ROMÂNIA
JUDEŢUL NEAMT
COMUNA GIROV

HOTĂRÂREA
NR. 37 /31.05.2022
pentru aprobarea Regulamentului privind protecţia datelor cu caracter personal în cadrul UAT Comuna Girov

Consiliul local al Comunei Girov

Având în vedere:

Referatul de aprobare al domnului primar al Comunei Girov, înregistrat cu nr.8599 din 12.05.2022;

Raportul compartimentuluide resort – DPO-din cadrul aparatului de specilaitate al primarului, înregistrat sub nr. 8591/12.05.2022

Regulamentul (UE) 679/2016 GDPR privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal si privind libera circulaţie a acestor date.

Legea 190/2018 privind masuri de punere în aplicare a Regulamentului (UE) 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal si privind libera circulaţie a acestor date.

în temeiul dispoziţiilor 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 Ş T E :

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

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

Art 3. Secretarul general al comunei va comunica prezenta , institutiilor si persoanelor interesate.

Presedinte de sedinta
Avasiloaiei Gabriela
[redacted]

ROMÂNIA JUDEŢUL NEAMŢ-COMUNA GIROV CONSILIUL LOCAL

Contrasemneaza pentru legalitate,
Secretar general al Comunei
Dascalu Elena Luminita
[redacted]

Nr.cons.in functie-15
Nr.cons.prezenti -13

Voturi pentru -13
Voturi impotriva-0

REGULAMENT GDPR
CU PRIVIRE LA PROTECŢIA DATELOR CU CARACTER PERSONAL
UAT COMUNA GIROV

CAP. I DISPOZIŢII GENERALE

1. Despre instituţia noastră

Suntem U.A.T Comuna Girov, administraţie publica locala, operator de date cu caracter personal, ce se angajează sa protejeze datele cu caracter personal ale persoanelor fizice, prelucrate de instituţie, respectând legislaţia europeana si naţionala in materie (Regulamentul UE 679/2016 GDPR si Directiva UE 680/2016, Legea 190/2018 etc.), conform îndrumărilor Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Datele de contact ale instituţiei noastre sunt: **U.A.T Comuna Girov**
Adresa de corespondenta: Comuna Girov, Strada: Calea Romanului, nr. 337, Judeţul: Neamt;
Adresa de corespondenta electronica: Telefon: 0233 291000, Fax: 0233.291000.
E-Mail:girov@nt.e-adm.ro
Portal: www.girov.ro.

Instituţia noastră prelucrează date cu caracter personal referitoare la persoane fizice. Acestea pot reprezenta date în legătură cu contribuabilii, rezidenţii, non rezidenţii, ale partenerilor comerciali, vizitatorii instituţiei sau ai localităţii, angajaţii, candidaţii, voluntarii, colaboratorii, persoane ce accesează portalul de internet al instituţiei sau comunica cu noi prin orice mijloc de comunicare, etc;

Instituţia 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 soluţii tehnice în vederea asigurării securităţii cibernetice a fluxurilor informatizate precum şi infrastructurii şi echipamentelor IT &C;

In acest sens ,prin politici, proceduri, regulamente, instruiri de personal şi prin desemnarea unui DPO- Responsabil cu protecţia datelor cu caracter personal, instituţia noastră s-a aliniat la Regulamentul UE 679/2016 şi va face eforturi constante şi considerabile în vederea menţinerii şi adoptării unor standarde cât mai înalte pentru protejarea datelor cu caracter personal ale persoanelor fizice vizate de prelucrările instituţiei noastre;

Datele de contact ale DPO Responsabilul cu protecţia datelor cu caracter personal sunt: **U.A.T Comuna Girov**-Responsabilului cu Protecţia Datelor cu Caracter Personal
Adresa de corespondenta:
U.A.T Comuna Girov, Strada: Calea Romanului, nr. 337, Judeţul: Neamt;
Adresa de corespondenta electronica:gdpr.comunagirov@gmail.com
Telefon/ Fax: 0233291000

2. Scopul şi Obiectivele Regulamentului

1. Scopul acestui regulament este de a garanta şi proteja
   a. 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;
   b. Conformitatea cu legislaţia si bunele practici privind protecţia datelor cu caracter personal;
   c. Transparenţa faţa de modul de securizare si protejare a datelor stocate si prelucrate;

privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul general privind protecţia datelor);

