pe care nu le poate rezolva la nivelul său, propunând în mod pro-activ soluții.
- **Acționează cu bună-credință și amabilitate în exercitarea sarcinilor profesionale**, prezentând o atitudine civilizată și un comportament bazat pe respect, corectitudine, integritate morală și profesională.
- **Îndeplinește orice alte atribuții dispuse de conducerea instituției**, în limitele competențelor legale.
- **Are toate drepturile și obligațiile prevăzute de Legea nr. 514 din 28 noiembrie 2003 privind organizarea și exercitarea profesiei de consilier juridic** în conformitate cu statutul profesional și cu reglementările legale ce stau la baza desfășurării activității DNSC, cu care are raporturi de muncă.
- **Respectă dispozițiile Regulamentului European nr. 679/2016 și a Legii nr. 190/2018** privind măsuri de punere în aplicare a Regulamentului (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.

2.3 Delegarea de atribuții și competență

- În situația și pe perioada în care titularul postului se află în imposibilitatea de a-și îndeplini atribuțiile de serviciu (spre exemplu: concediu de odihnă, concediu pentru incapacitate de muncă, delegații, concediu fără plată, suspendare, detașare etc.), o parte din atribuțiile sale menționate în secțiunea anterioară vor fi preluate prin delegare de către de către una sau mai multe din următoarele funcții din cadrul Direcției:
 - Expert securitate cibernetică
 - Expert analiză surse deschise, riscuri și amenințări securitate cibernetică
 - Expert legal politici, standardizare de securitate cibernetică
 - Asistent legal politici, standardizare de securitate cibernetică
 - Expert dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică
 - Specialist procese interne (inspector integritate)
 - Specialist securitatea informației (și responsabil PDCP)
 - Specialist securitatea informației

iar preluarea de atribuții se face prin desemnare de către **Managerul superior de securitate cibernetică din Direcția Protecția Datelor Personale, Etică și Securitate Internă**.

3 Condiții specifice de ocupare a postului

3.1 Studii de specialitate

- Studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată, absolvite cu diplomă de licență sau echivalentă, în **domeniul științe juridice**.

3.2 Experiență profesională, competențe și aptitudini necesare

- **Experiență de minim doi (2) ani în domeniul juridic, acumulată în ultimii cinci (5) ani.**

- **Experiență anterioară practică de minim un (1) an pe funcție de consilier juridic, sau de responsabil cu protecția datelor personale (Data Protection Officer), sau de responsabil cu informațiile clasificate.**
- Cunoașterea prevederilor legale referitoare la:
 - OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea nr. 11 din 07.01.2022.
 - Hotărârea Guvernului nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027.
 - Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.
 - Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.
 - Legea nr. 514/2003 privind organizarea și exercitarea profesiei de consilier juridic.
 - Regulamentului European nr. 679/2016 și a Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (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.
 - Legea nr. 361/2022 privind protecția avertizorilor în interes public.
 - Legea nr. 176/2010 privind integritatea în exercitarea funcțiilor și demnităților publice actualizată.
 - Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului.
 - Legea nr. 184/2016 privind instituirea unui mecanism de prevenire a conflictului de interese în procedura de atribuire a contractelor de achiziție publică.
 - Legea nr. 115/1996 pentru declararea și controlul averii demnitarilor, magistraților, a unor persoane cu funcții de conducere și de control și a funcționarilor publici, cu modificările și completările ulterioare.
 - Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.
 - Legea nr. 182/2002 privind protecția informațiilor clasificate.
 - Legea nr. 98/2016 privind achizițiile publice.
 - Legea nr. 544/2001 privind informațiile de interes public.
 - HG nr. 175/2008 privind stabilirea modelelor Registrului declarațiilor de avere și Registrului declarațiilor de interese.
 - HG nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.
 - HG nr. 781/2002 privind protecția informațiilor secrete de serviciu.
 - Hotărârea Guvernului nr. 395/2016 pentru aprobarea Normelor Metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului cadru din Legea 98/2016 privind achizițiile publice
- **Cunoștințe, competențe și abilități (KSAs - knowledge, skills, and abilities) specifice efectuării de activități în cadrul unei organizații de securitate cibernetică, așa cum acestea sunt definite de National Institute of Standards and Technologies (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Education (i.e. NICE Framework):**
 - Cunoștințe, competențe și abilități **profesionale:**

