ROMÂNIA
JUDEȚUL SUCEAVA
MUNICIPIULRĂDĂUȚI
CONSILIUL LOCAL

PROIECT DE HOTĂRÂRE
pentru aprobarea Regulamentului privind protecția datelor cu caracter personal în cadrul UAT Rădăuți

Consiliul Local al Municipiului Rădăuți, județul Suceava;
Având în vedere:

- Referatul de aprobare al domnului primar al Municipiului Rădăuți, Nistor Tătar, înregistrat cu nr. _____/_____
- Raportul compartimentului/serviciului de resort din cadrul aparatului de specilaitate al primarului, înregistrat sub nr. _____/_____
- Avizul Comisiei de specialitate din cadrul Consiliului Local, înregistrat sub nr. _____/_____
- Referatul de necesitate nr. 34210/27.04.2020
- Regulamentul (UE) 679/2016 GDPR privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu carácter personal si privind libera circulație a acestor date.
- Legea 190/2018 privind masuri de punere în aplicare a Regulamentului (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu carácter personal si privind libera circulație a acestor date.

În temeiul dispozițiilor art. 129 alin. (2) lit. a), 139 alin. (1), 196 alin. (1) lit. a) în OUG 57/2019 privind Codul Administrativ.

H O T Ă R Ă Ș T E :

Art.1 Se aprobă Regulamentul privind protecția datelor cu caracter personal în cadrul UAT Rădăuți conform Anexei 1 ce face parte integrantă din prezenta Hotărâre.

Art.2 Primarul municipiului Rădăuți, prin aparatul de specialitate, va duce la îndeplinire prevederile prezentei hotărâri.

INIȚIATOR,
Primar,
Nistor Tatar

AVIZEAZĂ PENTRU LEGALITATE,
Secretar general al municipiului
Marinică Sofroni

REGULAMENT GDPR UAT MUNICIPIUL RĂDĂUȚI
CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL

CAP. I DISPOZIȚII GENERALE

1. Despre instituția noastră

1.1. Suntem U.A.T. Municipiul Rădăuți, administrație publica locala, operator de date cu caracter personal, ce se angajează sa protejeze datele cu caracter personal ale persoanelor fizice, prelucrate de instituție, respectând legislația europeana si națională in materie (Regulamentul UE 679/2016 GDPR si Directiva UE 680/2016, Legea 190/2018 etc.), conform îndrumărilor Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

1.2. Datele de contact ale instituției noastre sunt:

U.A.T. MUNICIPIUL RĂDĂUȚI
Adresa de corespondenta: Municipiul Rădăuți, Strada: Piața Unirii nr. 2-4, Județul: Suceava;
Adresa de corespondenta electronica: Telefon: 0230.561.140, Fax: 0230.564.703,
E-Mail: relatiipublice@primariaradauti.ro, Portal: www.primariaradauti.ro.

1.3. Instituția noastră prelucrează date cu caracter personal referitoare la persoane fizice. Acestea pot reprezenta date în legătură cu contribuabilii, rezidenții, non rezidenții, ale partenerilor comerciali, vizitatorii instituției sau ai localității, angajații, candidații, voluntarii, colaboratorii, persoane ce accesează portalul de internet al instituției sau comunica cu noi prin orice mijloc de comunicare, etc;
1.4. Instituția noastră a adoptat măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Totodată s-au implementat soluții tehnice în vederea asigurării securității cibernetice a fluxurilor informatizate precum şi infrastructurii şi echipamentelor IT &C;
1.5. În acest sens prin politici, proceduri, regulamente, instruiri de personal şi prin desemnarea unui DPO Responsabil cu protecția datelor cu caracter personal, instituția noastră s-a aliniat la Regulamentul UE 679/2016 şi va face eforturi constante şi considerabile în vederea menținerii şi adoptării unor standarde cât mai înalte pentru protejarea datelor cu caracter personal ale persoanelor fizice vizate de prelucrările instituției noastre;

1.6. Datele de contact ale DPO Responsabilul cu protecția datelor cu caracter personal sunt:

U.A.T. MUNICIPIUL RĂDĂUȚI
Responsabilului cu Protecția Datelor cu Caracter Personal
Adresa de corespondenta:
U.A.T. Municipiul Rădăuți, Strada: Piața Unirii nr. 2-4, Mun. Rădăuți, Județul: Suceava;
Adresa de corespondenta electronica:
Telefon: 0230.561.140, Fax: 0230.564.703, E-Mail: dpo@primariaradauti.ro

2. Scopul şi Obiectivele Regulamentului

2.1. Scopul acestui regulament este de a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a drepturilor, cu privire la prelucrarea datelor cu caracter personal, în conformitate cu prevederile Regulamentului U.E. 679/2016 GDPR;
2.2. Conformitatea cu legislația si bunele practici privind protecția datelor cu caracter personal;
2.3. Transparența fața de modul de securizare si protejare a datelor stocate si prelucrate;
2.4. Protejarea instituției fata de posibilele riscuri referitoare la încălcarea securității datelor;
2.5. Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora;
2.6. Regulamentul stabilește măsuri tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării confidențialității datelor și informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente executate de angajații UAT Rădăuți;
2.7. Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate prevăzut Regulamentului UE 679/2016 GDPR;
2.8 Exercitarea drepturilor prevăzute în prezentul regulament nu poate fi restrânsă decât în cazurile expres și limitativ prevăzute de lege.

3. Domeniul de aplicare al Regulamentului
3.1. Regulamentul, se aplica tuturor angajaților UAT Rădăuți, cu atribuții de prelucrare a datelor cu caracter personal și persoanelor împuternicite ale UAT Rădăuți;
3.2. Regulamentul se aplica prelucrării datelor cu caracter personal, efectuat total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor;
3.3. Activitatea procedurală reprezintă aplicarea Regulamentului UE 679/2016 GDPR 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. GDPR se aplică direct în România începând cu 25 mai 2018.

4. Baza legală și documente de referință
4.1. Regulamentul UE 611/2016, al Comisiei Europene din 24 iunie 2013, privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice;
4.2. Regulamentul UE 679/2016, al Parlamentului European si a Consiliului Europei din 27 aprilie 2016, privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE
4.3. Directiva UE 680/2016, a Parlamentului European si a Consiliului Europei din 27 aprilie 2016, privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;

4.4. Directiva UE 1148/2016, a Parlamentului European si a Consiliului Europei din 6 iulie 2016, privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
4.5. Avizul 4/2007, al Grupului de lucru UE, privind conceptul de date cu caracter personal;
4.6. Legea nr. 102, din 3 mai 2005, a Parlamentului Romaniei, privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personale;
4.7. Legea nr. 129, din 15 iunie 2018, a Parlamentului Romaniei, pentru modificarea şi completarea Legii nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
4.8. Legea nr. 190/2018, din 31 iulie 2018, a Parlamentului Romaniei, privind măsuri de punere în aplicare a Regulamentului (UE) 679/2016, al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul general privind protecţia datelor);
4.9. Legea nr. 362/2018, din 28 decembrie 2018, privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;
4.10. Legea nr. 363, din 28 decembrie 2018, privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date;
4.11. Regulament ANSPDCP, din 2 noiembrie 2005, de organizare şi funcţionare a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, inclusiv cele cuprinse în Hotărârea Biroului permanent al Senatului nr.18/2019;
4.12. Decizia ANSPDCP nr. 128, din 22 iunie 2018, privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);
4.13. Decizia ANSPDCP nr. 133, din 3 iulie 2018 privind aprobarea Procedurii de primire şi soluţionare a plângerilor;
4.14. Decizia ANSPDCP nr. 161, din 9 octombrie 2018, privind aprobare a Procedurii de efectuare a investigaţiilor;
4.15. Decizia ANSPDCP, nr. 174, din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal;
4.16. Decizia ANSPDCP, nr. 184/2014, privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice;
4.17. Procedura ANSPDCP, din 9 octombrie 2018, de efectuare a investigaţiilor;

4.18. Informare ANSPDCP privind drepturile persoanelor vizate, extras din Reg. 679/2016;
4.19. Ghid orientativ ANSPDCP, de aplicare a Regulamentului GDPR;
4.20. Ghid ANSPDCP, privind Responsabilul cu protecția datelor DPO;
4.21. Ghid ANSPDCP, cu întrebări si răspunsuri cu privire la aplicarea Reg. 679/2016 GDPR;
4.22. Broșura ANSPDCP, Noul Regulament General privind Protecția Datelor;

5. Definiții si limbaj specific al legislației privind prelucrarea datelor cu caracter personal

5.1. Termenii și definițiile cele mai importante cu privire la această politică sunt următoarele:

5.1.1. **GDPR** - termenul de „GDPR" este abrevierea a „General Data Protection Regulation" sau în limba română, "RGPD - Regulamentul General privind Protecția Datelor", ambele abrevierii făcând referire la Regulamentului UE 679/2016, iar scopul acestei dispoziții legale este de a proteja datele cu caracter personal și a delimita clar modul în care acestea pot fi prelucrate;

5.1.2. **DPO** - termenul de „DPO" este abrevierea a „Data Protection Officer", Ofițer Responsabil cu protecția datelor cu caracter personal, desemnat în cadrul instituției cu atribuții privind protejarea datelor cu caracter personal, așa cum este definit în Regulamentului UE 679/2016;

5.1.3. **DCP - Date cu caracter personal** - orice informații privind o persoană fizică identificată sau identificabilă denumita „persoana vizată". O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator on-line, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

5.1.4. **Persoana vizată** - o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

5.1.5. **Operator** - persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

5.1.6. **Persoană împuternicită de operator** - persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

5.1.7. **Prelucrare** - orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

5.1.8. **Colectarea** - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale și din orice sursă;

5.1.9. **Înregistrarea** - consemnarea datelor cu caracter personal într-un sistem de evidență automată ori neautomată, care poate fi registru, fișier automat, bază de date sau orice formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire de date ori document, indiferent de modalitatea în care se înscriu datele;
5.1.10. **Organizarea** - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora;
Stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranță;
5.1.11. **Adaptarea** - transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;
5.1.12. **Modificarea** - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate, actualitate;
5.1.13. **Extragerea** - scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;
5.1.14. **Consultarea** - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioare;
5.1.15. **Utilizarea** - folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților operatorului ori destinatarului, dup caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;
5.1.16. **Dezvăluirea sau divulgarea** - a face disponibile date cu caracter personal către terți prin comunicare, transmitere, diseminare sau punerea la dispoziție în orice alt mod;
5.1.17. **Alăturarea** - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;
5.1.18. **Combinarea sau alinierea** - îmbinarea, unirea sau asamblarea unor date personale separate inițial, într-o formă nouă, prin criterii prestabilite, pentru scopuri anume determinate;
5.1.19. **Blocarea** - întreruperea prelucrării datelor cu caracter personal;
5.1.20. **Restricționarea** - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
5.1.21. **Ștergerea** - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența, inexactitatea;
5.1.22. **Transformarea** - operațiunea efectuat asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;
5.1.23. **Distrugerea** - aducerea la stare de neîntrebuințare, în condițiile legii, definitiv și irecuperabil, prin mijloace mecanice sau termice, a suportului fizică pe care au fost prelucrate date cu caracter personal;
5.1.24. **Creare de profiluri** - înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se afla persoana fizică respectiv deplasările acesteia;

5.1.25. **Pseudonimizare sau date anonime** - înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri tehnice și organizatorice care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
5.1.26. **Sistem de evidență a datelor** - înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
5.1.27. **Destinatar** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respect normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
5.1.28. **Utilizator** - înseamnă orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal; are calitatea de utilizator al datelor cu caracter personal, personalul Operatorului sau al împuternicitului acestuia ale cărei atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.
5.1.29. **Parte terță** - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoană împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
5.1.30. **Consimțimânt** - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o Declarație - sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
5.1.31. **Încălcarea securității datelor cu caracter personal** - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizat a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;
5.1.32. **Date genetice** - înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezulta în special în urma unei analize a unei mostre de material biologică recoltate de la persoană în cauză;
5.1.33. **Date biometrie** - înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
5.1.34. **Date privind sănătatea** - înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
5.1.35. **CNP - Codul numerică personal** - înseamnă un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a

stării civile a acesteia și de identificare în anumite sisteme informatice de către persoanele autorizate;
5.1.36. **ANSPDCP - Autoritate de supraveghere** - înseamnă Autoritatea Națională de Supraveghere a Datelor cu Caracter Personal;

CAP. II PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

6. Principii ale prelucrărilor datelor cu caracter personal
6.1. Regulamentul GDPR este guvernat de o serie de principii fundamentale privind prelucrarea datelor cu caracter personal, pe care le enumeram in prezentul Regulament:
6.1.2. **„Integritate și confidențialitate"** - date prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.
6.1.2. **„Legalitate, echitate și transparență"** - prelucrare legala, echitabila și transparenta față de persoana vizată;
6.1.3. **„Reducerea la minimum a datelor"** - date personale adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
6.1.4. **„Limitări legate de scop"** - datele sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89;
6.1.5. **„Limitări legate de stocare"** - date păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate;
6.1.6. **„Exactitate"** - date exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
6.2. Instituția noastră se va asigura că respectă toate aceste principii atât în procesul de prelucrare pe care îl desfășoară în prezent, cât și ca parte a introducerii de noi metode de procesare, prelucrare, stocare, criptografieze si securizare cum ar fi noile sisteme informatice.
6.3. **„Responsabilitate"** - Instiuția este responsabil de respectarea principiilor GDPR și are obligația de a demonstra respectarea principiilor și a legislației, prin documentarea deciziilor luate cu privire la activitățile de prelucrare, astfel:
6.3.1. Toate prelucrările de date cu caracter personal trebuie să fie legală și echitabilă;
6.3.2. Asigurarea transparenței pentru persoanele fizice vizate privind modul în care sunt colectate, utilizate sau prelucrate datele cu caracter personal și în ce măsură sunt sau vor fi prelucrate;

6.3.3. Toate informațiile și comunicările referitoare la prelucrarea respectivelor date cu caracter personal trebuie să fie ușor accesibile și ușor de înțeles și ca trebuie să se utilizeze un limbaj simplu și clar;
6.3.4. Persoanele fizice trebuie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care pot să își exercite drepturile în legătură cu prelucrarea;
6.3.5. Scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite și legitime și să fie determinate la momentul colectării datelor respective;
6.3.6. Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate, este limitată strict la minimum;
6.3.7. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinită în mod rezonabil prin alte mijloace;
6.3.8. Operatorul trebuie să stabilească termene pentru ștergere sau revizuirea periodică.
6.3.9. Operatorul trebuie să ia toate masurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse;
6.3.10. Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizat a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

CAP. III TEMEIURILE LEGALE ALE PRELUCRAILOR DE DATE CU CARACTER PERSONAL

7. Temeiurile legale in baza cărora prelucram datele cu caracter personal
7.1. Regulamentul UE 679/2016, specifica șase temeiuri în baza cărora se pot procesa datele cu caracter personal:

7.1.2. **„Obligația legală"** - În cazul instituitei noastre fiind o administrație publica locala în care datele cu caracter personal trebuie să fie colectate și prelucrate pentru a ne conforma legii, nu este necesar consimțământul explicit;

7.1.3. **„Îndeplinirea unor sarcini care deservesc interese publice"** - Este si cazul instituitei noastre întrucât trebuie să îndeplinească sarcini pe ce deservesc în interesul public sau ca parte a unei obligații oficiale, situații când nu va fi solicitat consimțământul persoanei vizate;

7.1.4. **„Încheierea sau executarea unui contract"** - Întrucât instituția noastră încheie contracte cu alte instituții, autorități publice sau colaboratori persoane juridice sau fizice, cazuri în care datele cu caracter personal colectate și prelucrate sunt necesare pentru a încheia sau executa un contract cu persoana vizată, nu este necesar consimțământul explicit.

7.1.5.„ **Interesul legitim"** - Sunt situații speciale in cadrul cărora este necesara prelucrarea datelor cu caracter personal în interesul legitim al instituitei noastre și prin analize specifice se considera că aceste prelucrări nu afectează în mod semnificativ drepturile și libertățile persoanei vizate, atunci aceasta poate fi definită ca fiind motivul legal al prelucrării.

7.1.6. **„Interesele vitale ale subiectului datelor"** - Pentru a proteja interesele vitale ale persoanelor vizate sau ale altor persoane fizice, in situații critice, vitale acestor persoane, instituția noastră va prelucra datele personale având ca temei protejarea intereselor vitale

ale persoanelor vizate. In acest sens instituția va păstra in evidentele sale dovezile prelucrării din aceste situații.

7.1.7. **„Consimțământul"** – În afara situațiilor prezentate mai sus, instituția noastră acorda o maxima importanta obținerii acordului explicit din partea unei persoane vizate pentru colectarea și prelucrarea datelor. În situațiile speciale, dar si in cazul copiilor sub vârsta de 16 ani va fi obținut consimțământul reprezentanților legali.
La momentul obținerii consimțământului pentru prelucrarea datelor cu caracter personal, persoanele vizate vor fi informate despre utilizarea datelor cu caracter personal prelucrate de instituția noastră si li se vor explica drepturile acestora cu privire la datele lor, cum ar fi dreptul de retragere a consimțământului. Toate informațiile vor fi furnizate într-o formă accesibilă, scrise în limbaj clar și gratuit, disponibile atât in sediul instituitei noastre cat si in portalul de internet.