9. Legea nr. 362/2018, din 28 decembrie 2018, privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;

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;

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;

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);

13. Decizia ANSPDCP nr. 133, din 3 iulie 2018 privind aprobarea Procedurii de primire şi soluţionare a plângerilor;

14. Decizia ANSPDCP nr. 161, din 9 octombrie 2018, privind aprobare a Procedurii de efectuare a investigaţiilor;

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;

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;

17. Procedura ANSPDCP, din 9 octombrie 2018, de efectuare a investigaţiilor;

18. Informare ANSPDCP privind drepturile persoanelor vizate, extras din Reg. 679/2016;

19. Ghid orientativ ANSPDCP, de aplicare a Regulamentului GDPR;

20. Ghid ANSPDCP, privind Responsabilul cu protecţia datelor DPO;

21. Ghid ANSPDCP, cu întrebări si răspunsuri cu privire la aplicarea Reg. 679/2016 GDPR;

22. Broşura ANSPDCP, Noul Regulament General privind Protecţia Datelor;

5. Definiţii si limbaj specific al legislaţiei privind prelucrarea datelor cu caracter personal

5.1. Termenii şi definiţiile cele mai importante cu privire la această politică sunt următoarele:

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;

DPO - termenul de „DPO" este abrevierea a „Data Protection Officer", Ofiţer Responsabil cu protecţia datelor cu caracter personal, desemnat în cadrul instituţiei cu atribuţii privind protejarea datelor cu caracter personal, aşa cum este definit în Regulamentului UE 679/2016;

DCP - Date cu caracter personal - orice informaţii 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 specia! 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

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

Transformarea - operaţiunea efectuat asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

Distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitiv şi irecuperabil, prin mijloace mecanice sau termice, a suportului fizică pe care au fost prelucrate date cu caracter personal;

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 performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se afla persoana fizică respectiv deplasările acesteia;

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 informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri tehnice şi organizatorice care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

Sistem de evidenţă a datelor - înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

Destinatar - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respect normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

Utilizator - înseamnă orice persoană care acţionează 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 atribuţii de serviciu presupun operaţiuni de prelucrare a datelor cu caracter personal.

Parte terţă - înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoană împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

Consimţimânt - al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o Declaraţie - sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

încălcarea securităţii datelor cu caracter personal - înseamnă o încălcare a securităţii 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;

Date genetice - înseamnă datele **cu** caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezulta în special în urma unei analize a unei mostre de material biologică recoltate de la persoană în cauză;

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;

Date privind sănătatea - înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

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 şi de identificare în anumite sisteme informatice de către persoanele autorizate;

7. Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinită în mod rezonabil prin alte mijloace;

8. Operatorul trebuie să stabilească termene pentru ştergere sau revizuirea periodică.

9. Operatorul trebuie să ia toate masurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau şterse;

10. Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea şi confidenţialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizat a datelor cu caracter personal şi 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

1. Regulamentul UE 679/2016, specifica şase temeiuri în baza cărora se pot procesa datele cu caracter personal:

2. **„Obligaţia legală"** -în cazul instituitei noastre fiind o administraţie publica locala în care datele cu caracter personal trebuie să fie colectate şi prelucrate pentru a ne conforma legii, nu este necesar consimţământul explicit;

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 obligaţii oficiale, situaţii când nu va fi solicitat consimţământul persoanei vizate;

4. **„încheierea sau executarea unui contract"** - întrucât instituţia noastră încheie contracte cu alte instituţii, autorităţi publice sau colaboratori persoane juridice sau fizice, cazuri în care datele cu caracter personal colectate şi prelucrate sunt necesare pentru a încheia sau executa un contract cu persoana vizată, nu este necesar consimţământul explicit.,, **Interesul legitim"** - Sunt situaţii speciale in cadrul cărora este necesara prelucrarea datelor cu caracter personal în interesul legitim al instituitei noastre şi prin analize specifice se considera că aceste prelucrări nu afectează în mod semnificativ drepturile şi libertăţile persoanei vizate, atunci aceasta poate fi definită ca fiind motivul legal al prelucrării.

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

6. ale persoanelor vizate. In acest sens instituţia va păstra in evidentele sale dovezile prelucrării din aceste situaţii.