- **Managementul conflictelor - Conflict Management (C009)** - are aptitudini privind la gestionarea și soluționarea conflictelor, reclamațiilor, confruntărilor sau dezacordurilor într-o manieră constructivă pentru a minimiza impactul negativ personal; colaborează cu alte persoane pentru a încuraja cooperarea și lucrul în echipă.
- **Gândire critică - Critical Thinking (C011)** - are aptitudini privind analiza obiectivă a faptelor pentru a forma o judecată profesională.
- **Comunicare orală/verbală - Oral Communication (C036)** - are aptitudini privind exprimarea informațiilor sau a ideilor prin viu grai.
- **Comunicare scrisă - Written Communication (C060)** - are aptitudini privind formularea și comunicarea oricărui tip de mesaj care utilizează cuvântul scris.

○ **Cunoștințe, competențe și abilități tehnice:**

- **Rezolvarea de probleme - Problem Solving (C040)** - are aptitudini privind determinarea exactității și relevanței informațiilor și utilizarea unei judecăți profesionale solide pentru a evalua alternative; luarea unor decizii bine informate, obiective, care să ia în considerare faptele, obiectivele, constrângerile și riscurile, percepend în același timp impactul și implicațiile deciziilor proprii.
- **Managementul cunoștințelor - Knowledge Management (C029)** - are aptitudini privind valoarea informațiilor și cunoștințelor colectate/acumulate și metodele de partajare a acestora în cadrul unei organizații.

○ **Cunoștințe, competențe și abilități operaționale:**

- **Confidențialitatea și protecția datelor - Data Privacy and Protection (C014)** - are aptitudini privind relația dintre colectarea, stocarea și difuzarea datelor, protejând în același timp viața privată a persoanelor fizice.
- **Juridic, Guvernanță și Jurisprudență - Legal, Government, and Jurisprudence (C030)** - are aptitudini privind legi, reglementări, politici și etică, care pot avea un impact asupra activităților organizaționale.
- **Cunoașterea/conștientizarea situației organizaționale - Organizational Awareness (C037) - este de dorit** - are aptitudini privind înțelegerea misiunii și funcțiilor unei organizații, a structurii și modului sau de organizare, și a modului în care programele, politicile, procedurile, regulile și reglementările conduc și influențează activitatea și obiectivele organizației.
- **Managementul Riscului - Risk Management (C044)** - are aptitudini privind metode și instrumente utilizate pentru identificarea, evaluarea și gestionarea riscurilor.
- **Managementul relațiilor - Client/Stakeholder Relationship Management (C003)** - are aptitudini privind conceptele, practicile și tehnicile utilizate pentru a identifica, a se angaja cu, a influența și monitoriza relațiile cu persoane și grupuri conectate la un efort de lucru, inclusiv cei implicați activ, cei care exercită influență asupra procesului și a rezultatelor sale și cei care au un interes legitim în rezultat (pozitiv sau negativ).

- **Experiență anterioară practică în analiza de date și informații și în pregătirea de rapoarte și rezumate de un nivel calitativ foarte ridicat**, ce includ utilizarea de tabele, imagini ilustrative sau grafice pentru sublinierea de concluzii și inter-relaționare a datelor și informațiilor analizate.
- Capacitatea de a colabora eficient cu colegii, partenerii externi și părțile interesate.
- Gândire critică și centrată pe rezolvarea problemelor profesionale din domeniul propriu.
- Abilitatea de a respecta instrucțiuni orale și scrise.
- Abilitatea de a procesa și de a analiza informații contextuale și volume mari de date.
- Abilitatea de a acționa într-o manieră logică și investigativă și cu atenție excelentă la detalii.
- Aptitudini excelente de prezentare, comunicare, relaționare și interpersonale.