CAP. IV INFORMAREA PERSOANELOR FIZICE VIZATE DE PRELUCRĂRILE DE DATE

8. Dreptul la informare al persoanei vizate

8.1. Persoanele vizate au dreptul să fie informate despre felul în care instituția le prelucrează datele;
8.2. Informarea trebuie realizată, dacă datele provin de la subiect, la momentul colectării datelor;
8.3. Datele provin din alte surse, informarea se va realiza în mult o lună de la momentul obținerii datelor;
8.4. Informarea trebuie să fie concisă, transparentă, inteligibilă, ușor accesibilă și într-un limbaj simplu și clar;
8.5. Informarea copiilor trebuie să se realizeze într-un limbaj pe care aceștia îl pot înțelege;
8.6. Articolul 12 din Regulament prevede că operatorul trebuie să realizeze informarea persoanei vizate astfel:
- într-o formă concisă, transparentă, inteligibilă și ușor accesibilă;
- utilizând un limbaj clar și simplu;
- în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic;
- la solicitarea persoanei vizate, informațiile pot fi prezentate oral;
- informarea trebuie să fie gratuită.;
8.7. Pentru o informare corectă a persoanelor fizice vizate de prelucrările de date se se vor consulta documentația privind informarea persoanelor vizate, precum:
„G03 Ghid privind informarea persoanelor vizate";
„PR01 Procedura de notificare privind confidențialitatea";
8.8. Informarea persoanelor vizate se va efectua prin afișarea în cadrul instituției, la avizier, în locuri destinate informării precum și in cadrul departamentelor ce interacționează cu persoanele fizice a documentului „N03 Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal;", document ce va fi pus la dispoziție și explicat persoanelor fizice vizate de prelucrările de date cu caracter personal de către instituție;
8.9. De asemeni, din prisma datelor cu caracter personal, se va avea în vedere informarea angajaților, a candidaților, a partenerilor contractuali (operatori economici), a consilierilor locali, a peroanelor juridice împuternicite, etc., utilizând următoarele note de informare:
„N01 Nota informare angajați, privind prelucrarea datelor cu caracter personal";
„N02 Nota informare candidați, privind prelucrarea datelor cu caracter personal";
„N03 Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal";

„N04 Nota informare parteneri contractuali, privind prelucrarea datelor cu caracter personal''
„N05 Scrisoare de informare din partea instituției'';
„N06 Scrisoare conformitate cu GDPR'';
„N07 Nota informare consilieri locali, privind prelucrarea datelor cu caracter personal'';
„N08 Scrisoare de conformitate cu GDPR, către persoanele juridice împuternicite'';
8.10. Informările se vor realiza prin intermediul angajaților din fiecare compartiment sau direcție ce lucrează cu publicul și cu operatorii comerciali, la indicațiile Responsabilului cu protecția datelor cu caracter personal și a superiorilor ierarhici;
8.11. O atenție deosebită se va acorda informării persoanelor fizice, privind prelucrările de date cu caracter personal, în situația înregistrărilor audio, video sau fotografiere, supravegherea video CCTV a instituției, a imobilelor si a spatiilor publice, înregistrări (audio-video-foto) și difuzări ale: ședințelor, investițiilor (construcții noi, modernizări, amenajări), festivităților, evenimentelor culturale sau de orice natura, din primărie, din instituțiile subordonate sau colaboratoare si de pe raza localității, in vederea mediatizării si popularizării localității și/sau a instituției, în mass media, radio, tv, publicații, precum si în mediul internet;
8.12. Astfel în funcție de fiecare situație, la toate obiectivele unde sunt instalate camerele video ce captează imagini, ale sistemului de supraveghere, sau prin alte mijloace tehnice se înregistrează imagini video, audio, se fotografiază, persoanele fizice vor fi avertizate de existența camerelor de supraveghere, sau a acestor mijloace tehnice, prin semne adecvate si note de informare, afișate vizibil, în mod permanent în zona supravegheată;
8.13. Instituția, va informa în prealabil, persoanele vizate, în formă scrisă, prin publicarea pe portalul de internet al instituției, prin afișare la sediul instituției sau la evenimente, conferințe, ședințe, etc de faptul ca instituția va prin mijloace tehnice va efectua înregistrări video, audio, ori va fotografia sau va difuza în mediul internet sau mass media (radio, tv) în direct sau sub formă de înregistrări, datele captate și prelucrate;
8.14. În acest sens, în scopul informării se va utiliza documentul, „POL14 Politica privind supravegherea video prin sistem CCTV''.
8.15. DPO - Responsabilul cu protecția datelor, va face demersurile in vederea informării prin intermediul portalului de internet al instituției astfel:
8.15.1. Crearea unei secțiuni distincte denumita GDPR sau Protecția Datelor, vizibila si accesibila din prima pagina a portalului, în cadrul unui meniu, buton, sau legătură (link) web; Secțiunea GDPR va trebui sa conțină in prin plan, vizibil, datele de contact ale Responsabilului cu protecția datelor, in vederea exercitării drepturilor de către persoanele vizate si datele de contact ale ANSPDCP Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
8.15.2. Tot in aceasta secțiune se vor afișa documentele:
„N03 Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal'';
„POL09 Politica privind confidențialitatea a portalului de internet'';
„POL01 Politica generala privind protecția datelor cu caracter personal'';
„POL14 Politica privind supravegherea video prin sistem CCTV''
8.15.2. La prima accesare a portalului, va trebui sa apară o opțiune vizibila in prin plan ce sa conțină următoarele doua elemente principale:
Un link prin accesarea căruia vizitatorii vor avea acces la „POL09 Politica privind confidențialitatea a portalului de internet'';

Un buton de „Accept" prin care vizitatorii portalului își vor da acceptul referitor la aceasta politica.

CAP. V CONSIMȚĂMÂNTUL PERSOANLOR FIZICE VIZATE DE PRELUCRARI

9. Consimțământul persoanelor fizice vizate de prelucrările de date cu caracter personal

9.1. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru, prin înmânarea și explicarea notei de informare cu privire la datele cu caracter personal;

9.2. În funcție de situație notele de informare sunt disponibile pentru angajații instituției, pentru viitorii candidați și în mod special pentru persoanele fizice sau reprezentanții legali ai minorilor, vizați de prelucrările de date cu caracter personal ce necesită consimțământul;

9.3. Pentru situațiile în care prelucrarea se bazează pe consimțământ, instituția trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul expres, neechivoc, liber și informat pentru prelucrarea datelor sale cu caracter personal;

9.4. Persoana fizică vizată de prelucrarea datelor cu caracter personal, are dreptul să își retragă în orice moment consimțământul, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

9.5. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.

9.6. **UAT Municipiul Rădăuți**, va solicita consimțământul în toate situațiile în care prelucrarea de date nu este o obligație legală, în situațiile în care se solicită copii ale documentelor necesare pentru documentarea sau procesarea solicitărilor însă legislația nu o prevede în mod expres în acele situații, sau în următoarele situații:

9.6.1. În vederea realizării procesului de recrutare sau selecție de personal, de la candidați;

9.6.2. În situațiile în care prelucrarea vizează copii minori sub 16 ani, se va solicita consimțământul tutorelui sau reprezentanților legali;

9.6.3. În vederea desfășurării unor anchete sociale sau a unor acțiuni ce implică colectarea si prelucrarea de date cu caracter personal (organizarea de evenimente, concursuri, premieri, burse, tombole, etc);

9.6.4. În vederea solicitării datelor de contact (telefon, email, adresă de corespondență) pentru furnizarea de informații, ce țin de servicii, evenimente, manifestări, comunicări, etc;

9.6.5. Pentru portalul de internet, in situația creării de conturi de utilizator sau pentru abonarea la e-mail în scopuri informative, privind activitatea instituției, servicii, evenimente;

9.7. În vederea obținerii consimțământului, după informarea prealabila prin intermediul notelor de informare, în funcție de situație se vor utiliza următoarele documente specifice:

9.7.1. „F10 Formular pentru obținerea consimțământului";

9.7.2. „F11 Formular pentru obținerea consimțământului părintelui";

9.8. Responsabilul cu protecția datelor cu caracter personal, va informa toți angajații cu privire obligativitatea de informare a persoanelor vizate prin notele de informare, precum și de situațiile privind solicitarea consimțământului, în funcție de caz, fără a se limita la situațiile expuse în prezentul Regulament;

9.9. Notele de informare precum și formularele pentru obținerea consimțământului se vor distribui de către Responsabilul cu protecția datelor cu caracter personal, către toate compartimentele sau direcțiile ce desfășoară activități cu publicul sau interacționează cu persoanele fizice sau juridice, conducătorii de compartimente și direcții având obligația de a le distribui angajaților în vederea obținerii consimțământului de la persoanele fizice în toate situațiile in care se impune;

9.10. Documentația privind informarea și obținerea consimțământului se va oferi gratuit, iar persoanele fizice ce vor solicita copii ale documentației prin care și-au dat consimțământul li se vor elibera gratuit;
9.11. Toată documentația privind obținerea consimțământului, semnată de către persoanele fizice ce și-au dat acordul privind prelucrările de date cu caracter personal se va returna săptămânal, Responsabilului cu protecția datelor cu caracter personal, care le va depozita și arhiva în ordine alfabetica, completând în acest sens un registru al persoanelor fizice ce și-au dat consimțământul privind prelucrarea de date cu caracter personal.

CAP. VI DATELE CU CARACTER SPECIAL

10. Prelucrarea datelor cu funcție de identificare generală
10.1. Numărul de identificare național, este numărul prin care se identifică o persoană fizică în anumite sisteme de evidentă și care are aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială de sănătate.
10.2. Aceste date cu caracter personal, vor fi prelucrate, doar pentru stabilirea identității persoanelor fizice cu obligația ca prelucrarea să fie prevăzută în mod expres de o dispoziție legală. Astfel, numărul de identificare națională sau orice alt identificator cu aplicabilitate general este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate.

11. Prelucrarea categoriilor de date cu caracter special
11.1. În vederea respectării Regulamentului U.E. 679/2016, se va avea în vedere restricționarea prelucrărilor de date cu caracter personal speciale, precum datele despre originea rasială sau etnică, apartenența și opiniile politice, confesiunea religioasă, convingerile filozofice, prelucrarea de date genetice, de date biometrie, date medicale, sau date privind viața sau orientarea sexuală ale persoanelor fizice;
11.2. Prelucrarea datelor cu caracter special se va putea realiza doar în următoarele condiții:
11.2.1. În situația în care persoană vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, pentru fiecare scop în parte;
11.2.2. Dacă prelucrarea se refera la date cu caracter personal făcute publice în mod voit de către persoana vizată;
11.2.3. Atunci când prelucrarea este necesara din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;
11.2.4. În vederea protejării intereselor vitale ale persoanei vizate, atunci când persoana vizată se afla in incapacitate fizică sau juridica de a-și da consimțământul;
11.2.5. Dacă prelucrarea este necesară pentru interesul public în domeniul sănătății publice, în situații precum protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale;
11.2.6. Pentru scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență

medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistenta social;
11.2.7. În scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă, al securității sociale sau al protecției sociale;
11.2.8. Doar dacă sunt autorizate de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă;
11.2.8. Atunci când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
11.2.9. Prelucrarea poate fi efectuată în scopuri în scopuri de cercetare științifică sau istorică, de arhivare în interes public ori în scopuri statistice;
11.2.10. Prelucrarea poate fi efectuata de către un ONG, asociație , fundație fără scop lucrativ în cadrul activităților lor legitime și cu garanții adecvate care să aibă un specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să fie pe seama membrilor sau la foștii membri ai entității sau prelucrări ce au la bază persoane ce au legătură cu scopurile sale sub condiția ca datele cu caracter personal sa fie comunicate terților doar cu consimțământul persoanelor vizate;
11.3. Aceste prelucrări se vor efectua în temeiul dreptului Uniunii sau al dreptului intern, ori al normelor stabilite de organisme naționale competente sau în temeiul temeiul unor contracte încheiat cu un cadru care prevăd măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, cu respectarea secretului profesional, a obligațiilor de confidențialitate, etc.

12. Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni
12.1 Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de legislația națională care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate;
12.2. Orice registru cuprinzător al condamnărilor penale se tine numai sub controlul unei autorități de stat.

13. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video
13. 1. Prin intermediul sistemului de supraveghere video CCTV, instituția noastră, prelucrează date aparținând angajaților, vizitatorilor (rezidenți sau non rezidenții), contribuabili, petenți, colaboratori, parteneri comerciali, voluntari și a oricăror altor persoane (cetățeni), care intră în sediul Primăriei Municipiului Rădăuți din str. Piața Unirii nr. 2-4, Mun. Rădăuți, Jud. Suceava, sau în incinta Muzeului Etnografic ,, Samuel si Eugenia Ioneț'' din Mun. Rădăuți, str. Piața Unirii nr. 63, sau care trec prin parcurile din Municipiul Rădăuți: Parcul ,,Bogdan Vodă Rădăuți'', prin Parcul Central (Flacăra), cu zona locului de joacă pentru copii și Piața agroalimentară a Mun. Rădăuți;
13.2. Instituția utilizează sistemul CCTV, pentru supravegherea instituției, a imobilelor, a obiectivelor si a spatiilor publice, în scopul asigurării securității persoanelor și bunurilor, paza și protecția bunurilor, imobilelor, a valorilor, control al accesului, ordine și liniște publică, etc.
13.3. Se supraveghează prin mijloace video: sediul instituției cu zonele de acces, spațiile destinate angajaților și vizitatorilor, zonele cu acces restricționat precum casieria unității,

zona taxe și impozite, împrejurimile clădirilor pentru a proteja spațiile exterioare, zonele publice menționate mai sus;
13.4. Scopul urmărit este acela de a supraveghea în timp real zonele de interes prin intermediul monitoarelor amplasate în dispeceratul video, precum și înregistrarea și stocarea imaginilor preluate din aceste zone. Perioada minima si maxima de stocare este 30 de zile;
13.5. Camerele de supraveghere video au fost amplasate cu atenție pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit;
13.6. Nu sunt monitorizate zonele în care există un nivel ridicat al așteptărilor privind viața privată, precum birourile, toaletele și alte locații similare;
13.7. În mod excepțional, în cazul unor necesități în materie de securitate justificate în mod corespunzător, se pot instala camere în astfel de locuri, însă numai după efectuarea unei evaluări de impact și după informarea responsabilului cu protecția datelor personale. În astfel de cazuri, se va amplasa un anunț specific și vizibil în locurile respective;
13.8. O atenție deosebită se va acorda informării persoanelor fizice, privind prelucrările de date cu caracter personal, în situația înregistrărilor audio, video sau fotografiere, supravegherea video CCTV a instituției, a imobilelor si a spatiilor publice, înregistrări (audio-video-foto) și difuzări ale: ședințelor, investițiilor (construcții noi, modernizări, amenajări), festivităților, evenimentelor culturale sau de orice natura, din primărie, din instituțiile subordonate sau colaboratoare si de pe raza localității, in vederea mediatizării si popularizării localității și a instituției, în mass media, radio, tv, publicații, precum si în mediul internet;
13.9. Astfel în funcție de fiecare situație, la toate obiectivele unde sunt instalate camerele video ce captează imagini, ale sistemului de supraveghere, sau prin alte mijloace tehnice se înregistrează imagini video, audio, se fotografiază, persoanele fizice vor fi avertizate de existența camerelor de supraveghere, sau a acestor mijloace tehnice, prin semne adecvate si note de informare, afișate vizibil, în mod permanent în zona supravegheată;
13.10. Instituția, va informa în prealabil, persoanele vizate, în formă scrisă, prin publicarea pe portalul de internet al instituției, prin afișare la sediul instituției sau la evenimente, conferințe, ședințe, etc de faptul ca instituția va prin mijloace tehnice va efectua înregistrări video, audio, ori va fotografia sau va difuza în mediul internet sau mass media (radio, tv) în direct sau sub formă de înregistrări, datele captate și prelucrate.

14. Prelucrarea datelor DCP în scopul informării, comunicărilor sau marketing direct
14.1. Instituția va putea prelucra date cu caracter personal ale persoanelor fizice, în special date privind modalitatea de contactare si de comunicare prin intermediul corespondenței clasice sau electronice precum: nume și prenume, adresa de corespondență, adresă de poșta electronică, telefon fix, telefon mobil, fax, etc, doar prin exprimarea în formă scrisă sau electronică a consimțământului persoanelor vizate;
14.2. Aceste prelucrări se vor face în următoarele scopuri; comunicări și informări a contribuabililor, concursuri, premieri, burse, tombole, marketing direct, etc;
14.3. Efectuarea de comunicări comerciale pentru serviciile instituției, inclusiv cele dezvoltate împreună cu un partener, prin orice mijloc de comunicare, inclusiv prin intermediul serviciilor de comunicații electronice.
14.4. În anumite situații, doar prin acordare consimțământului de către persoana vizată, se pot prelucra sau transfera date cu caracter personal în scopuri de marketing direct pentru

oferirea de servicii sau produse, în mod direct sau prin partenerii comerciali ai instituției, prin mijloace de comunicare clasică sau electronica;
14.5. Persoanele vizate, în aceste situații, vor putea uzita de drepturile lor pentru a solicita în orice moment ca datele cu caracter personal sa nu mai fie prelucrate de către instituție sau de către terți colaborator

CAP. VII DREPTURILE PERSOANELOR FIZICE VIZATE DE PRELUCRĂRILE DE DATE ,,DCP''

15. Drepturile persoanelor fizice vizate de prelucrările DCP (a datelor cu caracter personal)
15.1. Instituția implementat o politica astfel ca fiecare dintre drepturile implicate cu propriile sale aspecte și provocări specific sa fie respectate iar persoanele vizate sa își poată exercita pe deplin drepturile garantate prin legislație;
15.2. Întrucât, drepturile nu sunt absolute, există si excepții. În toate cazurile, instituția va decide dacă o cerere este întemeiată raportând-se la legislația GDPR. În unele cazuri, pentru a stabili dacă o cerere este întemeiată sau nu, se vor consulta departamentul juridic al instituției sau consultanții juridici externi;
15.3. Răspunsul la cererea persoanei vizate se va face în termen de o lună, fără întârzieri nejustificate. Perioada se poate prelungi la maxim doua luni în situații mai complexe, însă cu obligația de a informa persoana vizată cu privire la motivele întârzierii;
15.4. Indiferent de modalitatea prin care persoana vizată a solicitat instituției cererea, se va formula răspuns ținând cont de doleanța persoanei vizate și de informațiile furnizate în acest sen;
15.5. Dacă cererea este întemeiată, se va facilita exercitarea drepturilor. Dacă cererea nu este întemeiată, se va comunica motivul refuzului persoanei vizate și i se va comunica dreptul de a depune o plângere la ANSPDCP și dreptul de a se adresa Justiției;
15.6. Toate informațiile furnizate persoanei vizate, în temeiul Regulamentului UE 679/2016 GDPR se vor oferi gratuit. Însă în situații excesive, vădit nefondate sau repetitive, repetitiv, instituția poate:
15.7. Să refuze să dea curs cererii sub obligația de a demonstra caracterul nefondat sau excesiv al cererii;
15.8. Să perceapă o taxa rezonabilă raportată la costurile administrative pentru furnizarea informațiilor.