7. . **„Consimţământul"** - în afara situaţiilor prezentate mai sus, instituţia noastră acorda o maxima importanta obţinerii acordului explicit din partea unei persoane vizate pentru colectarea şi prelucrarea datelor. în situaţiile speciale, dar si in cazul copiilor sub vârsta de 16 ani va fi obţinut consimţământul reprezentanţilor legali.

8. La momentul obţinerii consimţământului pentru prelucrarea datelor cu caracter personal, persoanele vizate vor fi informate despre utilizarea datelor cu caracter personal prelucrate de instituţia noastră si li se vor explica drepturile acestora cu privire la datele lor, cum ar fi dreptul de retragere a consimţământului. Toate informaţiile vor fi furnizate într-o formă accesibilă, scrise în limbaj clar şi 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

1. Persoanele vizate au dreptul să fie informate despre felul în care instituţia le prelucrează datele;
2. Informarea trebuie realizată, dacă datele provin de la subiect, la momentul colectării datelor;
3. Datele provin din alte surse, informarea se va realiza în mult o lună de la momentul obţinerii datelor;

20. DPO - Responsabilul cu protecţia datelor, va face demersurile in vederea informării prin intermediul portalului de internet al instituţiei astfel:

21. Crearea unei secţiuni distincte denumita GDPR sau Protecţia Datelor, vizibila si accesibila din prima pagina a portalului,

22. Tot in aceasta secţiune se vor afişa documentele:

23. Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal"; Politica privind confidenţialitatea a portalului de internet"; Politica generala privind protecţia datelor cu caracter personal"; Politica privind supravegherea video prin sistem CCTV"

CAP. V CONSIMŢĂMÂNTUL PERSOANLOR FIZICE VIZATE DE PRELUCRĂRI

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

1. Inainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru, prin înmânarea şi explicarea notei de informare cu privire la datele cu caracter personal;
2. în funcţie de situaţie notele de informare sunt disponibile pentru angajaţii instituţiei, pentru viitorii candidaţi şi în mod special pentru persoanele fizice sau reprezentanţii legali ai minorilor, vizaţi de prelucrările de date cu caracter personal ce necesită consimţământul;
3. Pentru situaţiile în care prelucrarea se bazează pe consimţământ, instituţia trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul expres, neechivoc, liber şi informat pentru prelucrarea datelor sale cu caracter personal;
4. Persoana fizică vizată de prelucrarea datelor cu caracter personal, are dreptul să îşi retragă în orice moment consimţământul, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
5. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.
6. UAT Comuna Girov, va solicita consimţământul în toate situaţiile în care prelucrarea de date nu este o obligaţie legală, în situaţiile în care se solicită copii ale documentelor necesare pentru documentarea sau procesarea solicitărilor însă legislaţia nu o prevede în mod expres în acele situaţii, sau în următoarele situaţii:
   a. în vederea realizării procesului de recrutare sau selecţie de personal, de la candidaţi;
   b. în situaţiile în care prelucrarea vizează copii minori sub **16** ani, se va solicita consimţământul tutorelui sau reprezentanţilor legali;
   c. în vederea desfăşurării unor anchete sociale sau a unor acţiuni ce implică colectarea si prelucrarea de date cu caracter personal (organizarea de evenimente, concursuri, premieri, burse, tombole, etc);
   d. în vederea solicitării datelor de contact (telefon, email, adresă de corespondenţă) pentru furnizarea de informaţii, ce ţin de servicii, evenimente, manifestări, comunicări, etc;
7. Pentru portalul de internet, in situaţia creării de conturi de utilizator sau pentru abonarea la e-mail în scopuri informative, privind activitatea instituţiei, servicii, evenimente;
8. In vederea obţinerii consimţământului, după informarea prealabila prin intermediul notelor de informare, în funcţie de situaţie se vor utiliza următoarele documente specifice:
   a. Formular pentru obţinerea consimţământului";
   b. Formular pentru obţinerea consimţământului părintelui";
9. Responsabilul cu protecţia datelor cu caracter personal, va informa toţi angajaţii cu privire obligativitatea de informare a persoanelor vizate prin notele de informare, precum şi de situaţiile privind solicitarea consimţământului, în funcţie de caz, fără a se limita la situaţiile expuse în prezentul Regulament;
10. Notele de informare precum şi formularele pentru obţinerea consimţământului se vor distribui de către Responsabilul cu protecţia datelor cu caracter personal, către toate compartimentele sau direcţiile ce desfăşoară activităţi cu publicul sau interacţionează cu persoanele fizice sau juridice, conducătorii de compartimente şi direcţii având obligaţia de a le distribui angajaţilor în vederea obţinerii consimţământului de la persoanele fizice în toate situaţiile in care se impune;

