***ATRIBUŢIILE POSTULUI de INSPECTOR SUPERIOR***
***SERVICIUL INVESTITII – DIRECTIA DE INVESTITII – DIRECTIA GENERALA DE ACHIZITII SI INVESTITII***

## *I. Atribuţii generale*

1. Întocmeşte corespondenţa specifică domeniului de activitate, destinată atât circuitului intern cât şi extern, o tehnoredactează şi o prezintă spre avizare şefilor ierarhic superiori;
2. Întocmeşte borderourile de corespondenţă (lista lucrărilor înaintate spre avizare sefilor ierarhic superiori);
3. Cunoaşte şi se implică în problematica de serviciu, cunoscând şi sprijinind acţiunile sau manifestările iniţiate în cadrul Serviciului, conform principiului „lucrul în echipă";
4. Raportează, ori de câte ori este nevoie şefilor ierarhic superiori despre stadiul unui demers anume şi vine cu propuneri şi iniţiative noi ori de câte ori situaţiile ivite o impun;
5. Răspunde de cunoaşterea legislaţiei referitoare la problemele specifice activităţii postului pe care îl ocupă şi se informează în permanenţă cu privire la modificările legislative survenite;
6. Face propuneri referitoare la activitatea serviciului, pe care le supune aprobării coordonatorului direct;
7. Îndeplineşte alte sarcini stabilite de şefii ierarhic superiori, în domeniul specific de activitate;
8. Respectă Regulamentul de Organizare şi Funcţionare al Primăriei Sectorului 5, precum şi Regulamentul de Ordine Interioară;
9. Răspunde de respectarea programului zilnic de lucru;
10. Răspunde de corectitudinea raportărilor efectuate.
11. Cunoaşte şi respectă prevederile Regulamentul UE nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
12. Asigură securitatea şi confidenţialitatea datelor cu caracter personal pe care le prelucrează sau la care are acces în virtutea atribuţiilor de serviciu, inclusiv prin anonimizare şi/sau pseudonimizare;
13. Respectă politicile şi procedurile/instrucţiunile cu caracter general-instituţional sau specific compartimentului, tehnice, organizaţionale (inclusiv procedurile/instrucţiunile de lucru privind securitatea informatică) aprobate de conducerea instituţiei;
14. Nu va divulga, persoanelor neautorizate, parolele de acces în sistemele informatice ale instituţiei pe care le utilizează;
15. Nu va copia pe suport fizic niciun fel de date cu caracter personal disponibile în sistemele informatice ale instituţiei, cu exceptia situaţiilor în care aceasta activitate se regăseşte în atribuţiile sale de serviciu sau a fost autorizată de către superiorul ierarhic;
16. Interzice/împiedică accesul persoanelor neautorizate la canalele de accesare a datelor personale disponibile pe computerele instituţiei cu ajutorul căruia îşi desfăşoară activitatea;
17. Manipulează datele cu caracter personal stocate pe suport fizic, la care are acces în virtutea atribuţiilor sale, cu cea mai mare precauţie, atât în ce priveste conservarea suporturilor, cât şi în ce priveşte depunerea lor în locurile şi în condiţiile stabilite în procedurile/instrucţiunile de lucru sau dispoziţiile şefilor ierarhici;
18. Nu va divulga nimănui datele cu caracter personal la care are acces, cu excepţia situaţiilor prevăzute de lege sau în care comunicarea datelor cu caracter personal se regăseşte în atribuţiile sale de serviciu sau a fost autorizată de către superiorul ierarhic;
19. Nu va transmite, pe suport informatic şi nici pe un altfel de suport, date cu caracter personal către sisteme informatice care nu se află sub controlul instituţiei sau care sunt accesibile în afara acesteia, inclusiv stick-uri USB, HDD, discuri rigide, căsuţe de e-mail, foldere accesibile via FTP sau orice alt mijloc tehnic, cu excepţia situaţiilor în care există obligaţia legală de a transmite aceste date;
20. Respectă regulile de utilizare a e-mailului (poştei electronice) în scopul prevenirii incidentelor de securitate, precum şi transmiterea neautorizată a datelor cu caracter personal;
21. Respectă drepturile persoanei vizate prevăzute de Regulamentul UE nr. 679/2016;

22. Comunică responsabilului cu protecţia datelor schimbările care necesită actualizarea evidenţei activităţilor de prelucrare a datelor, precum şi cele apărute în fluxul de activitate, acestea putând necesita noi analize de risc asupra prelucrării datelor cu caracter personal.
23. Prelucrează datele obţinute prin activitatea specifică numai în scopurile permise de lege, cu atentie sporită pentru condiţiile suplimentare de securitate necesare în prelucrarea de date sensibile, referitoare la originea rasială sau etnică, convingerile politice, religioase, apartenenţa sindicală, starea de sănătate etc;
24. Se asigură că datele cu caracter personal sunt colectate în scopuri determinate, explicite şi legitime;
25. Prelucrează numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu;
26. Informează imediat conducerea instituţiei despre împrejurările care pot conduce la o diseminare neautorizată de date cu caracter personal sau despre situaţiile în care au fost accesate / prelucrate date cu caracter personal prin încalcarea normelor legale, despre care a luat la cunoştinţă;
27. Informează imediat Responsabilul cu protecţia datelor (DPO) şi/sau responsabilul de securitate informatică cu privire la orice incident sau eveniment care afectează confidenţialitatea, integritatea şi diponibilitatea datelor cu caracter personal sau care poate produce prejudicii instituţiei.