16. Modalitatea de contact, identitatea persoanelor și formularistica specifică
16.1. În vederea exercitării drepturilor, persoanele vizate se vor putea adresa instituției prin DPO – Responsabilul cu protecția datelor cu caracter personal care are atribuții în acest sens;
16.1. Informarea persoanelor vizate în privința datelor de contact, se va realiza prin intermediul portalului de internet, datele vor fi publicate la avizierul instituției, în notele de informare sau în mod direct prin intermediul angajaților ce au contact cu persoanele vizate.
16.2. Datele de contact în vederea exercitării drepturilor persoanelor vizate sunt:
U.A.T. MUNICIPIUL RĂDĂUȚI
Responsabilului cu Protecția Datelor cu Caracter Personal
Adresa de corespondenta:
U.A.T. Municipiul Rădăuți, Strada: Piața Unirii nr. 2-4, Mun. Rădăuți, Județul: Suceava;
Adresa de corespondenta electronica:
Telefon: 0230.561.140, Fax: 0230.564.703, E-Mail: dpo@primariaradauti.ro;

16.3. Pentru aşi putea exercita drepturile, DPO – Responsabilul cu protecţia datelor cu caracter personal va pune la dispoziţia solicitanţilor o cerere tip pentru accesul la date, prin care se va verifica identitatea solicitantului, în situaţiile comunicărilor electronice sau prin corespondenţă şi se vor putea stabili cu exactitate doleanţele persoanei vizate, pentru a i se asigura pe deplin drepturile conform Regulamentului UE 679/2016 GDPR.
16.4. În funcţie de solicitare se va transmite persoanei vizate tipul de cerere aferent:
16.4.1. C01 Cerere pentru exercitarea dreptului la acces;
16.4.2. C02 Cerere pentru exercitarea dreptului pentru rectificarea datelor cu caracter personal;
16.4.3. C03 Cerere pentru exercitarea dreptului de ştergere a datelor cu caracter personal;
C04 Cerere pentru exercitarea dreptului restricţionarea prelucrării datelor cu caracter personal;
16.4.4. C05 Cerere pentru exercitarea dreptului de portabilitate a datelor cu caracter personal;
16.4.5. C06 Cerere pentru exercitarea dreptului la opoziţia a prelucrării datelor cu caracter personal;
16.4.6. C07 Cerere pentru exercitarea dreptului la retragerea consimţământului;
16.4.7. C08 Cerere pentru exercitarea dreptului la opoziţie privind prelucrarea automata a datelor cu caracter personal;

17. Dreptul de retragere a consimţământului
17.1. În vederea exercitării dreptului de retragere a consimţământului, persoana vizată poate si are dreptul de a retrage consimţământul în cazul în care baza pentru prelucrarea datelor sale cu caracter personal este cea a consimţământului (adică prelucrarea nu se bazează pe alt temei legal, precum contractul, obligaţia legală, interesul legitim, interesele vitale sau interesul public);
17.2. Înainte de a exclude prelucrarea datelor cu caracter personal ale persoanei vizate, trebuie să se confirme că consimţământul este într-adevăr bază a prelucrării. În caz contrar, dacă prelucrarea nu se bazează pe un alt temei legal, precum contractul, obligaţia legală, interesul legitim, interesele vitale sau interesul public, chiar împreună cu temeiul consimţământului, cererea va fi respinsă. În caz contrar, se va da curs cererii;
17.2. Acordarea şi retragerea consimţământului vor fi disponibile pe cale electronica;
17.3. În cazul în care consimţământul implică un copil (persoana sub 16 ani) retragerea consimţământului, trebuie să fie autorizată de titularul răspunderii părinteşti asupra copilului.

18. Dreptul la informare
18.1. În momentul în care datele cu caracter personal sunt colectate de la persoana vizată sau obţinute din alte surse, există cerinţa de a informa persoana vizată despre scopul utilizării acestor date şi despre drepturile pe care le are asupra lor. Conformitatea cu acest drept este gestionată si explicata in documentul denumit, ,,PR04 Procedura privind cererile persoanelor vizate'';, care descrie ce informaţii trebuie furnizate şi explică cum şi când trebuie îndeplinit acest pas;
18.2. În toate situaţiile în care datele cu caracter personal ale persoanei vizate sunt colectate direct de la aceasta, instituţia, în momentul obţinerii datelor, va furnizează persoanei vizate următoarele informaţii:
18.2.1 Identitatea şi datele de contact ale operatorului sau al operatorului împuternicit;

18.2.2. Datele de contact ale Responsabilului cu protecția datelor;
scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridică al prelucrării;
18.2.3. Interesele legitime urmărite de operator sau de o parte terță, dup este cazul;
destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
18.2.4. Perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
18.2.5. Existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

18.3. Daca prelucrarea se bazează pe consimțământul persoanei vizate, se vor comunica si următoarele:
18.3.1. Existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
dreptul de a depune o plângere în fata unei autorități de supraveghere.
18.3.2. Se vor comunica persoanei vizate și situația în care furnizarea de date cu caracter personal reprezint o obligație legală sau contractuală, necesară pentru încheierea unui contract și dacă persoana vizată este obligată să furnizeze aceste date și care sunt eventualele consecințe ale nerespectării acestei obligații;

19. Dreptul de acces
19.1. Persoana vizată are dreptul să solicite organizației o confirmare că datele personale sunt prelucrate, iar în caz afirmativ, are dreptul de a obține o copie a acestor date, precum și următoarele informații:
19.1.1. Scopurile prelucrării;
19.1.2. Categoriile datelor cu caracter personal în cauză;
19.1.3. Destinatarii sau categoriile de destinatari ai datelor, dacă există, în special orice țări terțe sau organizații internaționale;
19.1.4. Durata de stocare a datelor cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade);
19.1.5. Drepturile persoanei vizate la rectificarea sau ștergerea datelor sale cu caracter personal și restricționarea sau opoziția față de prelucrare;
19.1.5. Dreptul persoanei vizate de a depune o plângere la o autoritate de supraveghere;
Informații privind sursa datelor, dacă nu provin direct de la persoana vizată;
19.1.6. Dacă datele personale vor face obiectul unor decizii automate, inclusiv crearea de profiluri și, dacă da, logica acestei decizii sau profilări și eventualele consecințe implicate;
19.1.7. În cazul în care datele sunt transferate unei țări terțe sau unei organizații internaționale, informații privind garanțiile care se aplică;
19.2. În cele mai multe cazuri, va trebui să dam acces persoanei la date, cu excepția situației când cererea este vădit nefondată sau excesivă.

20. Dreptul la rectificare
20.1. În cazul în care datele cu caracter personal sunt inexacte, persoana vizată are dreptul să solicite corectarea și completarea datelor personale incomplete pe baza informațiilor pe care le furnizează;

20.2. Dacă este necesar, instituția noastră va lua măsuri suplimentare pentru a verifica dacă informațiile furnizate de persoană sunt corecte înainte de a opera modificarea.

21. Dreptul la ștergere („dreptul de a fi uitat")

21.1. Persoana vizată are dreptul să solicite instituției noastre să șteargă fără întârziere datele cu caracter personal care o privesc în următoarele situații:

21.1.1. Datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

21.1.2. Persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;

21.1.3. Persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea;

21.1.4. Datele cu caracter personal au fost prelucrate ilegal;

21.1.5. Datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;

21.2. Ștergerea datelor nu se va realiza in următoarele situații:

21.3. Datele sunt necesare pentru exercitarea dreptului la liberă exprimare și informare;
datele sunt necesare pentru îndeplinirea unei obligații legale sau a unui interes public ori a unui interes legitim;

21.4. Din motive de interes public în domeniul sănătății publice;

21.5. In scopuri de arhivare în interes public;

21.6. Pentru constatarea, exercitarea sau apărarea unui drept în instanță.

22. Dreptul la restricționarea prelucrării

22.1 Persoana vizată își poate exercita dreptul la restricționarea prelucrării în următoarele situații:

22.1.1. Persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;

22.1.2. Prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;

22.1.3. Operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;

22.1.4. Persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1) din Regulamentul GDPR, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate;

22.2. Instituția noastră, în situația în care primește o cerere de restricționare, va verifica dacă cererea de încadrează într-unul din cazurile de mai sus, iar pentru a se lua o decizie potrivită, se va apela la DPO Responsabilul cu protecția datelor.

22.3. În cazul în care se vor restricționa datele, acestea vor rămâne stocate, dar nu pot fi prelucrate fără consimțământul persoanei, însă vor putea fi prelucrate pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

22.4 În toate cazurile, de restricționare a prelucrării, persoana vizată care a obținut restricționarea prelucrării va fi informată de către instituție înainte de ridicarea restricției de prelucrare.

23. Dreptul la portabilitatea datelor

23.1. Articolul 20 din Regulamentul GDPR, specifica faptul ca, persoana vizată are dreptul să solicite ca datele personale să fie furnizate într-un format "structurat, utilizat în mod obișnuit și care poate fi citit de mașină" și să transfere datele respective unei alte părți, de exemplu alt furnizor de servicii. Aceasta se aplică datelor cu caracter personal pentru care prelucrarea se bazează pe consimțământul persoanei vizate, pe temeiul legal al contractului sau în situația în care prelucrarea este efectuată prin mijloace automate;

23.2. Instituția noastră se va conforma si in aceasta situație in funcție de posibilitățile tehnice existente in cadrul instituției precum si ale operatorului unde se dorește purtarea acestor date.

23.3. Persoana vizată poate, de asemenea, solicita ca datele personale să fie transferate direct de la un operator la altul.

24. Dreptul la opoziție

24.1. Conform Regulamentului GDPR, persoana vizată are dreptul de a se opune prelucrării care se bazează pe interesul legitim al operatorului sau al unei terțe părți sau interesul public.

24.2. Odată ce obiecția a fost făcută, instituția trebuie să justifice motivele pe care se bazează prelucrarea și să suspende prelucrarea până când decizia a fost luată.

24.3. Instituția nu mai prelucrează datele cu caracter personal, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

25. Drepturi în legătură cu deciziile automate, inclusiv crearea profilurilor

25.1. Persoana vizată are dreptul să nu facă obiectul unei decizii automate, inclusiv crearea de profiluri în cazul în care decizia are un efect semnificativ sau juridic asupra acesteia. 30.2. Persoana vizată are, de asemenea, dreptul de a-și exprima punctul de vedere, de a solicita intervenție umană și de a contesta decizia.

25.2. Se exceptează de la acest drept, următoarele situații:

25.2.1. Este necesară pentru încheierea sau executarea contractului;

25.2.2. Este autorizată prin lege națională sau europeană;

25.2.3. Se bazează pe consimțământul explicit al persoanei vizate.

25.3. Instituția va pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia;

25.4. Pentru a evalua temeinicia unei astfel de cereri, instituția va decide dacă excepțiile de mai sus se vor aplica situației, iar DPO Responsabilul cu protecția datelor va analiza situația si va oferi un răspuns persoanei vizate.

CAP. VIII RESPONSABILITATEA OPERATORULUI

26. Politici si responsabilități ale operatorului

26.1. În vederea protejării datelor cu caracter personal și pentru respectarea drepturilor persoanelor vizate, instituția noastră a adoptat măsuri tehnice și organizatorice și a implementat soluții tehnice în vederea asigurării securității cibernetice a fluxurilor informatizate precum și infrastructurii și echipamentelor IT &C. Astfel s-au adoptat politici și proceduri pentru a se putea atinge standard cat mai înalte în vederea alinierii cu Regulamentul UE 679/2016.

27. Politica instituției privind securitatea informațiilor

27.1. Instituția noastră a conceput „POL08 Politica privind securitatea informației" cu scopul de a conștientiza și familiariza personalul instituției cu privire la metodele de protecție și securitate pentru asigurarea confidențialității, integrității și disponibilității informației;

27.2. De asemenea, politica conturează metodele acceptabile de utilizare a resurselor informatice. Resursele informaționale vor fi utilizate într-o manieră aprobată, etică și în conformitate cu prevederile legale pentru a evita pierderea sau deteriorarea operațiunilor curente, a imaginii sau a activelor financiare. Angajații trebuie să se adreseze conducerii instituției înainte să se angajeze în orice activitate care nu este acoperită de prezenta politică.

27.3. Această Politică se aplică întregului personal, instituțiilor colaboratoare, partenerilor și colaboratorilor externi care au acces la sistemul informatic al instituției;

27.4. Obiectivele prezentei politici privind securitatea informației sunt:

27.4.1. Dezvoltarea unei strategii privind securitatea sistemelor informatice;

27.4.2. Promovarea standardelor etice în domeniul securității sistemelor informatice;

27.4.3. Asigurarea confidențialității, integrității și disponibilității resurselor informatice ale organizației;

27.4.4. Educarea personalului pentru a face față eficient amenințărilor cibernetice;

27.4.5. Cunoașterea riscurilor și amenințărilor venite din spațiul cibernetic;

27.4. 6. Oferirea soluțiilor pentru a preveni și contracara amenințările cibernetice;

27.5. Instituția noastră va asigura securitatea informației si va aplica următoarele masuri:

27.5.1. Accesul la echipamentele IT ale instituției de către terți se va face sub supraveghere. În contractele cu terții se vor include clauze privind măsurile de protecție a datelor și, în special, a datelor cu caracter personal;

27.5.2. Informațiile vor avea diferite grade de sensibilitate și importanță, informațiile personale (datele cu caracter personal) necesitând un nivel suplimentar de protecție;

27.5.3. Responsabilitatea angajaților privind securitatea va fi implementată încă din etapa recrutării și inclusă în contractele de muncă sau fișă postului și monitorizată permanent;

27.5.4. Parolele utilizate pentru autentificare sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție, conținând majuscule și caractere speciale si sunt formate din cel puțin 8 caractere. Parolele nu sunt afișate pe monitor. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați;

27.5.5. Angajații instituției sau alte terțe părți care au acces la sistemele informatice ale organizației ar trebui să semneze un contract de confidențialitate;

27.5.6. Angajații ar trebui să fie instruiți cu privire la Securitatea Informațiilor;

27.5.7. Toate incidentele de Securitate vor fi raportate conducerii, pentru a decide dacă este cazul ca acestea să fie raportate Autorității de Supraveghere și/sau persoanelor vizate. In

acest sens avem implementat o politică privind managementul adecvat al incidentelor de securitate;
27.5.8. Informațiile critice sau sensibile, precum și datele cu caracter personal trebuie să fie adăpostite în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare și interferențe. Protecția oferită trebuie să fie proporțională cu riscurile identificate;
27.5.9. Sistemele IT vor fi protejate împotriva amenințărilor de Securitate și se vor implementa măsuri de securitate pentru a preveni și detecta accesul neautorizat in sistemele informatice si asupra datelor;
27.5.10 Se vor introduce proceduri pentru efectuarea de back-up strategic, simularea periodică a restaurării de pe copiile realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice;
27.5.11. Utilizarea oricărui sistem IT va fi conformă legislației în vigoare cât și a normelor interne.
27.5.12. Este strict interzisă distribuirea oricăror documente interne sau alte informații către persoane neautorizate;
27.5.13. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;
27.5.14. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice echipament al organizației (PC, server, rețea internă). Nerespectarea acestei reguli aduce după sine posibilitatea desfacerii contractului de muncă sau alte măsuri disciplinare;
27.5.15. Toate sursele externe (CD, atașamente la e-mail, stick-uri, hard-disk etc) vor fi verificate cu un program anti-virus;
27.5.16. Este strict interzisă utilizarea sistemelor IT în alte scopuri decât îndeplinirea atribuțiilor de serviciu;
27.5.17. Infrastructura IT (Servere, Echipamente rețea, website) vor fi scanate de vulnerabilități si raportul de risc va fi distribuit managementului companiei si departamentului IT in vederea remedierii riscurilor in cel mai scurt timp. Scanările vor trebui efectuate periodic cu o recurență cel puțin semestrială;
27.5.18. Este interzisă orice intervenție asupra echipamentelor IT de către personal neautorizat de către instituție în mod scris;
27.5.19. Se interzice folosirea oricărui echipament IT de către orice persoană care nu face parte din personalul instituției fără acordul prealabil și scris al conducerii instituției;
27.5.20. Mijloacele de autentificare în sistem (nume utilizator, parolă etc) sunt proprietatea fiecărui angajat și el este singurul responsabil de a nu divulga aceste informații. De asemenea se recomandă utilizarea de sisteme de autentificare cu dublu factor (SMS, Token, etc.)
27.5.21. Este strict interzisă utilizarea datelor de acces ale altui angajat;
27.5.22. Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere);
27.5.23. Pentru copierea fișierelor electronice, instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus f instituției;
27.5.24. Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil;