k. Prelucrarea poate fi efectuată în scopuri în scopuri de cercetare ştiinţifică sau istorică, de arhivare în interes public ori în scopuri statistice;

l. Prelucrarea poate fi efectuata de către un ONG, asociaţie , fundaţie fără scop lucrativ **în** cadrul activităţilor lor legitime şi **cu** garanţii adecvate care să aibă **un** specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să fie pe seama membrilor sau la foştii membri ai entităţii sau prelucrări ce au la bază persoane ce au legătură cu scopurile sale sub condiţia ca datele **cu** caracter personal sa fie comunicate terţilor doar **cu** consimţământul persoanelor vizate;

4. Aceste prelucrări se vor efectua în temeiul dreptului Uniunii sau al dreptului intern, ori al normelor stabilite de organisme naţionale competente sau în temeiul temeiul unor contracte încheiat cu un cadru care prevăd măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, cu respectarea secretului profesional, a obligaţiilor de confidenţialitate, etc.

11. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video

1. Prin intermediul sistemului de supraveghere video CCTV, instituţia noastră, prelucrează date aparţinând angajaţilor, vizitatorilor (rezidenţi sau non rezidenţii), contribuabili, petenţi, colaboratori, parteneri comerciali, voluntari şi a oricăror altor persoane (cetăţeni), care intră în sediul Primăriei Comunei Girov din str. Calea Romanului, nr.337.

2. Instituţia utilizează sistemul video , pentru supravegherea instituţiei, si a spatiilor din parcare si curtea institutiei publice, în scopul asigurării securităţii persoanelor şi bunurilor, paza şi protecţia bunurilor, imobilelor, a valorilor, control al accesului, , etc.

3. Se supraveghează prin mijloace video: sediul instituţiei cu zonele de acces, spaţiile destinate vizitatorilor, zonele cu acces restricţionat precum casieria unităţii,zona taxe şi impozite, împrejurimile clădirilor pentru a proteja spaţiile exterioare, zonele publice menţionate mai sus;

4. Scopul urmărit este acela de a supraveghea în timp real zonele de interes prin intermediul monitoerului amplasat în spatial separat, precum şi înregistrarea şi stocarea imaginilor preluate din aceste zone.

5. Perioada minima si maxima de stocare este 30 de zile;

6. Camerele de supraveghere video au fost amplasate cu atenţie pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit;

7. Nu sunt monitorizate zonele în care există un nivel ridicat al aşteptărilor privind viaţa privată, precum birourile, toaletele şi alte locaţii similare;

8. In mod special , o atenţie deosebită se va acorda informării persoanelor fizice, privind prelucrările de date cu caracter personal, în situaţia înregistrărilor audio, video sau fotografiere, supravegherea video CCTV a instituţiei, a imobilelor si a spatiilor publice, înregistrări (audio-video-foto) şi difuzări ale: şedinţelor, investiţiilor (construcţii noi, modernizări, amenajări), festivităţilor, evenimentelor culturale sau de orice natura, din primărie, in vederea mediatizării si popularizării localităţii şi a instituţiei, în mass media, radio, tv, publicaţii, precum si în mediul internet;

9. Astfel, în funcţie de fiecare situaţie, la toate obiectivele unde sunt instalate camerele video ce captează imagini, ale sistemului de supraveghere, sau prin alte mijloace tehnice se înregistrează imagini video, persoanele fizice vor fi avertizate de existenţa camerelor de supraveghere, sau a acestor mijloace tehnice, prin semne adecvate si note de informare, afişate vizibil, în mod permanent în zona supravegheată;

10. Instituţia, va informa în prealabil, persoanele vizate, în formă scrisă, prin publicarea pe portalul de internet al instituţiei, prin afişare la sediul instituţiei sau la evenimente, conferinţe, şedinţe, etc de faptul ca instituţia 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 şi prelucrate.

