

8. Atribuțiile postului:

1. elaborează și supune aprobării conducerii instituției normele interne privind protecția informațiilor clasificate, potrivit legii,
2. întocmește programul de prevenire a scurgerii de informații clasificate și îl supune avizării instituțiilor abilitate, iar după aprobare acționează pentru aplicarea acestuia,
3. acordă sprijin reprezentanților autorizați ai instituțiilor abilitate, potrivit competențelor legale, pe linia verificării persoanelor pentru care se solicită accesul la informații clasificate,
4. asigură păstrarea și organizează evidența certificatelor de securitate și autorizațiilor de acces la informații clasificate;
5. actualizează permanent evidența certificatelor de securitate și a autorizațiilor de acces;
6. întocmește și actualizează listele informațiilor clasificate elaborate sau păstrate de instituție, pe clase și nivele de secretizare;
7. prezintă conducătorului instituției propuneri privind stabilirea obiectivelor, sectoarelor și locurilor de importanță deosebită pentru protecția informațiilor clasificate din sfera de responsabilitate și, după caz, solicită sprijinul instituțiilor abilitate;
8. efectuează cu aprobarea conducerii instituției controale privind modul de aplicare a măsurilor legale de protecție a informațiilor clasificate;
9. efectuează operațiunile de predare-primire a corespondenței neclasificate prin unitatea specializată a SRI;
10. efectuează orice activitate de elaborare, luare în evidență, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, păstrare, arhivare sau distrugere a informațiilor clasificate,
11. exercită alte atribuții în domeniul protecției informațiilor clasificate, potrivit legii;
12. elaborează Procedurile Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;
13. cooperează cu administratorul de securitate a SIC SIOCWEB cu privire la orice aspect legat de securitatea componentei proprii a sistemului;
14. aplică măsurile cuprinse în Programul de prevenire a scurgerii de informații clasificate, referitoare la managementul securității SIC SIOCWEB;
15. acționează pentru îndeplinirea întocmai și în termenele stabilite, a sarcinilor și atribuțiilor din documentele de planificare, implementare și dezvoltare a SIC SIOCWEB;
16. asigură corecta aplicare a măsurilor de securitate fizică și buna funcționare a acestora la nivelul locațiilor proprii în care sunt dispuse resursele SIC SIOCWEB;
17. asigură verificarea periodică a integrității resurselor SIC SIOCWEB prin verificarea sigiliilor de securitate aplicate la nivelul acestora;
18. informează șeful structurii de securitate și a AOSIC cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;

19. aplică măsurile de control al accesului în locația terminalului propriu aferent SIC SIOCWEB și la terminalul SIC SIOCWEB, potrivit Programului de prevenire a scurgerii de informații clasificate și Procedurilor Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;
20. asigură pe plan local evidența și actualizarea fișelor de pregătire individuală a persoanelor autorizate să acceseze informații clasificate naționale și a administratorului de securitate local/înlocuitor,
21. primește cererile de vizitare a locației proprii a SIC SIOCWEB coordonând toate activitățile aferente;
22. asigură instruirea și pregătirea utilizatorului terminalului distant al SIC privind securitatea informațiilor, resurselor și serviciilor sistemului;
23. asigură reluarea semestrială a procesului de analiză de risc la nivelul componentei proprii a SIC SIOCWEB, rezultatele urmând a fi transmise AOSIC,
24. informează șeful structurii de securitate și cooperează cu administratorul de securitate a sistemului (componenta centrală) cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;
25. notifică SRI imediat cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc;
26. verifică anual modul de acțiune în situații de urgență, în conformitate cu prevederile capitolului VI al Procedurilor Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;
27. În calitate de responsabil cu protecția datelor cu caracter personal (DPO) îndeplinește următoarele atribuții și obligații:
 - a) informează și consiliază conducerea ANAP, precum și angajații care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul Regulamentului (UE) 2016/679 și al altor dispoziții de drept intern referitoare la protecția datelor;
 - b) monitorizează respectarea Regulamentului (UE) 2016/679 sau de drept intern referitoare la protecția datelor și a politicilor/procedurilor interne ale ANAP în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
 - c) furnizează consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35 din Regulamentul (UE) 2016/679;
 - d) cooperează cu autoritatea de supraveghere Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
 - e) îndeplinește rolul de punct de contact pentru autoritatea de supraveghere privind aspectele legale de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36 din Regulamentul (UE) 2016/679 precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;
 - f) identifică acțiunile care trebuie întreprinse pentru conformarea la cerințele impuse de Regulamentul (UE) 2016/679 și, împreună cu conducerea compartimentelor din cadrul ANAP care în activitatea acestora prelucrează date cu caracter personal, prioritizează aceste acțiuni în funcție de riscurile pe care le prezintă prelucrările efectuate pentru drepturile și libertățile persoanelor vizate cu accent pe estimarea riscurilor asupra protecției datelor din punctul de vedere al acestora luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii;
 - g) asigură elaborarea procedurilor interne care să garanteze în orice moment respectarea protecției datelor cu caracter personal, împreună cu conducerea compartimentelor din cadrul ANAP care în activitatea acestora pretucrează date cu

caracter personal, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date, precum: breșe de securitate, solicitări privind exercitarea drepturilor persoanelor vizate, modificarea datelor cu caracter personal colectat;

h) are obligația de a respecta confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu prevederile drptului intern;

i) răspunde pentru activitatea desfășurată direct față de președintele ANAP;

j) nu poate fi demis sau sancționat de președintele ANAP pentru îndeplinirea sarcinilor sale;

k) are obligația de a nu fi în conflict de interes cu alte sarcini sau atribuții.

28. Asigură suport Compartimentului de coordonare a investițiilor din PNRR în vederea respectării cerințelor impuse de Regulamentul (UE) nr. 2016/679 în derularea activității de colectare și prelucrare a datelor aferente realizării reformelor/investițiilor/jaloanelor/țintelor pentru care ANAP are calitatea de coordonator de reformă și care necesită expertiză de specialitate.

29. Identifică, împreună cu conducerea Compartimentului de coordonare a investițiilor din PNRR, acțiunile care trebuie întreprinse în vederea asigurării respectării obligațiilor României, așa cum sunt prevăzute la art. 22 alin. (2) și alin. (3) din Regulamentul (UE) nr. 2021/241."