27.5.25. Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizare complet;
27.5.26. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicire și, în special, existența unor clauze contractuale exprese privind protecția datelor;
27.5.27. Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă;
27.5..28. Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul, iar după terminarea programului, calculatorul va fi închis;
27.5.29. Este strict interzisă utilizarea „Print screen-ului" (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor;
27.5.30. Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii;
27.5.31. Se va realiza back-up periodic la toate informațiile stocate pe sistemele IT;
27.5.32. Angajații nu vor uita documente pe birou care conțin date cu caracter personal după terminarea programului sau în pauză;
27.5.33. Angajații vor lua din imprimantă documentele proprii imediat după tipărire.
27.5.34. In funcție de modificările aduse de legislație, precum si de îmbunătățirea continua a procedurilor, a masurilor de securitate asupra infrastructurii IT, instituția noastră, va actualiza prezenta politica privind securitatea informației, in situația in care modificările aduse vor fi substanțiale;
27.6. Modificarea politicii noastre privind securitatea informației, va fi publica si comunicata către persoanele direct implicate la solicitare acestora. Fiecare actualizare a politicii noastre privind securitatea informației, va fi indexata prin numerotarea documentului, acest lucru verificând-se simplu in partea inferioara a documentului publicat de noi.
27.7. Beneficiind de o continuitate in utilizarea serviciilor publice oferite de către instituția noastră, după actualizarea politicii noastre, înseamnă acceptarea de către dumneavoastră a politicii noastre privind securitatea informației in forma noua, modificată.
27.8. Nerespectarea prezentei politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse instituției ca urmare a nerespectării prezentei politici.
27.9. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date sau accesarea neautorizata ori compromiterea sistemelor informatice), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

28. Protejarea datelor cu caracter personal prin adoptarea de politici, proceduri și acorduri
28.1 Totodată, instituția noastră a adoptat o serie de politici, proceduri și acorduri specifice menite sa protejeze datele cu caracter personal, precum și drepturile persoanelor vizate, prin securizarea sistemelor informatice, și prin responsabilizare a angajaților și a colaboratorilor ce vor trebui să le respecte cu strictețe și pe care le enumerăm:
28.2. POL01 Politica generala privind protecția datelor cu caracter personal;
28.3. POL02 Politica privind exercitarea drepturilor persoanelor vizate;
28.4. POL03 Politica privind gestionarea datelor cu caracter personal;

28.5. POL04 Politica privind păstrarea datelor cu caracter personal;
28.6. POL05 Politica privind stocarea si protejarea înregistrărilor;
28.7. POL06 Politica privind accesul la date;
28.8. POL07 Politica privind managementul incidentelor de securitate;
28.9. POL08 Politica privind securitatea informației;
28.10. POL10 Politica privind Anti-Spam si comunicările transmise prin sisteme de telecomunicații;
28.11. POL11 Politica privind fluxurile de date, utilizarea internetului si a sistemelor de posta electronica;
28.12. POL12 Politica privind utilizarea dispozitivelor mobile;
28.13. POL13 Politica privind securitatea fizica a instituției;
28.14. POL14 Politica privind supravegherea video prin sistem CCTV
28.15. PR01 Procedura de notificare privind confidențialitatea;
28.16. PR02 Procedura de Notificare a Încălcării Securității Datelor Personale;
28.17. PR03 Proceduri si responsabilități operaționale privind securitatea;
28.18. PR04 Procedura privind cererile persoanelor vizate;
28.19. PR05 Procesul pentru Evaluarea Impactului asupra Datelor Personale;
28.20. PR06 Procedura de evaluare a persoanelor juridice împuternicite;
28.21. AC01 Acord privind confidențialitatea angajaților;
28.22. AC02 Acord privind prelucrarea datelor cu caracter personal, persoane juridice împuternicite;
28.23. AC03 Acord privind prelucrarea datelor cu caracter personal, operatori persoane juridice;
28.24. AC04 Acord privind prelucrarea datelor cu caracter personal, operatori IT cu acces la sisteme informatice;
28.25. AD01 Act adițional la contractul de munca, pentru angajații ce prelucrează date cu caracter personal;
28.26. AD02 Act adițional la contractul de munca, pentru angajații ce nu prelucrează date cu caracter personal;
28.27. AN01 Anexa la Fisa Postului funcționari publici ce prelucrează date cu caracter personal;
28.28. N01 Nota informare angajați, privind prelucrarea datelor cu caracter personal;
28.29. N04 Nota informare parteneri contractuali, privind prelucrarea datelor cu caracter personal;
28.30. N07 Nota informare consilieri locali, privind prelucrarea datelor cu caracter personal;
28.31. N08 Scrisoare de conformitate cu GDPR, către persoanele juridice împuternicite;

29. Măsuri și reguli pentru asigurarea securității cibernetice și protejarea datelor DCP

29.1. Pentru a spori gradul de Securitate cibernetică și în vederea asigurării unui nivel adecvat de protejare a datelor cu caracter personal, se adoptă prin prezentul regulament și următoarele măsuri și reguli:
29.1.1. Responsabilul cu Protecția Datelor, va alinia in mod deplin instituția cu Regulamentul U.E. 679/2016, abreviat G.D.P.R., având si obligația de a de a superviza in mod continuu, respectarea Regulamentului 679/2016, a legislației in materia prelucrării datelor si a legislației privind securitatea cibernetică;
29.1.2. Respectarea prelucrării datelor cu caracter personal, conform legislației in vigoare, are un caracter complex, însă pentru o foarte buna aliniere cu GDPR, se vor înlesni pentru

actualizarea si însușirea de către Responsabilul cu Protecția Datelor cu Caracter Personal a tuturor informațiilor disponibile in portalul A.N.S.P.D.C.P, a bazei legale din Regulamentul UE 679/2016 si Directiva UE 680/2106 si Legea nr. 190/2018, certificarea prin cursuri, instruiri si participări la sesiuni legate de GDPR;

29.1.3. DPO - Responsabilul cu protecția datelor, va superviza prelucrarea datelor cu caracter personal din instituție, va furniza consiliere privind impactul asupra datelor, va gestiona riscurile operațiunilor de prelucrare si va evalua sistemele informatice, monitorizându-le in mod continuu, propunând masuri in vederea conformării cu legislația, atunci când situația o impune si va efectua evaluările de impact, analizele de interes legitim aferente GDPR, pentru garantarea protejării datelor cu caracter personal și a drepturilor persoanelor vizate;

29.1.4. Responsabilul cu protecția datelor, ca ave un rol activ, adaptând și modificând documentația și formularistica specifica protecției datelor în funcție de necesitățile instituției, de schimbarea legislației, a noilor conjuncturi sau schimbări a procedurilor sau regulamentelor instituției, având în vedere, acoperirea tuturor situațiilor ce implică protecția datelor precum: operatori împuterniciți, servicii oferite de firme de IT, cu acces la infrastructura informatizată a instituției;

29.1.5. De asemeni, va gestiona situațiile, evenimentele și a procedurile ce implică: copiile de siguranță ale bazelor de date instalate pe servere, control al accesului în infrastructura informatizată și sistemele informatice ale societăților cu servicii in IT ce oferă mentenanță, înregistrările audio, video și fotografierea, precum și difuzarea acestora în mediul internet.

29.1.6. Un rol important, este asumarea rolului de contact, pentru persoanele vizate, cărora are obligația de a le răspunde in vederea exercitării drepturilor, dar si sa colaboreze cu A.N.S.P.C.P.D. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

29.2. Specialistul IT & C , responsabil al infrastructurii Informatizate a Instituției, va avea un rol deosebit de important în protejarea datelor cu caracter personal, precum și în vederea alinierii depline a instituției cu Regulamentul U..E. 679/2016 și legislația în materia securității cibernetice, dar și in menținerea în cei mai buni parametri de funcționare a sistemelor informatice și a întregii structuri informatizate a instituției;

29.3. Specialistul IT, este persoana cheie, fundamentală din cadrul instituției, care va asigura zilnic, funcționalitatea sistemelor informatice (stații de lucru, servere, imprimante) pentru ca angajații instituției să poată desfășura în condiții optime atribuțiile de serviciu, fără a întâmpina dificultăți în utilizarea acestor sisteme, deservind în final eficient persoanele fizice ce interacționează cu instituția sau colaborările instituției cu autoritățile, instituțiile, operatorii economici, asociații, organizații, etc.;

29.4. Un rol deosebit de important, îl are Specialistul IT, în a fi garantul pentru asigurarea securității cibernetice și protejarea datelor cu caracter personal din instituție. Acesta, prin administrarea eficientă a întregii infrastructuri informatizate, va asigura instituția că sistemele informatice precum și datele conținute sunt în siguranță în orice moment;

29.5. Specialistul IT, va administra și monitoriza întreaga infrastructură informatizată, va colabora direct cu Responsabilul cu protecția datelor și Conducerea instituției, informând periodic sau de câte ori situația o impune, cu privire la starea infrastructurii, vulnerabilități, necesități, modernizare, echipamente depășite, utilizare necorespunzătoare ale sistemelor de către angajați, accesări neautorizate, sau eventuale breșe de securitate, etc.;

29.6. Acesta va face anual o evaluare a întregii infrastructuri informatizate, pe care o va prezenta Conducerii și Responsabilului cu protecția datelor, va propune proceduri specifice

pentru angajați și va gestiona din punct de vedere tehnic, toate colaborările cu operatorii economici, autorități sau instituții, în privința serviciilor sau produselor IT & C;
29.7. Acesta va avea verifica, specificațiile tehnice ce privesc echipamentele sau serviciile și in mod deosebit condițiile și modalitățile de interconectare, instalare sau acces la infrastructura informatizată sau la sistemele informatice, echipamentele instalate de către externi;
29.8. Specialistul IT va avea și sarcina gestionării din punct de vedere tehnic, a relațiilor cu operatorii asociați sau împuterniciți ai instituției, în situațiile ce implică IT&C, sprijinind Responsabilul cu protecția datelor în verificarea situației de conformitatea a capacității tehnice de a asigura protejarea datelor instituției prelucrate de către acești operatori împuterniciți sau asociați;
29.9. De asemeni, Specialistul IT va gestiona, toate situațiile ce implică echipamente tehnice și utilizarea acestora, precum sistemul de supraveghere video CCTV, echipamente și mijloace tehnice ce permit înregistrările audio, video și fotografierea, precum și difuzarea, stocarea sau prelucrările înregistrărilor, fie că acestea sunt realizate de către instituție sau prin operatori împuterniciți;

30. Reguli generale pentru angajații instituției
30.1. Singurele persoane care sunt apte să acceseze datele personale sunt cele cărora le este necesară pentru activitatea pe care o realizează;
30.2. Datele trebuie să nu fie împărtășite către toți angajații. Când este necesar accesul la informații confidențiale, angajații pot solicita direct de la managerii lor;
30.3. Instituția asigura trainingul aferent tuturor angajaților pentru a-i ajuta în procesul înțelegerii responsabilității pe care o au în momentul în care utilizează datele;
30.4. Angajații trebui să asigure securitatea datelor luând precauții și folosind instrucțiunile de mai jos si vor utiliza parole puternice;
30.5. Datele personale nu vor fi dezvăluite către persoane neautorizate, fie din interiorul companiei sau în afară;
30.6. Datele trebui să fie revizuite și actualizate dacă există situația în care datele nu sunt concordante cu realitatea. Dacă nu mai sunt necesare, datele vor fi șterse conform procedurilor interne;
30. Angajații vor cere ajutorul managerului lor sau responsabilului cu protecția datelor dacă nu sunt siguri în legătura cu orice aspect al protecției datelor;

31. Reguli privind stocarea datelor
31.1. Întrebările despre stocarea datelor pot fi redirecționate în siguranță managerului IT sau operatorului de date;
31.2. Când datele sunt stocate pe hârtie, ele trebuie păstrate in arhiva instituitei sau in fișete si birouri închise unde persoanele neautorizate nu pot avea acces;
31.3. Aceste instrucțiuni se aplică, de asemenea, asupra datelor care sunt stocate în mod obișnuit în format electronic, dar au fost printate din anumite considerente:
31.4. Hârtiile sau fișierele trebuie păstrate într-un loc închis sau într-un sertar închis;
31.5. Angajații trebuie să se asigure că hârtia sau cele printate nu sunt lăsate către oameni neautorizați ce ar putea să le vadă, ca de exemplu pe imprimantă;
31.6. Printurile ar trebui distruse când nu mai sunt necesare;
31.7. Când datele sunt stocate în format electronic, trebuie să fie protejate de accesul neautorizat, ștergerilor accidentale sau atacurilor cibernetice;

31.8. Datele trebuie protejate de parole puternice ce sunt schimbate regulat și niciodată împărtășite între angajați;
31.9. Dacă datele sunt stocate pe suporturi amovibile (precum CD, DVD), acestea se păstrează în siguranță atunci când nu sunt folosite;
31.10. Datele trebuie stocate numai în servere sau unități specializate localizate in sediul instituției și in mod excepțional, in urma analizei si aprobării să fie încărcate într-un serviciu de ,,cloud computing'', la un furnizor certificat, in deplina siguranța;
31. 11. Serverele ce conțin informații personale trebuie plasate într-un loc sigur, departe de spațiul general de birouri, intru-un spațiu special amenajat de forma centru de date securizat;
31.12. Datele nu ar trebui salvate direct pe laptopuri sau alte dispozitive mobile precum tablete sau telefoane inteligente;
31.13. Datele trebuie să aibă un sistem de salvare de siguranța (back-up), care sa poata fi testate regulat;
31.14. Toate serverele și calculatoarele ce conțin date trebuie protejate de software de Securitate și firewall.

32. Reguli privind utilizarea datelor
32.1. Instituția va adopta masuri de prevenție in utilizarea datelor cu caracter personal din care enumeram:
32.1.1. Când se lucrează cu date personale, angajații vor asigura ecranele calculatoarelor întotdeauna închise când le lasă nesupravegheate;
32.1.2. Datele personale vor fi transmise prin e-mail, având în vedere că aceasta cale de comunicare nu este sigură;
32.1.3. Datele vor ar trebui criptate înainte de a fi transferate electronic. In situațiile in care nu este implementat încă acest procedeu se vor lua masuri pentru a se implementa cat mai repede astfel de procedee;
32.1.4. Datele personale nu se vor transfera în afara Spațiului Economic European;
32.1.5. Angajații nu vor salva datele personale în dispozitivele lor personale, unități de stocare mobile. Întotdeauna ar trebui să existe acces și actualizare a copiei centrale a tuturor datelor;

33. Reguli privind precizia datelor
33.1. Este responsabilitatea tuturor angajaților care lucrează cu aceste date să urmărească pașii pentru a asigura acuratețea și actualitatea datelor pe cât posibil;
33.2. Datele vor fi păstrate în puține locuri. Personalul nu trebuie să creeze alte locuri adiționale deloc necesare, ca de exemplu copii inutile;
33.3. Personalul ar trebui să se folosească de fiecare oportunitate pentru a asigura actualizarea datelor;

34. Precizări privind furnizare informațiilor
34.1. În acest scop, se va consulta Politica de confidențialitate, stabilind modalitatea de utilizare a datele persoanelor vizate sau a informațiilor furnizate in raport cu Regulamentul U.E. 679/2016 dar si cu legislația in vigoare precum Legea 544/2001, cu supervizarea Responsabilului cu Protecția Datelor cu Caracter Personal, prin consultarea șefilor de departamente, a secretarului sau consilierului juridic, utilizând formularistica adecvata, in funcție de solicitare sau de particularitățile situațiilor care impun furnizarea de informații;

35. Divulgarea datelor din alte motive

35.1 În anumite circumstanțe, legislația permite datelor personale să fie dezvăluite către organele legii fără consimțământul persoanei subiect al datelor;

35.2. În aceste circumstanțe, va dezvălui datele necesare. Operatorul de date va asigura faptul că cererea este legitimă, căutând asistență de la consilierii juridici ai companiei unde este necesar;

36. Cooperarea cu Autoritatea de Supraveghere

36.1. Instituția își va asumarea rolului de punct de contact pentru Autoritatea de Supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;

36.2. Instituția își va asumarea rolului de punct de contact cu persoanele vizate privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul Regulamentului;

36.3. Instituția va oferi sprijin concret în situația unui incident de securitate și oferirea de sprijin cu privire la notificarea Autorității de Supraveghere și a persoanelor vizate;

36.4. Instituția va lua toate măsurile în vederea respectării secretului și a confidențialității în ceea ce privește îndeplinirea sarcinilor sale;

36.5. Instituția va monitorizarea și va oferi sprijin concret în orice alt aspect legat de protecția datelor cu caracter personal, conform dispozițiilor legale în vigoare.

CAP. IX INSTRUIREA ȘI ANGAJAMENTUL DE CONFORMARE A ANGAJAȚILOR

37. Instruirea angajaților cu privire la GDPR

37.1. Se vor întocmi planuri anuale de pregătire continuă, elaborate în condițiile legii, ce trebuie să conțină teme privind cunoașterea legislației naționale și comunitare în materia prelucrării datelor cu caracter personal, precum și teme specifice privind riscurile pe care le comportă prelucrarea datelor și măsurile minime de securitate, în funcție de specificul activității instituției;

37.2. Planurile anuale vor fi elaborate de către DPO Responsabilul cu protecția datelor cu caracter personal și sunt aprobate de către primar;

37.3. Conducătorii structurilor din cadrul instituției vor organiza periodic, cu sprijinul DPO Responsabilul cu protecția datelor, instruiri cu angajații pentru cunoașterea procedurilor specifice de lucru instituite la instituției, cu privire la prezentul Regulament și cu privire la riscurile generate de vulnerabilități și amenințări informatice la adresa datelor cu caracter personal prelucrate;

37.4. În mod obligatoriu la modificarea cadrului legal în materie, se vor efectua instruiri iar prelucrarea incidentelor se va realiza cu întregul personal al instituției implicat în activitatea de prelucrare a datelor cu caracter personal;

37.5. Sesiunile de instruire și pregătire vor putea fi asigurate și de către operatori economici specializați, sau de către DPO Responsabil cu protecția datelor cu caracter personal extern, în virtutea externalizării serviciilor, atunci când legislația sau situația o impune.