CAP. VII DREPTURILE PERSOANELOR FIZICE VIZATE DE PRELUCRĂRILE DE DATE

1. In 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);
2. Inainte 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;
3. Acordarea şi retragerea consimţământului vor fi disponibile pe cale electronica;
4. In cazul în care consimţământul implică un copil (persoana sub 16 ani) retragerea consimţământului, trebuie să fie autorizată de titularul răspunderii părinteşti asupra copilului.

14 .Dreptul la informare

1. In 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;
2. In 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:
   a. Identitatea şi datele de contact ale operatorului sau al operatorului împuternicit;
   b. Datele de contact ale Responsabilului cu protecţia datelor;
   c. scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridică al prelucrării;
   d. Interesele legitime urmărite de operator sau de o parte terţă, dup este cazul; destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
   e. Perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
3. Existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
4. Daca prelucrarea se bazează pe consimţământul persoanei vizate, se vor comunica si următoarele:
   a. Existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia; dreptul de a depune o plângere în fata unei autorităţi de supraveghere.
   b. Se vor comunica persoanei vizate şi situaţia în care furnizarea de date cu caracter personal reprezint o obligaţie legală sau contractuală, necesară pentru încheierea unui contract şi dacă persoana vizată este obligată să furnizeze aceste date şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

15.Dreptul de acces

1. Persoana vizată are dreptul să solicite organizaţiei o confirmare că datele personale sunt prelucrate, iar în caz afirmativ, are dreptul de a obţine o copie a acestor date, precum şi următoarele informaţii:
   a. Scopurile prelucrării;
   b. Categoriile datelor cu caracter personal în cauză;
   c. Destinatarii sau categoriile de destinatari ai datelor, dacă există, în special orice ţări terţe sau organizaţii internaţionale;
   d. Durata de stocare a datelor cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade);
   e. Drepturile persoanei vizate la rectificarea sau ştergerea datelor sale cu character

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.

4. In 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.

19.Dreptul la portabilitatea datelor

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;

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.

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

20.Dreptul la opoziție

a. 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.
b. 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.
c. 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.

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

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. Persoana vizată are, de asemenea, dreptul de a-și exprima punctul de vedere, de a solicita intervenție umană și de a contesta decizia.

2. Se exceptează de la acest drept, următoarele situații:
a. Este necesară pentru încheierea sau executarea contractului;
b. Este autorizată prin lege națională sau europeană;
c. Se bazează pe consimțământul explicit al persoanei vizate.

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;

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

22. Politici si responsabilități ale operatorului

In 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

m. Este strict interzisă distribuirea oricăror documente interne sau alte informaţii către persoane neautorizate;

n. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;

o. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice echipament al organizaţiei (PC, server, reţea internă). Nerespectarea acestei reguli aduce după sine posibilitatea desfacerii contractului de muncă sau alte măsuri disciplinare;

p. Toate sursele externe (CD, ataşamente la e-mail, stick-uri, hard-disk etc) vor fi verificate cu un program anti-virus;

q. Este strict interzisă utilizarea sistemelor IT în alte scopuri decât îndeplinirea atribuţiilor de serviciu;

r. Infrastructura IT (Servere, Echipamente reţea, website) vor fi scanate de vulnerabilităţi 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 recurenţă cel puţin semestrială;

s. Este interzisă orice intervenţie asupra echipamentelor IT de către personal neautorizat de către instituţie în mod scris;

t. Se interzice folosirea oricărui echipament IT de către orice persoană care nu face parte din personalul instituţiei fără acordul prealabil şi scris al conducerii instituţiei;

u. Mijloacele de autentificare în sistem (nume utilizator, parolă etc) sunt proprietatea fiecărui angajat şi el este singurul responsabil de a nu divulga aceste informaţii. De asemenea se recomandă utilizarea de sisteme de autentificare cu dublu factor (SMS, Token, etc.)