- Aptitudini de planificare, organizare și control al activității proprii și ale unei echipe.
- Aptitudini de luare de decizii, inițiativă și autonomie în acțiune.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară dovedită și poate să utilizeze **la un nivel avansat** aplicații de tip Office (sau echivalent):
 - Microsoft Word, Excel, Powerpoint, Outlook, Teams, etc.
 - Google Docs, Sheets, Slides, Calendar, Sites etc.
 - Libre Office Writer, Calc, Impress, Draw, Math, Base etc.
- **Este de dorit experiența anterioară practică** în utilizarea sau cunoașterea de aplicații și platforme juridice de tipul următor (sau echivalent):
 - Platforma <https://legislatie.just.ro>
 - Portalul instanțelor de judecată <https://portal.just.ro>

3.4 Certificări

- **Este de dorit să posede, la data preluării postului, cel puțin una (1) din următoarele certificări sau cursuri de specializare (sau echivalent):**
 - Cursuri de perfecționare organizate de Colegiul Național al Consilierilor Juridici
 - Curs acreditat de Ministerul Muncii și Solidarității Sociale (MMSS), Ministerul Educației (ME), Autoritatea Națională pentru Calificări (ANC) sau de Comisia de Autorizare a Furnizorilor de Formare Profesională (CAFFPA) pentru:
 - COR 261101 Avocat
 - COR 261102 Jurisconsult
 - COR 261103 Consilier juridic
 - COR 261903 Expert jurist
 - COR 261910 Consilier armonizare legislativă
 - COR 261911 Expert armonizare legislativă
 - COR 261912 Analist armonizare legislativă
 - COR 261914 Revizor jurist
 - COR 261920 Expert prevenire și combatere a corupției
 - COR 241239 Ofițer securitatea informației (Security Officer - SO)
 - COR 121118 Manager securitatea informației (Chief Information Security Officer - CISO)
 - COR 242231 Responsabil cu protecția datelor cu caracter personal
 - CISA - Certified Information Systems Auditor
 - CISM - Certified Information Security Manager
 - CISSP - Certified Information Systems Security Professional
 - CISM CompTIA Security+
 - CySA + - CompTIA Cybersecurity Analyst
 - CASP + - CompTIA Advanced Security Practitioner
 - ISO 27001, ISO 27002, ISO 27005, ISO 270035, ISO 270032

- **Are obligația ca în termen de maximum un (1) an de la data preluării postului, să obțină cel puțin una (1) din următoarele certificări** (sau echivalent) - costurile aferente acestora fiind suportate de către DNSC:
 - Cursuri de perfecționare organizate de Colegiul Național al Consilierilor Juridici
 - Curs acreditat de Ministerul Muncii și Solidarității Sociale MMSS, Ministerul Educației ME, Autoritatea Națională pentru Calificări ANC sau de Comisia de Autorizare a Furnizorilor de Formare Profesională CAFFPA pentru:
 - COR 261101 Avocat
 - COR 261102 Jurisconsult
 - COR 261103 Consilier juridic
 - COR 261903 Expert jurist
 - COR 261910 Consilier armonizare legislativă
 - COR 261911 Expert armonizare legislativă
 - COR 261912 Analist armonizare legislativă
 - COR 261914 Revizor jurist
 - COR 261920 Expert prevenire și combatere a corupției
 - COR 241239 Ofițer securitatea informației (Security Officer - SO)
 - COR 121118 Manager securitatea informației (Chief Information Security Officer - CISO)
 - COR 242231 Responsabil cu protecția datelor cu caracter personal
 - CISA - Certified Information Systems Auditor
 - CISM - Certified Information Security Manager
 - CISSP - Certified Information Systems Security Professional
 - CISM CompTIA Security+
 - CySA + - CompTIA Cybersecurity Analyst
 - CASP + - CompTIA Advanced Security Practitioner
 - ISO 27001, ISO 27002, ISO 27005, ISO 270035, ISO 270032

3.5 Metodologii cunoscute

- Trebuie să cunoască **la un nivel general** cel puțin una din metodologiile sau prevederile legale următoare (sau echivalent):
 - Ordinul nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităților publice.
 - HG nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.
 - HG nr. 781/2002 privind protecția informațiilor secrete de serviciu.