38. Angajamentele angajaților cu privire la protejarea datelor cu caracter personal

38.1. În vederea garantării protecției datelor cu caracter personal, la angajare, toți angajații trebuie să semneze documentația de conformare cu GDPR, ca angajament individual de conformare față de legislația GDPR și a prezentului Regulament în funcție de situație după cum urmează:

38.2. AC01 Acord privind confidențialitatea angajaților;

38.3. AD01 Act adițional la contractul de munca, pentru angajații ce prelucrează date cu caracter personal;

38.4. AD02 Act adițional la contractul de munca, pentru angajații ce nu prelucrează date cu caracter personal;

38.5. AN01 Anexa la Fisa Postului funcționari publici ce prelucrează date cu caracter personal;

38.6. N01 Nota informare angajați, privind prelucrarea datelor cu caracter personal;

38.7. N02 Nota informare candidați, privind prelucrarea datelor cu caracter personal;

38.8. Semnarea documentației reprezintă asumarea individuala a angajamentului de respectare a legislației specifice și a Regulamentului instituției privind protecția datelor cu caracter personal, în scopul protejării reputației instituției și aplicării legislației în materia GDPR.

38.9. Semnătura de confirmare a angajamentului individual are următoarea însemnătate:

38.9.1. Angajatul a luat la cunoștință despre prevederile Regulamentului UAT Municipiul Rădăuți, privind protecția datelor cu caracter personal;

38.9.2. Angajatul a participat la programele de pregătire și a fost instruit conform prevederilor Regulamentului instituției adoptat în acest domeniu;

38.9.3. Angajatul înțelege importanța respectării în totalitate a cerințelor cuprinse în legislația specifică și în Regulamentul instituției privind protecția datelor cu caracter personal;

38.9.4. Angajatul își asumă necondiționat responsabilitatea în ceea ce privește conformarea cu cerințele cuprinse în legislația specifică și în Regulamentul instituției, privind protecția DCP;

38.9.5. Angajatul înțelege că, în situația nerespectării principiilor și cerințelor cuprinse în Regulamentul UAT Municipiul Rădăuți, privind protecția datelor cu caracter personal, se face direct răspunzător pentru încălcarea angajamentului individual și pentru consecințele ce decurg din acesta;

38.10. Refuzul de a semna confirmarea angajamentului individual are următoarea însemnătate:

38.10.1. Este necesară identificarea motivelor reale care au condus la refuz;

38.10.2. Este necesară instruirea suplimentară, dacă motivul real este neînțelegerea mesajului sau informațiilor transmise;

38.10.3. Este necesară examinarea atentă a angajatului respectiv, urmat de luarea unor măsuri adecvate, mai ales în situația în care acesta ocupă o funcție care prezintă un risc sensibil la adresa UAT Municipiul Rădăuți, dacă refuzul de a semna confirmarea nu are o motivație reală;

38.11. Angajamentele de Conformare semnate de salariații UAT Municipiul Rădăuți se vor păstra în evidențele serviciului Resurse Umane, iar copii ale documentelor vor fi păstrate de către DPO Responsabilul cu protecția datelor cu caracter personal.

CAP. X ELIMINAREA RISCURILOR ȘI GARANTAREA SECURITĂȚII CIBERNETICE

39. Eliminarea Riscurilor si Garantarea Securității Cibernetice si a Protecției Datelor

39.1. Pentru garantarea securității cibernetice, pentru protejarea datelor cu caracter personal si pentru a exclude si limita la maxim orice breșa informatica, pierderi de date sau de informații, DPO Responsabilul Datelor cu Caracter Personal, împreuna cu factorii de decizie si Conducătorul Unității, vor decide si reglementa, drepturile de acces (local sau de la distanta) si de utilizare pentru fiecare angajat al instituției sau colaboratori (operatorilor economici ce asigura mentenanța la echipamente sau aplicații, instituții, autorități, etc).

39.2. Astfel, se vor autoriza individual, angajații cu drepturile de acces si utilizare prevăzute in fisa postului sau in cadrul unei anexe la contractul de munca, precum si colaboratori (operatorilor economici ce asigura mentenanța la echipamente sau aplicații, instituții, autorități, etc), in baza unor acte adiționale ce vor prevedea modalitatea de acces locala si de la distanta, caracteristici tehnice si condiții de conectare, precum si accesul strict si condiționat doar la serviciile ce fac obiectul contractului sau al colaborării, fără a avea posibilitatea de accesa alte sisteme sau date informatice, garantând instituției posibilitatea de a monitoriza intervențiile, de a putea decide si aproba in prealabil accesul in vederea accesării sistemelor sau aplicațiilor informatice;

39.3. In vederea autorizării se va avea in vedere reglementarea următoarelor situații: utilizarea si accesarea din cadrul instituției sau de la distanta (remote acces) a adreselor de e-mail ale instituției, a aplicațiilor, a programelor de calculator, a camerelor de supraveghere, a dispozitivelor de control, a dispozitivelor de monitorizare, a dispozitivelor ce tin de securitatea infrastructurii informatizate, a echipamentelor IT (servere, routere, switch-uri, puncte de acces, firewall),echipamente Smart sau IOT, a stațiilor de lucru fixe (desktop) sau mobile (laptop), a dispozitivelor mobile (telefoane inteligente si tablete), a camerelor de supraveghere sau a dispozitivelor ce țin de securitatea fizica a instituției, GPS, dispozitive sau echipamente de telecomunicații, etc;

39.4. O importanta majora se va acorda autorizării angajaților, ce vor avea dreptul de a utiliza pe dispozitivele mobile (laptop, tableta, telefon inteligent) proprii sau ale instituției, aplicații ce vor putea accesa serverul de e-mail al instituției, putând vizualiza sau stoca date si informații, precum si accesarea infrastructurii IT a instituției de la distanta (echipamente IT, camere de supraveghere, echipamente de securitate, echipamente Smart sau IOT, dispozitive sau echipamente de telecomunicații, GPS, etc);

39.5. Toate aceste dispozitive, ale angajaților ce au primit autorizare, vor trebui protejate corespunzător, prin limitarea accesului persoanelor neautorizate (colegi neautorizați, familie, prieteni, necunoscuți), accesarea echipamentelor in baza unei parole puternice, criptarea dispozitivelor, activarea GPS si a posibilității de găsire a echipamentelor in caz de pierdere sau furt, activarea posibilității de ștergere si formatare de la distanta a echipamentului in caz de pierdere sau furt, atunci când construcția si posibilitățile tehnice ale echipamentelor o permit.

39.6. In situațiile foarte limitate in care, doar cu titlu de excepție, sunt autorizați, in baza unei necesitați de importanta majora privind operațiunile instituției, unii angajați din conducere sau administratorii sistemelor informatice, au necesitatea de a accesa de la distanta sistemele informatice sau au de a avea instalate aplicații de gestionare a sistemului informatic de posta electronica, ori alte aplicații sau programe informatice (contabilitate, salarizare, situații de urgenta, etc), pe dispozitive informatice fixe (calculator desktop, server) personale aflate in locații personale, se vor evalua riscurile si se vor securiza cibernetic acele dispozitive de către administratorul IT al instituției, asigurându-se ca

dispozitivele accesează doar securizat sau prin VPN sistemele autorizate si au instalate sisteme hardware sau software adecvate pentru o securizare maxima. Aceste operațiuni fiind efectuate cu supervizarea DPO Responsabilului cu Protecția Datelor si aprobarea Conducerii Unității;
39.7. Nu in cele din urma, se vor introduce in regulamentele interne, pe lângă procedurile ce vor garanta securitatea cibernetica si proceduri privind securitatea fizica si instituționala, ce vor trebui sa reducă orice risc privind protejarea datelor cu caracter personal;
39.8. Astfel, se recomanda ca pe lângă sistemele de securitate antiefracție instalate, sa se implementeze in instituție sisteme de monitorizare si control;
39.9. In punctele foarte sensibile precum Centrul de Date unde sunt locate echipamentele esențiale din instituție, precum si in Arhiva instituției unde se afla toate documentele arhivate, precum si in alte puncte sensibile, se vor implementa sisteme de supraveghere video, sisteme antiefracție, sisteme de control al accesului, sisteme anti incendiu, sisteme de monitorizare a temperaturii si sisteme anti inundație, etc.;
39.10. Toate încăperile din instituție, vor fi prevăzute cu sisteme de închidere, control al accesului si sisteme antiefracție (grilaje la parter sau etaje inferioare ori sisteme de alarmare anti efracție);
39.11. Stațiile de lucru fixe si mobile, vor fi securizate prin parola puternica de acces, iar stațiile ce prelucrează date cu caracter personal sau confidențiale in măsura in care posibilitățile tehnice o permit, vor fi securizate prin criptare integrala sau parțiala si nu vor împărtăși in rețeaua locala discuri sau dosare, iar instalarea programelor va fi limitata, putând fi efectuata doar de către administratorul IT;
39.12. Toate stațiile de lucru vor avea instalate doar sisteme de operare si programe de calculator licențiate si vor fi securizate prin instalarea de programe de securitate informatica de tip antivirus si firewall configurate corespunzător, încât sa asigure securitatea stației de lucru, in timpul prelucrării datelor, a accesării internetului precum si a utilizării suporturilor informatice (cd, dvd, memorii externe);
39.13. Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, memorii portabile USB sau HDD etc.) care conțin date cu caracter personal, decât cu aprobarea prealabilă a conducerii;
39.14. În locațiile unde se interacționează cu publicul sau in locațiile unde se procesează multe date cu caracter personal sau confidențial, se recomanda aplicarea unei folii sau sticle de protecție (privacy glass), care sa facă vizibile informațiile doar utilizatorului calculatorului;
39.15. Terminalele de tip, laptop, computer, tableta, smartphone se securizează cu parolă;
39.16. Aplicațiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acționează asupra datelor afișate pe ecran pe o perioadă de timp stabilit, iar terminalele de acces trebuie să aibă setate funcția de închidere automată a ecranului cu solicitarea parolei pentru revenirea la sesiunea de lucru;
39.17. In fiecare departament, vor exista fișete cu sistem de închidere, pentru protejarea documentelor confidențiale si de maxima importanta si se va avea in vedere adoptarea unor proceduri care sa protejeze toate tipurile de documente tipărite prelucrate in cadrul departamentelor, după cum urmează: minimizarea timpurilor de păstrare in departament si arhivarea acestora in Arhiva instituției, depozitarea in fișete încuiate in cadrul departamentului, depozitarea documentelor in lucru in mape si dosare, interzicerea fotocopierii sau a fotografierii neautorizate a documentelor interne, interzicerea sustragerii sau a transportării neautorizate a documentelor înafara sediului instituției, transportarea

documentelor in mape închise intre departamente, elaborarea de proceduri clare si simple privind circuitul documentelor intre departamente in funcție de clasificarea si confidențialitatea acestora, afișarea la avizier, in locuri publice, comunicarea către instituții, autorități, colaboratori sau persoane fizice;
39.18. Toate prelucrările de date cu caracter personal, colectare, introducere, modificare și actualizare a datelor cu caracter personal se realizează numai de către personalul specializat, cu atribuții specific în fișa postului, anume desemnat de către conducătorii unității, conform actelor de reglementare internă;
30.19. Pentru ca transmiterea datelor către contribuabili, instituții, autorități, colaboratori, parteneri comerciali, persoane fizice si terți se face si in mod electronic, se recomanda utilizarea stricta in cadrul instituției a sistemului informatic securizat de posta electronica, având domeniul personalizat de forma numeinstitutie.ro, degaja existent, având instalat certificat de securitate SSL si putând fi accesat prin aplicații sau browser securizate, cu posibilitatea de a cripta datele transmise atunci când se considera necesara transmiterea informațiilor cu un caracter ridicat de securitate;
39.20. Atât portalul de internet cat si adresele de e-mail vor trebuie sa fie securizate prin certificate SSL iar serverul ce gestionează si stochează informațiile, sa se afle localizat într-un centru de date din Romania, sau in spatele unui firewall hardware in incinta instituției;
39.21. Se va avea în vedere, ca în orice situație, să se utilizeze servicii sau sisteme care să întrunească, parametrii si caracteristicile menționate, sau dacă se utilizează serviciile tradiționale de tip SaaS sau Cloud de la furnizori precum Yahoo sau Gmail, ori alți furnizori ce au localizate serverele in afara Comunității Europene, se vor lua masuri imediate privind schimbarea furnizorului de servicii daca nu poate oferi si garanta servicii pe servere localizate in Comunitatea Europeana, sau se va adapta sistemul pentru a corespunde cerințelor Regulamentului U.E. 679/2016;
39.22. In acest sens se recomanda ca toți angajații instituției ce transmit sau primesc informații prin intermediului poștei electronice in numele instituției sa utilizeze strict doar adresele de e-mail securizate ale instituției de forma primariaradauti.ro.
39.23. Se interzice utilizarea serviciului de posta electronică în orice mod ce ar avea drept consecință transmiterea, distribuirea și livrarea de mesaje nesolicitate (Spam) de poșta electronică în volum mare sau de mesaje comerciale nesolicitate și folosirea sau distribuirea de liste de emailuri care aparțin unor persoane care nu și-au exprimat consimțământul anterior;
39.24. Angajații nu vor deschide mesaje de poștă electronică de tip Spam/Malware sau orice alte comunicații electronice care nu au legătură cu activitatea desfășurată în calitate de angajat;
39.25. In toate situațiile in care este necesara publicarea sau transmiterea de informații, ce conțin date cu caracter personal sau informații confidențiale, șefii de departamente sau angajații se vor consulta cu Responsabilul cu Protecția Datelor, pentru a reduce la minim orice risc, pentru a minimiza sau anonimiza datele cu caracter personal ale persoanelor fizice si pentru a îndeplini obligațiile prevăzute de Regulamentul U.E. 679/2016;

40. Supravegherea video, înregistrările audio, video si fotografierea

40.1. Întrucât, dezvoltarea tehnică în domeniul IT&C, telecomunicații și echipamente tehnice, permite acum înregistrare și difuzarea în orice moment, a imaginilor, a vocii, a comportamentului, precum și a alor elemente ce pot duce la identificarea persoanelor, fiind în esență prelucrări de date cu caracter personal, se va avea în vedere gestionarea situațiilor, precum și încadrarea acestor situații în regulamente si proceduri, care să

garanteze respectarea Regulamentului U.E. 679/2016, precum și a drepturilor persoanelor vizate;
40.2. Specialistul IT, precum și Responsabilul cu date cu caracter personal, vor avea un rol cheie în identificarea tuturor situațiilor, ce necesită înregistrări audio, video sau fotografiere, precum: supravegherea video CCTV a instituției, a imobilelor si a spatiilor publice, înregistrări (audio-video-foto) și difuzări ale: ședințelor, investițiilor (construcții noi, modernizări, amenajări), festivităților, evenimentelor culturale sau de orice natura, din primărie, din instituțiile subordonate sau colaboratoare si de pe raza localității, in vederea mediatizării si popularizării localității și/sau a instituției, în mass media, radio, tv, publicații, precum si în mediul internet, cu respectarea Regulamentului U.E. 679/2016 GDPR;
40.3. Indiferent că aceste înregistrări se vor efectua prin sistemul de supraveghere CCTV, sau prin alte echipamente sau mijloace tehnice moderne, se vor lua toate măsurile ca înregistrările și difuzările realizate de către instituție prin personalul responsabil sau de către operatorii împuterniciți, respectă in totalitate drepturile persoanelor vizate precum și Regulamentul U.E. 679/2016;
40.4. Angajații instituției vor fi instruiți în legătură cu aspectele legale privind protecția datelor personale și cu privire la riscurile pe care le comportă prelucrarea datelor personale;
40.5. Se va asigura monitorizarea instituției, a centrului de date și a obiectivelor importante prin sistemul CCTV de supraveghere video;
40.6. Personal specializat va asigura monitorizarea permanentă și intervenția în cazul situațiilor ce țin de securitatea instituționala, a infrastructurii informatizate, echipamentelor IT&C și a datelor;
40.7. Se vor respecta cu strictețe procesele privind circuitul documentelor, începând cu înregistrarea, regulile de păstrare, procesare, multiplicare, transport, distrugere și arhivare conform Nomenclatorului Arhivistic, stabilite și prin Legea Arhivelor Naționale sau legislația internă și internațională privind protecția datelor cu caracter personal, urmându-se și procedurile interne în acest scop;
40.8. Se vor stabil pentru fiecare angajat tipurile de acces la date, încăperi, infrastructură informatizată și operațiunile permise doar pentru îndeplinirea atribuțiilor de serviciu, conform fisei postului;
40.9. Se vor lua măsuri de salvare a bazelor de date ale instituției, prin copii de siguranță la un interval necesar să asigure siguranța acestor baze de date în situații neprevăzute, pentru a se elimina orice risc de pierdere a datelor; În acest sens se va desemna un specialist care să aibă atribuții de serviciu și executarea copiilor de siguranță ale bazelor de date ale sistemelor informatice sau stațiilor de lucru;
40.10. Angajații care prelucrează date cu caracter personal sunt obligați să își închidă sesiunea de lucru sau să blocheze ecranul terminalelor de acces atunci când părăsesc biroul iar la sfârșitul programului de lucru să închidă computerele;
40.11. Imprimarea prin intermediul imprimantelor a datelor cu caracter personal se va realiza numai de angajații autorizați, iar unde tehnologia o permite, imprimantele vor tine evidența imprimărilor sau se vor proteja cu o parole;
40.12. Angajații vor avea dreptul să prelucreze date cu caracter personal doar pe perioada în care ocupă funcția respectivă, cu extinderea sau restrângerea atribuțiilor de prelucrare a datelor cu caracter personal atunci când intervin situații precum modificarea raporturilor de muncă sau a atribuțiilor, prevăzute în fișa postului, cu impact asupra DCP;

40.13. Astfel, se va suspenda dreptul de acces al angajaților la sisteme ce presupun prelucrarea datelor cu caracter personal, pe perioada în care acesta se afla în una dintre următoarele situații:
40.13.1. Concediu pentru incapacitate temporară de muncă sau concediu de maternitate; concediu pentru creșterea sau îngrijirea copilului minor, concediu fără plată, concediu medical, pentru o perioada mai mare de 3 luni;
40.13.2. Urmează un curs sau o specializare, pentru o perioada mai mare de 3 luni, cu scoatere din program;
40.13.3. Dacă este cercetat disciplinar, pe toată perioada cercetării, până la finalizarea cercetărilor;
40.14. În vederea mentenanței, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, se interzice accesul operatorilor economici ce oferă serviciile de întreținere a sistemelor informatice la orice fel de date cu caracter personal existente în sistemele informatice ale instituției. În acest sens se vor urma se vor semna acorduri ce au prevederi foarte stricte și reglementează modalitățile de acces la infrastructura informatizata a instituției precum:
40.14.1. ,,AC03 Acord privind prelucrarea datelor cu caracter personal, operatori persoane juridice";
40.14.2. ,,AC04 Acord privind prelucrarea datelor cu caracter personal, operatori IT cu acces la sisteme informatice";

CAP. XI PERSOANE ÎMPUTERNICITE

41. Operatorul și persoanele împuternicite
41.1. **UAT Municipiului Rădăuți**, va colabora doar cu persoanele împuternicite, care vor oferi garanții în privința prelucrărilor de date cu caracter personal ale Operatorului;
41.2. Aceste garanții constau în demonstrarea de către persoanele juridice împuternicite a faptului că dispun de resursele necesare și au capacitatea de a proteja datele cu caracter personal ale Operatorului, sunt aliniate la Regulamentul U.E. 679/2016 și la legislația privind securitatea cibernetică, dețin certificările necesare și se angajează prin acorduri față de Operator să garanteze confidențialitatea și protejarea datelor cu caracter personal;
41.3. Persoanele împuternicite au rolul de a colabora cu Operatorul, în asigurarea unor servicii menite să asigure funcționalitatea instituției precum: servicii de mentenanță și întreținere a infrastructurii informatizate, a sistemelor informatice, a echipamentelor, intervenții, configurare și adaptare de versiune a pachetelor de programe informatice, aplicații, echipamente sau servere, etc. servicii de fotografiere, filmare a ședințelor, a evenimentelor culturale sau de orice natură, servicii de promovare si mediatizare a instituției, servicii de tipărire de documente, servicii de arhivare clasică a documentelor, servicii de arhivare digitală a documentelor, servicii de stocare, copii de siguranță sau stocare date, etc.
În principiu, toate tipurile de activități, furnizare de servicii sau produse ce implică prelucrarea de date cu caracter personal de către Împuternicit în numele Operatorului.
41.4. Conform Regulamentului U.E. 679/2016, persoanele împuternicite, trebuie să furnizeze serviciile, într-o manieră sigură și să ofere garanții în privința protejării datelor cu caracter personal ale operatorului;

41.5. Prin această procedură instituția se va asigura că persoanele Împuternicite, au capacitatea și dispun de resursele necesare, pentru a proteja datele cu caracter personal, ale Operatorului, sunt aliniate la Regulamentul U.E. 679/2016 și la legislația privind securitatea cibernetică, dețin certificările necesare și se angajează prin acorduri față de Operator să garanteze confidențialitatea și protejarea datelor cu caracter personal, prelucrate în numele Operatorului;
41.6. Pentru a putea evalua persoanele juridice împuternicite, prin această procedura, sunt relevante și necesare următoarele documente conexe:
41.6.1. ,,Procedura de evaluare a persoanelor împuternicite conform GDPR'';
41.6.2. ,,Scrisoarea de conformitate cu GDPR, către persoanele juridice împuternicite'';
41.6.3. ,,Formular de verificare a persoanelor juridice împuternicite'';
41.6.4. ,,Acord privind prelucrarea datelor cu caracter personal, persoane juridice împuternicite''.

42. Condiții minime pentru utilizarea procedurii de evaluare
42.1. Înainte de a începe procedura, trebuie îndeplinite următoarele condiții:
42.1. S-au stabilit cu exactitate cerințele referitoare la produsele sau serviciile ce se doresc a fi achiziționate, sau specificul colaborării ce urmează a fi perfectate;
42.2. Dacă, deja persoana împuternicită prelucrează datele cu caracter personal în numele Operatorului, sau urmează să prelucreze după încheierii contractului cu Operatorul;
42.3. Este indicat, ca această procedură să fie utilizată de fiecare dată când instituția are în vedere, externalizarea sau achiziționarea unor servicii, produse ce implică prelucrări de date cu caracter personal aparținând Operatorului, de către persoane juridice în calitate de Împuterniciți;

43. Procedură de evaluare a persoanelor juridice împuternicite
43.1. Pentru a evalua în mod corect o persoana juridică din punct de vedere GDPR, ce urmează să prelucreze date cu caracter personal ale Operatorului va trebui completat ,,Formularul de verificare a persoanelor juridice Împuternicite'', dovadă a evaluării ce va trebui păstrată.
43.2. Evaluarea GDPR a persoanei împuternicite ar trebui făcută utilizând chestionarul de evaluare și păstrată ca dovadă a evaluării, precum și în baza dovezilor puse la dispoziție de către persoana împuternicită;
43.3. În prima faza a evaluării, va înmâna persoanei juridice ,, Scrisoarea de conformitate cu GDPR, către persoanele juridice împuternicite'' anexând și ,,Formularul de verificare a persoanelor juridice Împuternicite'', aceasta având obligația de al înapoia Operatorului, completat cu acuratețe conform cerințelor din formular;
43.4. În a doua fază, se vor solicita persoanei juridice Împuternicite dovezi că dispun de resursele necesare și are capacitatea de a proteja datele cu caracter personal ale Operatorului, este aliniat[la Regulamentul U.E. 679/2016 și la legislația privind securitatea cibernetică;
43.5. Dovezile pot fi: proceduri, politici, regulamente, analize GAP, analize DPIA, dovezi ale conformării cu GDPR, audituri, certificări ale firmei și ale specialiștilor, ISO 27001, dovezi de conformare cu legislația securității cibernetice, privind infrastructura informatizată, sistemele informatice, metode de prevenție, criptare, copii de protecție și securizare date, precum și echipamentele unde se vor prelucra și stoca datele cu caracter personal în numele Operatorului;

43.6. În a treia fază se vor cerceta în detaliu, ,,Formularul de verificare a persoanelor juridice Împuternicite'', completat de către persoana juridică Împuternicită și se vor verifica informațiile privind persoana juridică Împuternicită;
43.7. Compania care face obiectul evaluării, serviciile sau produsele furnizate, și identificarea datelor cu caracter personal care sunt sau pot fi împărtășite cu Împuternicitul;
43.8. Se vor face cercetări în privința companiei care furnizează serviciile sau produsele, precum data înființării, sediul social, sediile secundare, sediul unde sunt locate sistemele informatice ce vor prelucra datele Operatorului, administratori, numărul de angajați, serviciile sau produsele, portofoliul de clienți, situația juridică, economică, solvabilitatea și rezultatele financiare ale companiei;
43.9. Se vor verifica în detaliu, oferta tehnică și comercială, termenii contractuali, durata, legea aplicabilă, reînnoirea și rezilierea, precum și termenii sau clauzele privind protecția datelor;
43.10. Din dovezile puse la îndemână de către persoana juridică, verificați cu acuratețe, politicile, procedurile, responsabilizarea angajaților, subcontractanții (dacă este cazul cu serviciile subcontractate), auditările, certificările, ISO, privind GDPR, confidențialitatea și securitatea cibernetică;
43.11. Ca urmare a unui contract între părți, definiți ce date cu caracter personal ale Operatorului sunt prelucrate, stocate de către Împuternicit și care este scopul prelucrărilor. Specificați dacă sunt prelucrate și categorii de date speciale și care ar fi volumul total al prelucrărilor;
43.12.Va trebui stabilită cu exactitate, locația fizică a prelucrării datelor cu caracter personal, sediul, punctul de lucru, centrul de date, infrastructura informatizata si sistemele informatice unde se stochează sau se prelucrează datele cu caracter personal ale Operatorului de către Împuternicit;
43.13. Este de preferat ca locația echipamentelor să fie la sediul Împuternicitului, sau în Romania într-un centru de date securizat care să garanteze protecția datelor și să fie conforme cu Regulamentul U.E. 679/2016;
43.14. Din dovezile puse la dispoziție de către Împuternicit, precum și din întrebări sau investigații suplimentare, determinați ce metode de securizare și protecție folosește Împuternicitul pentru a proteja datele cu caracter personal, precum: control al accesului și monitorizarea sistemelor informatice, copii de siguranță a datelor, criptarea datelor și a sistemelor informatice, sisteme de Securitate specializate precum firewall hardware, antivirus de rețea;
43.15. Vor trebui făcute verificări în privința subcontractanților, sau a terților, în situațiile în care Împuternicitul, subcontractează serviciile, sau apelează la serviciile altor terți, în mod special dacă aceștia vor avea acces la datele cu caracter personal ale Operatorului. Dacă există astfel de situații, se vor solicita dovezi de la Împuternicit, precum că a verificat faptul că subcontractorii au implementat GDPR, măsuri de securitate a datelor cu caracter personal, există acorduri de responsabilizare a angajaților, iar Împuternicitul are încheiat un acord de confidențialitate cu subcontractorii și garantează pentru aceștia în fața Operatorului;
43.16. În funcție de informațiile obținute va trebui să evaluați dacă sunt necesare măsuri suplimentare în vederea asigurării protecției datelor cu caracter personal și să va asigurați că sunt puse in aplicare;
43.17. Astfel, asigurându-se pe deplin de faptul că Împuternicitul întrunește toate condițiile reglementate de către Regulamentul U.E. 679/2016 GDPR, instituția în calitate de Operator

va încheia cu împuternicitul, un ,,Acord privind prelucrarea datelor cu caracter personal, persoane juridice împuternicite'';
43.18. Instituția în calitate de Operator, va avea ca sarcină, supravegherea modului în care Împuternicitul, prelucrează sau stochează datele cu caracter personal, în acest sens, periodic sau de câte ori consideră necesar in baza ,,Acordului privind prelucrarea datelor cu caracter personal, persoane juridice împuternicite'', să solicite Împuternicitului, un audit, dovezi privind securitatea și conformitatea prelucrărilor, precum și vizitarea efectivă a sediilor unde se efectuează prelucrările.

CAP. XII DOCUMENTAȚIA PRIVIND IMPLEMENTAREA GDPR

44. Proceduri privind documentația specifică GDPR

44.1 În vederea alinierii instituției la Regulamentul U.E. 679/2016 GDPR, pentru protejarea datelor cu caracter personal, documentația specifică implementării GDPR, documente, formulare, fișe, registre, politici, proceduri, cereri, se aprobă și se introduce în circuitul de documente al UAT Municipiul Rădăuți și a instituțiilor subordonate. Documentația se va adopta în cadrul UAT Municipiul Rădăuți și în fiecare direcție, serviciu, compartiment, birou, precum și în cadrul instituțiilor subordonate;
44.2. Documentația va fi adaptata in funcție de specificul ei, pentru contractele de munca, fisa postului, acorduri de confidențialitate cu angajații, contracte comerciale cu partenerii comerciali, acorduri de confidențialitate cu partenerii comerciali, operatori împuterniciți, operatori persoane juridice IT, etc., conform Regulamentului UE 679/2016, acesta putând suferi modificări sau îmbunătățiri, conforme exigentelor sau necesitaților departamentelor din cadrul instituției;
44.3. In baza documentației, instituția, va trebui sa informeze si sa notifice, cu privire la activitățile sale de prelucrare a datelor cu caracter personal, angajații instituției, persoanele vizate, partenerii comerciali, instituții sau autorități, colaboratori precum profesioniști, asociații sau ONG-uri, vizitatorii ai instituitei cat si vizitatorii portalului de internet;
44.4. In acest sens se vor afișa la sediul instituitei si pe portalul de internet in secțiunea GDPR specifica, in mod vizibil toate documentele ce fac referire la prelucrarea datelor cu caracter personal de către instituție, politici, note de informare, formulare de consimțământ si de exercitare a drepturilor pentru persoanele vizate;
44.5. In vederea obținerii consimțământului persoanelor vizate, prin formularul de consimțământ, instituția va trebui sa informeze persoanele vizate, cărora dorește sa le obțină consimțământul, prin afișarea vizibila la sediul instituitei, a notei de informare privind prelucrarea datelor cu caracter personal. Nota de informare se va înmâna persoanei vizate, explicând in mod logic si simplu conținutul notei de informare cat si ce presupune acordul in vederea obținerii consimțământului de către instituție, dar si care sunt drepturile sale garantate de Regulamentul 679/2016;
44.6. De asemeni, partenerii comerciali si colaboratorii, vor fi informați prin orice mijloc de corespondenta, in privința alinierii de către instituție cu Regulamentul UE 679/2016.
44.7. Se aprobă și se introduce în circuitul documentelor din cadrul UAT Municipiul Rădăuți și a instituțiilor subordonate, documentația specifică implementării GDPR din Anexa 1 ,,Documentație specifică implementării Regulamentului UE 679/2016'', parte integrantă a prezentului Regulament.
44.8. Documentația specifică GDPR din Anexa 1 ,,Documentație specifică implementării Regulamentului UE 679/2016'', se introduce in circuitul documentelor UAT Municipiul

Rădăuți precum și a instituțiilor subordonate, in vederea utilizării, pentru alinierea si conformarea instituției cu Regulamentul UE 679/2016 si a Directivei UE 680/2016 ale Parlamentului European și a Consiliului Europei cu privire la protecția datelor cu caracter personal;

44.9. Elemente ale documentației, în funcție de fiecare situație specifică, se vor pune la dispoziția angajaților, de către șefii de direcții, servicii, compartimente, etc., la indicația si cu supervizarea DPO Responsabilului cu Protecția Datelor, spre informare si consultare, pe suport electronic si tipărit, disponibile in mod permanent in fiecare departament;

44. 10. Toate documentele aprobate, sunt obligatorii in toate elementele sale, pentru întreg personalul din cadrul UAT Municipiul Rădăuți și a instituțiilor subordonate, fiecare document in funcție de specificul sau, va fi asumat si utilizat in direcția, serviciul, compartimentul, biroul, adecvat, sub îndrumarea DPO – Responsabil cu Protecția Datelor;

44.11. Planul de masuri, in vederea alinierii instituției la Regulamentul U.E. 679/2016 GDPR, verificat si aprobat, se adoptă in cadrul **UAT Municipiului Rădăuți**, începând cu implementarea imediata a procedurilor si masurile operaționale si in cel mai scurt timp cu implementarea soluțiilor tehnice de modernizare a infrastructurii informatizate, centru de date modern, securizare cibernetica a fluxurilor de date informatizate, asigurarea unui mediu protejat al datelor cu caracter personal printr-un sistem informatic securizat, care sa garanteze securitatea datelor procesate, cu management al documentelor, arhivare electronica, server de fișiere, sisteme de criptare, copii de siguranța ale datelor, redundant si independent energetic, in vederea alinierii complete la Regulamentul U.E. 679/2016 GDPR;

44.12. Toate documentele enumerate mai sus, sunt anexate la prezentul Regulament și sunt obligatorii in toate elementele sale, pentru întreg personalul din cadrul Aparatului de specialitate al **U.A.T. Municipiul Rădăuți**;

44.13. Politicile și procedurile menționate, asumate de către instituție, reprezintă ansamblul de reguli ce se vor respecta de către toți angajații instituției, ca si regulament intern, fiind dovada către terți a alinierii instituției cu Regulament UE 679/2016;

44.14. DPO Responsabilul cu Protecția Datelor, va transmite prezentul regulament, precum și documentația adecvată, conducătorilor de departamente, servicii și compartimente, care la rândul lor le vor comunica tuturor angajaților instituției, respectiv către terți, la indicațiile DPO si după cum urmează:

44.14.1. Documentele N03, F10 si F11, se vor afișa vizibil in sediul instituției (la avizier, ghișee si birourile ce lucrează cu publicul, in vederea informării si obținerii consimțământului, persoanelor vizate;

44.14.2. Către, toți conducătorii de departamente, servicii, compartimente, Regulamentul GDPR precum și următoarea documentație GDPR: POL01, POL02, POL03, POL04, POL05, POL06, POL07, POL08, POL09, POL10, POL11, POL12, POL13, POL 14, N01, N03, F10, F11, G03 documente ce se vor aduce la cunoștința tuturor angajaților instituției întrucât reprezintă ansamblul de reguli ce se vor respecta de către toți angajații instituției, ca si regulament intern

44.1.4.3. Către, Compartimentul Resurse Umane, documentele: F07, AC01, AD01, AD02, AN01, N01, N02, N03, F10, documente ce se vor aduce la cunoștința, se vor explica si se vor semna cu fiecare angajat sau candidat, în vederea responsabilizării personalului, cu privire la respectarea Regulamentului UE 679/2016 GDPR, a legislației naționale în domeniu, precum și pentru garantarea protejării datelor cu caracter personal ale persoanelor fizice vizate de prelucrările din cadrul instituției;