3.6 Cunoștințe de limba română și de limbi străine

- Cunoașterea limbii române ca limbă maternă sau limbă română de **minimum nivel C1** conform [Common European Framework of Reference for Languages CEFR](#)
- Cunoașterea limbii engleze de **minimum nivel B1** conform [Common European Framework of Reference for Languages CEFR](#). Titularul postului are obligația ca în termen de maximum trei (3) luni de la data angajării să prezinte dovada îndeplinirii cerinței obligatorii de limbă engleză de **minimum nivel B1** conform Common European Framework of Reference for Languages CEFR.
- Cunoașterea unei a doua limbi străine la nivel operațional este de dorit.

3.7 Cerințe privind cetățenia

- Cetățenie română, a unui alt stat membru al Uniunii Europene ori al Spațiului Economic European, ori cetățenia Confederației Elvețiene.
- *Notă: Persoanele care au cetățenia unui alt stat membru al Uniunii Europene ori al Spațiului Economic European ori cetățenia Confederației Elvețiene pot fi încadrate în muncă pe teritoriul României în baza unui contract individual de muncă în aceleași condiții în care pot fi angajați și cetățenii români.*

3.8 Autorizații speciale pentru exercitarea atribuțiilor

- Titularul postului are obligația ca în termen de maximum trei (3) luni de la data angajării / reîncadrării să efectueze, cu sprijinul DNSC demersurile de înscriere în tabloul profesional al consilierilor juridici definitivi sau stagiați în condițiile Legii nr. 514 din 28 noiembrie 2003 privind organizarea și exercitarea profesiei de consilier juridic. În cazul în care sunt costuri implicate, acestea vor fi suportate de către DNSC, cu aprobarea superiorilor ierarhici.
- Deținere/obținere autorizație de acces la informații clasificate secrete de stat, nivel **SECRET**.

4 Indicatori de performanță

- **Elaborarea anuală, în termenul stabilit, a raportului anual al activităților rolului de responsabil cu protecția datelor personale (Data Protection Officer - DPO).**
- **Efectuarea a minimum două (2) sesiuni interne de pregătire și conștientizare cu personalul DNSC, pe tema securității informațiilor clasificate, a datelor cu caracter personal, a aplicării prevederilor codului de etică și integritate.**
- **Coordonarea și îndrumarea activității pentru minimum un (1) voluntar anual, asignat Direcției Protecția Datelor Personale, Etică și Securitate Internă, pe o perioadă de voluntariat de minimum o (1) lună.**
- **Numărul de avize sau opinii juridice redactate / întocmite într-o anumită perioadă de timp (lunar, trimestrial, anual) pentru care Conducerea DNSC sau cea a compartimentelor funcționale implicate a confirmat că au fost folosite efectiv.**
- **Numărul de documente avizate din punct de vedere juridic într-o anumită perioadă de timp (lunar, trimestrial, anual).**
- **Efectuarea anual a unui număr minimal de șaisprezece (16) ore de cursuri online sau fizic, într-un domeniu relevant pentru activitatea proprie, dovedită cu certificat de participare/absolvire/diplomă sau similar. În cazul în care sunt costuri implicate de efectuarea cursurilor, acestea vor fi suportate de către DNSC, cu aprobarea superiorilor ierarhici.**
- **Lipsa absențelor nemotivate pentru participarea la sesiunile de pregătire profesională organizate trimestrial la nivelul Direcției Protecția Datelor Personale, Etică și Securitate Internă, ce au ca obiectiv asigurarea menținerii și îmbunătățirii cunoștințelor profesionale proprii.**
- **Concluzii pozitive la evaluarea independentă bi-anuală (la 6 luni) a performanței în acest post, cu accent pe îndeplinirea sarcinilor, atribuțiilor și activităților postului.**
- **Lipsa unor plângeri sau reclamații fundamentate privind activitățile specifice pentru care este responsabil(ă) sau în care este implicat(ă), venite din partea personalului DNSC, sau după caz a partenerilor instituționali ai DNSC sau a contractorilor (furnizorilor, executanților sau prestatorilor) implicați.**

Directoratul Național de Securitate Cibernetică

Angajat/Salariat

Nume + Prenume

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Data _____