44.14.4. Către, toţi conducătorii de Departamente, Servicii, sau Compartimente, ce colaborează cu persoanele juridice, operatori economici, ONG, asociaţii, etc documentele: N03, N04, N05, N06, N08, PR06, F10, F11, F12, AC02, AC03, AC04 documente ce vor fi comunicate, afişate si semnate cu terţii in funcţie de specificul fiecărui document, sub îndrumarea DPO;
44.15. DPO – Responsabilul cu protecţia datelor, va face demersurile in vederea informării prin intermediul portalului de internet al instituţiei astfel:
44.15.1. Crearea unei secţiuni distincte denumita GDPR, vizibila si accesibila din prima pagina a portalului;
44.15.2. Secţiunea GDPR va trebui sa conţină in prin plan, vizibil, datele de contact ale DPO – Responsabilului cu protecţia datelor, in vederea exercitării drepturilor de către persoanele vizate si datele de contact ale ANSPDCP Autoritatea Naţionala de Supraveghere a Prelucrării Datelor cu Caracter Personal;
44.16. Tot in aceasta secţiune se vor afişa documentele:
44.16.1. N03 Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal;
44.16.2. POL03 Politica privind confidenţialitatea a portalului de internet;
44.16.3. POL14 Politica privind supravegherea video prin sistem CCTV;
44.17. La prima accesare a portalului, va trebui sa apară o opţiune vizibila in prin plan ce sa conţină următoarele doua elemente principale:
44.17.1. Un link prin accesarea căruia vizitatorii vor avea acces la Politica privind confidenţialitatea a portalului de internet (se va introduce formularul POL03);
44.17.2. Un buton de „Accept" prin care vizitatorii portalului îşi vor da acceptul referitor la aceasta politica;
44.18. In situaţiile ce implica, comunicări, transmitere de informaţii, afişare la avizier, in spaţiul public, sau publicare in portalul de internet ori in mediul online sau răspunsuri la solicitări, ce implica date cu caracter personal si implicit drepturi ale persoanelor vizate, indiferent de forma de comunicare, se va consulta DPO – Responsabilului cu protecţia datelor;
44.19. Toata documentaţia aprobata, va fi gestionata de către DPO – Responsabilului cu protecţia datelor, conform Regulament UE 679/2016 si a Directivei UE 680/2016 ale Parlamentului European si a Consiliului Europei cu privire la protecţia datelor cu caracter personal si potrivit îndrumărilor ANSPDCP Autoritatea Naţionala de Supraveghere a Prelucrării Datelor cu Caracter Personal, in calitate de Autoritate Publica Centrala Autonoma cu competenta generala in domeniul protecţiei datelor personale;
44.20 .În măsura în care legislaţia o impune sau este necesar, DPO Responsabilului cu protecţia datelor, va transmite către şefii de departamente, servicii sau compartimente, documentaţia aferentă, în funcţie de fiecare situaţie în parte.
44.21. Datele de contact ale DPO – Responsabilul cu protecţia datelor din cadrul instituţiei sunt:

UAT MUNICIPIUL RĂDĂUŢI

DPO - Responsabilului cu Protecţia Datelor cu Caracter Personal
Adresa de corespondenta: cu sediul in:
Municipiul Rădăuţi, Strada: Piaţa Unirii nr. 2-4, Judeţul: Suceava;
Adresa de corespondenta electronica:
Telefon: 0230.561.140, Fax: 0230.564.703, E-Mail: dpo@primariaradauti.ro.

CAP. XIII CĂI DE ATAC, RĂSPUNDERI ŞI SANCŢIUNI ÎN MATERIA GDPR

45. Dreptul de a formula o plângere la o autoritate de supraveghere

45.1. Orice persoană vizată, are dreptul de a depune o plângere la o autoritate de supraveghere, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încălcă drepturile prevăzute de Regulamentul UE 679/2016 GDPR;

45.2. Autoritatea de supraveghere la care s-a depus plângerea va informa reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv despre posibilitatea de a se adresa Justiției.

46. Dreptul la o cale de atac judiciar împotriva unei autorități de supraveghere

46.1. Persoanele vizate, au dreptul de a exercita o cale de atac judiciar împotriva deciziilor obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează;

46.2. Totodată, orice persoană vizată are dreptul de a exercit o cale de atac judiciar în cazul în care autoritatea de supraveghere competentă nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse;

46.3. Persoanele vizate vor formula acțiunile împotriva unei autorități de supraveghere doar instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

46.4. Dreptul la o cale de atacă împotriva unui operator sau a unei persoane împuternicite
Persoanele vizate au dreptul de a exercita o cale de atac judiciară în cazul în care consideră că drepturile de care beneficiază în temeiul legii au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prevederile legale specifice;

46.5. Persoanele vizate vor putea formula acțiunile împotriva unui operator sau unei persoane împuternicite de operator, instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu sau instanțelor din statul membru în care persoana vizată își are reședința obișnuită, dacă operatorul sau persoana împuternicită de operator nu este o autoritate publică;

47. Dreptul la despăgubiri și răspunderea operatorului sau a persoanei împuternicite

47.1. Este îndreptățită la despăgubiri orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a legislației de către operator sau de la persoana împuternicită de operator, ce vor avea sarcina despăgubirii;

47.2. Operatorul este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prevederile legislației GDPR. Persoana împuternicită de operator este răspunzătoare numai în cazul în care nu a respectat obligațiile din legislația sau nu s-a conformat acordului cu operatorul.

48. Condiții generale pentru impunerea amenzilor administrative

48.1. Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislației specifice este, în fiecare caz, eficace, proporțional și disuasiv;

48.2. În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate de legislația GDPR.

48.3. Autoritatea poate sa ia următoarele masuri:

48.3.1 Să emită avertizări, să emită mustrări, să dea dispoziții

48.3.2. Să oblige operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor;

48.3.3. Să limiteze sau să interzică prelucrarea;

48.3.4. Să dispună rectificarea sau ștergerea datelor sau restricționarea prelucrării.

48.4. În cazul în care operatorul va fi sancționat administrativ pentru nerespectarea legislației privind protecția datelor cu caracter personal, Responsabilul de protecția datelor va analiza oportunitatea contestării sancțiunii administrative și va formula propuneri în legătură cu promovarea căii de atac, precum și, dacă este cazul, va elabora contestația, urmând să analizeze cel puțin următoarelor aspecte:
48.4.1 Natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;
48.4.2. Dacă încălcarea a fost comisă intenționat sau din neglijență;
48.4.3. Orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
48.4.4. Gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia;
48.4.5. Eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
48.4.6. Gradul de cooperare cu Autoritatea de Supraveghere pentru a remedia încălcarea sau a atenua posibilele efecte negative ale încălcării;
48.4.7. Categoriile de date cu caracter personal afectate de încălcare;
48.4.8. Modul în care încălcarea a fost adusă la cunoștința Autorității de Supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
48.4.9. In cazul în care măsurile menționate de legislația specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauza cu privire la același obiect, obligarea la respectarea respectivelor masuri;
48.4.10 Aderarea la coduri de conduită sau la mecanisme de certificare aprobate;
48.5. Responsabilul de date personale va reprezenta operatorul în cadrul procedurii administrative în fata Autorității cât și în situația în care se va contesta decizia Autorității în fata instanțelor judecătorești;
48.6. In situația neconformării fata de Regulamentul UE 679/2016 GDPR, se poate atrage aplicarea de amenzi administrative cuprinse între 10.000.000 EUR și 20.000.000 EUR sau între 2% si 4% din cifra de afaceri total anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul valoarea cea mai mare.

CAP. XIV RESPONSABILITĂȚI

49. Responsabilități in cadrul UAT Municipiul Rădăuți

49.1. Prezentul Regulament este obligatoriu întregului personal al UAT Municipiul Rădăuți, iar cunoașterea și aplicarea corespunzătoare a prezentului regulament reprezint obligația tuturor angajaților;
49.2. Protejarea datelor cu caracter personal și respectarea drepturilor persoanelor vizate reprezintă responsabilitatea întregului personal al UAT Municipiul Rădăuți.
49.3. Responsabilitatea în ceea ce privește: elaborarea, avizarea, aprobarea, implementarea, supravegherea și evaluarea aplicabilității prezentului Regulament, precum și dispunerea măsurilor care se impun revin UAT Municipiul Rădăuți (cu toate structurile și instituțiile subordonate);

49.4. Toți angajații instituției își vor asuma răspunderea individual, pentru a asigura colectarea, stocarea și utilizate datelor în mod corespunzător, conform legislației GDPR a securității cibernetice și a prezentului Regulament;
49.5. Fiecare șef de serviciu, departament sau compartiment care prelucrează date cu caracter personal se va asigura de faptul că acestea sunt utilizate și prelucrate în concordanță cu politica și principiile generale ale protecției datelor, conform prezentului Regulament și a legislației specifice GDPR si a securității cibernetice;
49.6. Responsabilitățile instituției precum și a tuturor angajaților in mod individual privind protejarea datelor cu caracter personal precum și respectarea drepturilor persoanelor vizate, nu se rezumă la acest capitol, sau la prezentul Regulament, care este obligatoriu în integralitatea sa, ci la întreg ansamblul de norme prevăzute în Regulamentul UE 679/2016 GDPR, precum și la prevederile din legislația naționala și a Comunității Europene, în materia protecției datelor cu caracter personal și a securității cibernetice.

50. Responsabilitățile UAT Municipiul Rădăuți
50.1 UAT Municipiul Rădăuți (cu toate structurile și instituțiile subordonate), în calitate de Operator:
50.2 Este responsabilă cu privire la asigurarea îndeplinirii obligațiilor legale ale instituție conform Regulamentului UE 679/2016, a legislației naționale și a Comunității Europene în materia datelor cu caracter personal precum și a securității cibernetice;
50.3. Asigură implementarea GDPR (legislația UE și națională privind protecția datelor cu caracter personal) la nivelul UAT-ului, prin prezentul regulament sau dispoziții, proceduri, etc.
50.4. Asigură conformarea tuturor activităților de prelucrare cu prevederile GDPR (legislația UE și națională privind protecția datelor cu caracter personal);
50.5. Asigură informarea persoanelor vizate și garantează respectarea drepturilor acestora;
50.6. Ia toate măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;
50.7. In funcție de situație, asigură toate resursele si face toate demersurile in vederea implementării GDPR, a planurilor de masuri aprobate pentru alinierea deplină a instituției cu Regulamentul UE 679/2016, prin angajații proprii sau prin intermediul operatorilor economici specializați si cu experiența in domeniu;
50.8. Totodată daca situația o impune, se vor asigura si resursele necesare pentru achiziția de: cursuri si sesiuni de pregătire a angajaților, evaluări ale sistemelor informatice, consultanta, consultanta, analiza si evaluări GDPR, audituri, certificări sau externalizarea de servicii: IT&C, DPO, precum si achiziția de lucrări si produse, in vederea implementării planurilor de masuri aprobate, etc.
50.9. Supervizează respectarea prezentului regulament privind masurile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal.

51. Responsabilități ale Primarului UAT Municipiul Rădăuți
51.1. Aprobă documentația, regulamente, proceduri operaționale și toate măsurile de implementare GDPR (legislația UE și națională privind protecția datelor cu caracter personal);
51.2. Asigură prin specialiști, evaluarea proceselor aferente prezentului Regulament și aplicarea legislației în domeniul protecției datelor;
51.3. Aprobă modificări ale prezentului Regulament, în situația în care schimbările legislative impun acest lucru în regim de urgentă;

51.4. Aprobă planurile de masuri si alocarea tuturor resurselor necesare in vederea alinierii depline a instituției la Regulamentul UE 679/2016;

52. Responsabilitățile Conducătorilor structurilor organizatorice ale UAT Municipiul Rădăuți

52.1. Conducătorii structurilor organizatorice ale UAT Municipiul Rădăuți sunt responsabili cu protecția datelor cu caracter personal pentru activitățile coordonate și au următoarele responsabilități:

52.2. Stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal în următoarele situații: în vederea desfășurării curente a activități instituției, în vederea îndeplinirii obligațiilor legale, pentru derularea activității comerciale, contractuale, participarea le evenimente, etc.;

52.3. Asigură implementarea GDPR, coordonând și monitorizând activitatea personalului din subordine în vederea respectării Regulamentului;

52.4. Asigură desfășurarea pregătirii de specialitate și instruirea utilizatorilor conform GDPR;

52.5. Dispun măsuri de completare sau, dup caz, de modificare a fișei posturilor angajaților;

52.6. Analizează și dispun suspendarea sau revocarea dreptului de acces al utilizatorilor la sistemele informatice ce conțin date cu caracter personal, la arhiva sau la documentație specific;

52.7. Dispun măsuri organizatorice in vederea exercitării drepturilor de către persoana vizată;

52.8. Coordonează procesul de furnizare a datelor și informațiilor necesare în vederea soluționării cererilor persoanelor vizate;

52.9. Analizează periodic activitatea angajaților în privința GDPR si a securității cibernetice;

52.10. Informează operativ Responsabilul de protecția datelor despre vulnerabilitățile și riscurile semnalate în sistemele informatice sau riscuri de securitate a prelucrărilor DCP și orice încălcare a normelor de protecție a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate și propune măsuri pentru înlăturarea acestora;

53. Responsabilități ale angajaților UAT Municipiul Rădăuți

53.1. Să cunoască și să aplice prevederile Regulamentului precum și a legislației GDPR.

53.2. Să aplice procedurile de informare a persoanelor vizate și să le pună la dispoziție notele de informare și după caz declarațiile de consimțământ, atunci când datele cu caracter personal sunt colectate direct de la aceștia.

53.3. Vor oferi peroanelor vizate informații cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, conidiile în care pot fi exercitate aceste drepturi etc.;

53.4. Să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin șefilor ierarhici, conducerii instituției, pentru realizarea activităților specifice ale acestora;

53.5. Să păstreze confidențialitatea datelor prelucrate, a datelor de acces la sistemele informatice prin care sunt gestionate date cu caracter personal;

53.6. Să respecte masurile de securitate, precum și celelalte reguli stabilite la nivelul instituției

53.7. Să informeze de imediat șeful ierarhic și Responsabilul cu protecția datelor DCP, în situații precum: breșe informatice, atacuri informatice, vulnerabilități, pierderi de date,

defecțiuni tehnice ale sistemelor informatice, accesări neautorizate, pierderi sau diseminări de date DCP, etc.

54. Răspunderi ale structurilor Achiziții Publice, Juridic, Departament IT și DPO

54.1. Au responsabilitatea și obligativitatea încheierii de acorduri sau a adăugarea de clauze contractuale în contractele încheiate și gestionate de către aceștia privind GDPR, la indicația DPO;

54.2. In situațiile în care sunt prelucrate date cu caracter personal în numele UAT Municipiul Rădăuți de către persoane împuternicite vor avea responsabilitate și obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite, acorduri de prelucrare a datelor cu caracter personal;

54.3. Au responsabilitatea și obligativitatea încheierii de acorduri în contractele încheiate și gestionate de către aceștia privind GDPR, cu operatorii IT cu acces la sistemele informatice ale instituției;

54.4. In funcție de situațiile ce se impun, derulează achizițiile de consultanta, servicii, lucrări si produse, de la operatori economici specializați ce au calificările si experiența necesara, in vederea implementării GDPR in cadrul instituției si a planurilor de masuri aprobate pentru alinierea instituției cu Regulamentul UE 679/2016 GDPR, a proiectelor, sau a externalizării serviciilor de DPO, serviciilor IT&C, cursuri si sesiuni de pregătire a angajaților, evaluări ale sistemelor informatice, consultanta, analiza si evaluări GDPR, audituri, certificări, etc.

55. Responsabilități ale DPO Responsabilul cu cu protecția datelor DCP

55.1. DPO este responsabil cu alinierea instituției la Regulamentul UE 679/2016 GDPR si elaborarea Regulamentului, incluzând: monitorizarea și controlul aplicării unitare a Regulamentului, testarea conformității, audituri de specialitate și Informarea conducerii instituției; participă la organizarea și administrarea programelor de pregătire continuă a angajaților în domeniul GDPR;

55.2. Informarea, sfătuirea angajatorului și a celorlalți angajați, emiterea de recomandări către angajator, precum și către ceilalți angajați cu privire la obligațiile care le revin în temeiul Regulamentului (EU) 2016/679 și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

55.3. Promovarea unei culturi a protecției datelor cu caracter personal în cadrul instituitei; Organizarea de training-uri în vederea pregătirii și sensibilizării angajaților cu privire la prelucrarea datelor cu caracter personal;

55.4. Participarea activa la sesiuni de pregătire, training si specializări privind securitatea informației in mediul informatic si legalitatea prelucrării datelor cu caracter personal;

55.5. Participarea în mod regulat la ședințele conducerii, unde se iau hotărâri cu implicații privind prelucrarea datelor și oferirea de opinii concrete și documentate;

55.6. Colectarea informațiilor necesare pentru identificarea activităților de prelucrare;

55.7. Colaborarea cu departamentele instituitei precum HR, Juridic, IT, Securitate pentru a avea informațiile necesare îndeplinirii sarcinilor;

55.8. Recomandări și sprijin concret în privința implementării cerințelor Regulamentului (EU) 2016/679, cum ar fi principiile prelucrării datelor, drepturile persoanei vizate, protecția datelor începând cu momentul conceperii și în mod implicit, păstrarea evidenței activităților de prelucrare, securitatea și managementul adecvat al incidentelor de securitate;

55.9. Monitorizarea respectării Regulamentului, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor;

55.10. Monitorizarea respectării politicilor tehnice și organizaționale ale operatorului;

55.11. Monitorizarea efectuării evaluărilor sau auditurilor necesare, in funcție de situație;
55.12. Alocarea responsabilităților, sensibilizarea și formarea personalului implicat în operațiunile de prelucrare;
55.13. Recomanda, stabilește metodologia si efectuează evaluarea de impact privind protecția datelor cu caracter personal, potrivit art. 35 din Regulamentul UE 679/2016 GDPR;
55.14. Recomanda Conducerii Unității măsurile care trebuie implementate (inclusiv politici tehnice și organizatorice), planuri de masuri, proiecte de securizare a infrastructurii IT, digitalizare, arhivare electronica, cursuri si sesiuni de pregătire a angajaților, evaluări ale sistemelor informatice, consultanta, analiza si evaluări GDPR, audituri, certificări, etc., pentru a elimina orice riscuri la adresa drepturilor persoanelor vizate si protejarea datelor DCP;
55.15. Face demersuri si acționează prin toate mijloacele pentru a implementa planurile de masuri aprobate, a masurilor necesare sau proiectelor si se asigura de implementarea acestora, supervizând toate activitățile ce intra in atribuțiile sale;
55.16. În situația în care instituția nu dispune de resursele necesare pentru implementarea GDPR, a planurilor de masuri aprobate, a implementării proiectelor sau a asigurării serviciilor de DPO, serviciilor IT, cursuri si sesiuni de pregătire a angajaților, evaluări ale sistemelor informatice, consultanta, analiza si evaluări GDPR, audituri, certificări, etc., va recomanda externalizarea proceselor, a serviciilor, a lucrărilor si achiziția produselor și va îndruma organizația în alegerea corectă a operatorilor economici specializați si cu experiența care pot oferi serviciile, produsele si realiza lucrările;
55.17. Este responsabil de tinerea evidenței activităților de prelucrare, potrivit art. 30 din Regulamentul UE 679/2016 GDPR, precum si de toate evidentele necesare si actualizarea acestora, in vederea alinierii depline a instituției cu GDPR.
55.18. Responsabilitățile DPO se regăsesc in prezentul Regulament și sunt specificate în fișa postului sau în contractual de externalizare a serviciilor către un DPO extern, în funcție de caz.

56. Responsabilități ale Serviciului Resurse Umane

56.1. Asigură informarea potențialilor angajați și a angajaților instituției cu privire la prelucrarea datelor cu caracter personal și la drepturile de care beneficiază potrivit legii;
56.2. Participă la organizarea programelor de pregătire continuă a angajaților în GDPR;
Asigură responsabilizarea angajaților cu privire la GDPR, iar la angajarea salariaților în cadrul instituției, pune la dispoziția acestora în documentele în vederea informării și luării la cunoștință cu privire la prevederile prezentului Regulament și a legislației GDPR și se asigură de semnarea de către salariați a acordurilor de confidențialitate.
56.3. Se va avea totodată în vedere pentru fiecare angajat, completarea fisei postului și a contractelor de muncă cu responsabilitățile privind GDPR și a prezentului Regulament. În acest sens se vor semna acte adiționale la contractual de muncă sau anexe la fisa postului, după caz, în funcție de angajat, funcționar public sau contractual.
56.4. Va informa Conducerea Unității si va face toate demersurile necesare pentru a asigura resursele umane necesare asigurării securității cibernetice, precum si a implementării Regulamentului UE 679/2016 GDPR.
56.5. In situația in care resursele umane interne nu sunt disponibile sau se verifica situații de incompatibilități, se vor face demersurile necesare in vederea angajării, transferului intre departamente, a calificării personalului sau se va propune externalizarea serviciilor către operatori economici specializați, cu experiența, care sa întrunească condițiile si sa poată oferi serviciile la standarde cat mai superioare.

57. Responsabilităţi ale Compartimentului IT/Responsabil IT

57.1 Luarea măsurilor tehnice şi organizatorice, specifice zonei IT&C, prevăzute de prezentul Regulament;

57.2. Elaborarea, implementarea şi monitorizarea permanentă a politicilor şi a procedurilor specifice de protecţie şi securitate a datelor cu caracter personal la nivelul instituţiei;

57.3. Instruirea utilizatorilor şi a angajaţilor cu privire la politicile şi procedurilor specifice de protecţie şi securitate a datelor cu caracter personal la nivelul instituţiei;

57.4. Asigurarea tuturor sistemelor, serviciilor şi echipamentului folosit pentru a stoca datele, în condiţiile unor standarde adecvate de securitate, asigurând confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;

57.5. Efectuarea verificărilor şi scanărilor în mod constant pentru a asigura nivelul înalt de securitate al hardware-ului şi software-ului, precum şi funcţionarea decentă a lor;

57.6. Evaluarea fiecărui serviciu al terţilor pe care compania îl consideră că utilizează sau stochează date, precum Cloud sau SaaS;

57.7. Implementează măsuri pentru pseudonimizarea şi criptarea datelor DCP;

57.8. Implementează măsuri pentru digitalizarea documentelor, arhivarea electronica si adoptarea unui circuit electronic al documentelor, pentru o cartografiere optima a datelor cu caracter personal precum si pentru sporirea securităţii datelor cu caracter personal;

57.9. Implementează măsuri pentru a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

57.10. Verifica si supervizează operatorii împuterniciţi care gestionează date DCP ale Operatorului, precum si operatorii economici ce oferă instituţiei servicii, produse IT&C, executa lucrări sau implementează proiecte, in vederea protejării datelor DCP, asigurării securităţii cibernetice, a drepturilor persoanelor vizate, a funcţionalităţii produselor si calităţii lucrărilor sau serviciilor oferite;

57.11 Este garant al infrastructurii informatizate, al sistemelor informatice, precum şi al datelor, informaţiilor şi tuturor prelucrărilor de date cu caracter personal procesate prin intermediul acestor sisteme, având obligaţia de a colabora deplin cu Responsabilul cu protecţia datelor şi Conducerea instituţiei.

58. Responsabilităţi ale Serviciului Contabilitate Buget Finanţe

58.1. Serviciul Contabilitate Buget Finanţa, a asigura toate resursele financiare necesare alinierii pe deplin a instituţiei cu Regulamentul UE 679/2016 GDPR, după cum urmează:

58.1.1. Asigurară in funcţie de situaţie, resurse financiare in vederea realizării activităţilor operaţionale ale instituţiei, privind contractarea consultanta, servicii, lucrări si produse, de la operatori economici specializaţi ce au calificările si experienţa necesara, in vederea implementării GDPR in cadrul instituţiei si a planurilor de masuri aprobate pentru alinierea instituţiei cu Regulamentul UE 679/2016 GDPR, a proiectelor, sau a externalizării serviciilor de DPO, serviciilor IT&C, cursuri si sesiuni de pregătire a angajaţilor, evaluări ale sistemelor informatice, consultanta, analiza si evaluări GDPR, audituri, certificări, etc;

58.1.2. Prevederea in buget si asigurarea resurselor financiare necesare implementării planului de masuri aprobat precum si a investiţiilor necesare alinierii instituţiei la Regulamentul UE 679/2016 GDPR si de realizarea a proiectelor, sau a externalizării serviciilor de DPO, serviciilor IT&C, cursuri si sesiuni de pregătire a angajaţilor, evaluări ale sistemelor informatice, consultanta, analiza si evaluări GDPR, audituri, certificări, etc.

CAP. XV DISPOZIȚII FINALE

59 Dispoziţii finale

59.1. Prezentul Regulament emis de UAT Municipiul Rădăuți, are caracter public și este complementar, documentelor de ordine interioară;

59.2. Prezentul Regulament se aplică și activității Consiliului Local al UAT Municipiul Rădăuți, precum și instituțiilor subordonate;

59.3. Nerespectarea prevederilor regulamentului atrage, în temeiul OUG 57/2019 privind Codul Administrativ și Codul Muncii, după caz, sancțiuni disciplinare și pecuniare (financiare);

59.4. În situațiile de nerespectare a prezentului regulament de către angajații instituției, în mod special dacă se aduc prejudicii instituției, aplicând principiul proporționalității, sancționarea angajatului care a produs prejudiciul poate fi inclusiv desfacerea contractului de muncă;

59.5. Prin Specialist/Departament IT se înțelege dup caz și furnizor extern de servicii IT&C;

59.6. Prin DPO se înțelege dup caz și DPO externalizat conform Regulamentului UE 679/2016.

59.8. Aplicarea sancțiunilor administrative nu înlătură răspunderea penală, civilă, materială sau contravențională, dup caz, a persoanelor vinovate.

59.9. Prezentul Regulament completează: regulamentele, procedurile interne, precum și orice alte acte de ordine interioară

59.10. În situația apariției unor prevederi legale ce modifică, completează sau abrogă dispozițiile prezentului regulament, născute, ulterior datei intrării în vigoare a prezentei reglementări, se vor aplica prevederile legale în vigoare.

59.11. In situația existentei elementelor de drept intelectual si de proprietate intelectuala, in cadrul documentației anexate la prezentul Regulament, acestea nu vor avea caracter Public, se vor utiliza doar ca documente interne, fără a se publica sau a se transfera către terți;

59.12. Prezentul Regulament intră în vigoare de la data de 2020.

Se aprobă,

UAT MUNICIPIUL RĂDĂUȚI
Primar
TATAR NISTOR

CUPRINS

REGULAMENT GDPR UAT MUNICIPIUL RĂDĂUȚI
CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL

ANEXA 1

DOCUMENTAȚIE SPECIFICĂ IMPLEMENTĂRII REGULAMENTULUI UE 679/2016 GDPR

A01 Analiza GAP inițiala, cu anexele specifice: Rezultat Procentual Analiza Inițiala si Diagrama conformitate;
A02 Analiza GAP Finala – Instrument Evaluare GDPR;
AC01 Acord privind confidențialitatea angajaților;
AC02 Acord privind prelucrarea datelor cu caracter personal, persoane juridice împuternicite;
AC03 Acord privind prelucrarea datelor cu caracter personal, operatori persoane juridice;
AC04 Acord privind prelucrarea datelor cu caracter personal, operatori IT cu acces la sisteme informatice;
AD01 Act adițional la contractul de munca, pentru angajații ce prelucrează date cu caracter personal;
AD02 Act adițional la contractul de munca, pentru angajații ce nu prelucrează date cu caracter personal;
AN01 Anexa la Fisa Postului funcționari publici ce prelucrează date cu caracter personal;
C01 Cerere pentru exercitarea dreptului la acces;
C02 Cerere pentru exercitarea dreptului pentru rectificarea datelor cu caracter personal;
C03 Cerere pentru exercitarea dreptului de ștergere a datelor cu caracter personal;
C04 Cerere pentru exercitarea dreptului restricționarea prelucrării datelor cu caracter personal;
C05 Cerere pentru exercitarea dreptului de portabilitate a datelor cu caracter personal;
C06 Cerere pentru exercitarea dreptului la opoziția a prelucrării datelor cu caracter personal;
C07 Cerere pentru exercitarea dreptului la retragerea consimțământului;
C08 Cerere pentru exercitarea dreptului la opoziție privind prelucrarea automata a datelor cu caracter personal;
DISP01 Dispoziție numire DPO Responsabil cu Protecția Datelor;
F01 Fisa individuala IT&C inventariere si evaluare sistem informatic;
F02 Fisa Departament IT&C Inventariere si Evaluare Sisteme Informatice;
F03 Formular individual cartografiere date cu caracter personal;
F04 Formular cu privire la stabilirea temeiurilor legale;
F05 Formular pentru analiza si stabilirea interesului legitim;
F06 Formular inițial de verificare conformitate GDPR;
F07 Fișa Postului DPO;
F08 Formular pentru captarea datelor personale;
F09 Formular final de verificare conformitate GDPR;
F10 Formular pentru obținerea consimțământului;
F11 Formular pentru obținerea consimțământului părintelui;
F12 Formular pentru planificarea notificării - Persoana Vizata;
F13 Formular pentru planificarea notificării - Alte Surse;
F14 Formular DPIA privind Analiza Impactului asupra Protecției Datelor;
F15 Formular de verificare a persoanelor juridice împuternicite;
Formular declarare DPO Responsabil cu Protecția datelor la ANSPDCP;
Formular Notificare Breșa ANSPDCP;
G01 Ghid de completare fisa individuala IT&C sistem informatic;
G02 Ghid notificare incidente de securitate;

G03 Ghid privind informarea persoanei vizate;
N01 Nota informare angajați, privind prelucrarea datelor cu caracter personal;
N02 Nota informare candidați, privind prelucrarea datelor cu caracter personal;
N03 Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal;
N04 Nota informare parteneri contractuali, privind prelucrarea datelor cu caracter personal;
N05 Scrisoare de informare din partea instituției;
N06 Scrisoare conformitate cu GDPR;
N07 Nota informare consilieri locali, privind prelucrarea datelor cu caracter personal;
N08 Scrisoare de conformitate cu GDPR, către persoanele juridice împuternicite;
P01 Procedura de cartografiere a datelor cu caracter personal;
P02 Procedura de evaluare a interesului legitim;
P03 Plan Inițial Conformitate GDPR;
P04 Plan Inițial de pregătire pentru conformitate;
P05 GDPR - dovezile conformării inițiale;
P06 Stadiul final de conformitate cu GDPR;
P07 Dovezile conformării finale cu GDPR;
PLAN01 Plan de masuri in vederea alinierii instituției la Regulamentul U.E. 679/2016;
POL01 Politica privind stocarea si protejarea înregistrărilor;
POL02 Politica generala privind protecția datelor cu caracter personal;
POL03 Politica privind confidențialitatea a portalului de internet;
POL04 Politica privind Anti-Spam si comunicările transmise prin sisteme de telecomunicații;
POL05 Politica privind accesul la date;
POL06 Politica privind exercitarea drepturilor persoanelor vizate;
POL07 Politica privind gestionarea datelor cu caracter personal;
POL08 Politica privind managementul incidentelor de securitate;
POL09 Politica privind păstrarea datelor cu caracter personal;
POL10 Politica privind securitatea informației;
POL11 Politica privind fluxurile de date, utilizarea internetului si a sistemelor de posta electronica;
POL12 Politica privind utilizarea dispozitivelor mobile;
POL13 Politica privind securitatea fizica a instituției;
POL14 Politica privind supravegherea video prin sistem CCTV;
PR01 Procedura de notificare privind confidențialitatea;
PR02 Procedura de Notificare a Încălcării Securității Datelor Personale;
PR03 Proceduri si responsabilități operaționale privind securitatea;
PR04 Procedura privind cererile persoanelor vizate;
PR05 Procesul pentru Evaluarea Impactului asupra Datelor Personale;
PR06 Procedura de evaluare a persoanelor juridice împuternicite;
R01 Registrul prelucrărilor datelor cu caracter personal – operator;
R02 Registru intrări ieșiri date personale;
R03 Registrul datelor cu caracter personal la nivel de organizație;
R04 Registrul incidentelor de securitate;
R05 Registrul cererilor Persoanelor Vizate.
RA01 Raportul DPIA privind Analiza Impactului asupra Datelor Personale;
Regulament 01 Regulament GDPR

ROMÂNIA
JUDEŢUL SUCEAVA
MUNICIPIULRĂDĂUŢI
CONSILIUL LOCAL

ROMÂNIA
JUDEŢUL SUCEAVA
MUNICIPIUL RĂDĂUŢI
PRIMAR

REFERAT DE APROBARE

la proiectul de hotărâre pentru aprobarea Regulamentului privind protecţia datelor cu caracter personal în cadrul UAT Rădăuţi

Stimaţi consilieri,

In vederea alinierii depline a UAT Municipiul Rădăuţi, la legislaţia in materia protejării datelor cu caracter personal precum si la prevederile legislaţiei privind securitatea cibernetica este necesar şi se impune, adoptarea si implementarea unui regulament intern GDPR.

Termenul de „GDPR" este abrevierea a „General Data Protection Regulation" sau în limba română, "RGPD - Regulamentul General privind Protecţia Datelor", ambele abrevierii făcând referire la Regulamentului UE 679/2016, iar scopul acestei dispoziţii legale este de a proteja datele cu caracter personal şi a delimita clar modul în care acestea pot fi prelucrate;

Scopul acestui regulament va fi de a garanta şi proteja drepturile şi libertăţile fundamentale ale persoanelor fizice, în special a drepturilor, cu privire la prelucrarea datelor cu caracter personal, în conformitate cu prevederile Regulamentului U.E. 679/2016 GDPR;

Prin acest regulament, se va asigura conformitatea cu legislaţia si bunele practici privind protecţia datelor cu caracter personal, informarea si respectarea drepturilor persoanelor fizice vizate de prelucrările de date, precum si transparenţa faţa de modul de securizare si protejare a datelor stocate si prelucrate;

Adoptând un regulament GDPR, se va asigura protejarea instituţiei fata de posibilele riscuri referitoare la încălcarea securităţii datelor;

Regulamentul va stabili normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestora;

De asemeni, regulamentul va stabili măsurile tehnice şi organizatorice pentru îndeplinirea obligaţiilor referitoare la securitatea şi controlul sistemelor informatice, în vederea asigurării confidenţialităţii datelor şi informaţiilor precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente executate de angajaţii UAT Rădăuţi;

Prin Regulamentul GDPR, în vederea alinierii instituţiei la Regulamentul U.E. 679/2016 GDPR, pentru protejarea datelor cu caracter personal, se va aproba şi se vor introduce în circuitul de documente al UAT Municipiul Rădăuţi şi a instituţiilor subordonate, documentaţia specifică implementării GDPR, documente, formulare, fişe, registre, politici, proceduri, cereri. Documentaţia se va adopta în cadrul UAT Municipiul Rădăuţi şi în fiecare direcţie, serviciu, compartiment, birou, precum şi în cadrul instituţiilor subordonate.

Regulamentul va fi obligatoriu întregului personal al UAT Municipiul Rădăuţi, iar cunoaşterea şi aplicarea corespunzătoare a regulamentului va reprezintă obligaţia tuturor angajaţilor.

Având în vedere cele expuse, în temeiul art. 136 alin.1) şi 2) din OUG 57/2019 privind Codul Administrativ, propun Consiliului Local aprobarea proiectului de hotărâre în forma prezentată.

INITIATOR
PRIMAR
NISTOR TATAR