v. Este strict interzisă utilizarea datelor de acces ale altui angajat;

w. Fiecare angajat va fi responsabil să menţină securitatea oricărei informaţii, şi în special informaţiilor personale (datelor cu caracter personal) şi să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere);

x. Pentru copierea fişierelor electronice, instituţia îşi rezervă dreptul de a depune plângere penală împotriva angajatului şi de a-l acţiona pe acesta la instanţele civile pentru acoperirea oricărui prejudiciu adus f instituţiei;

y. Este interzisă navigarea prin fişierele personale sau conturile altor angajaţi, cu excepţia cazului în care acest lucru a fost aprobat în prealabil;

z. Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizare complet;

aa. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situaţii excepţionale şi, în toate cazurile, cu respectarea tuturor obligaţiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicire şi, în special, existenţa unor clauze contractuale exprese privind protecţia datelor;

bb. Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă;

cc. Sistemul trebuie blocat ori de câte ori angajatul părăseşte biroul sau nu utilizează calculatorul, iar după terminarea programului, calculatorul va fi închis;

dd. Este strict interzisă utilizarea „Prinţ 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;

ee. Listarea documentelor ce conţin date cu caracter personal se va realiza doar de către utilizatorii autorizaţi sau cu aprobarea scrisă şi prealabilă a conducerii;

ff. Se va realiza back-up periodic la toate informaţiile stocate pe sistemele IT;

gg. Angajaţii nu vor uita documente pe birou care conţin date cu caracter personal după terminarea programului sau în pauză;

hh. Angajaţii vor lua din imprimantă documentele proprii imediat după tipărire.

ii. In funcţie de modificările aduse de legislaţie, precum si de îmbunătăţirea continua a procedurilor, a masurilor de securitate asupra infrastructurii IT, instituţia noastră, va actualiza prezenta politica privind securitatea informaţiei, in situaţia in care modificările aduse vor fi substanţiale;

sistemele informatice ale societăților cu servicii in IT ce oferă mentenanță, înregistrările audio, video și fotografierea, precum și difuzarea acestora în mediul internet.

f. 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;

2. Specialistul IT (serviciul extern),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;

3. Specialistul IT (serviciul extern), 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.;

4. Un rol deosebit de important, îl are Specialistul IT (serviciul extern), 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;

5. Specialistul IT (serviciul extern), 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.;

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;

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;

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, 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;

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;

26. Reguli generale pentru angajații instituției

1. Singurele persoane care sunt apte să acceseze datele personale sunt cele cărora le este necesară pentru activitatea pe care o realizează;

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;

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;

4. Angajații trebui să asigure securitatea datelor luând precauții și folosind instrucțiunile de mai jos si vor utiliza parole puternice;

5. Datele personale nu vor fi dezvăluite către persoane neautorizate, fie din interiorul companiei sau în afară;

2. Datele vor fi păstrate în puține locuri. Personalul nu trebuie să creeze alte locuri adiționale deloc necesare, ca de exemplu copii inutile;

3. Personalul ar trebui să se folosească de fiecare oportunitate pentru a asigura actualizarea datelor;

30 Precizări privind furnizare informațiilor

In 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;

31. Divulgarea datelor din alte motive

1. In anumite circumstanțe, legislația permite datelor personale să fie dezvăluite către organele legii fără consimțământul persoanei subiect al datelor;

2. In 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;

32. Cooperarea cu Autoritatea de Supraveghere

1. Instituția își va asumarea rolului de punct de contact pentru Autoritatea de Supraveghere privind aspectele legate de prelucrare a datelor , precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;

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;

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;

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

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

33. Instruirea angajaților cu privire la GDPR

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;

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

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;

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;

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.

34. **Angajamentele angajaților cu privire la protejarea datelor cu caracter personal**

posibilitatea de a monitoriza intervenţiile, de a putea decide si aproba in prealabil accesul in vederea accesării sistemelor sau aplicaţiilor informatice;

3. In vederea autorizării se va avea in vedere reglementarea următoarelor situaţii: utilizarea si accesarea din cadrul instituţiei sau de la distanta (remote acces) a adreselor de e-mail ale instituţiei, a aplicaţiilor, 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 staţiilor de lucru fixe (desktop) sau mobile (laptop), a dispozitivelor mobile (telefoane inteligente si tablete), a camerelor de supraveghere sau a dispozitivelor ce ţin de securitatea fizica a instituţiei, GPS, dispozitive sau echipamente de telecomunicaţii, etc;

Importanta majora se va acorda autorizării angajaţilor, ce vor avea dreptul de a utiliza pe dispozitivele mobile {laptop, tableta, telefon inteligent) proprii sau ale instituţiei, aplicaţii ce vor putea accesa serverul de e-mail al instituţiei, putând vizualiza sau stoca date si informaţii, precum si accesarea infrastructurii IT a instituţiei de la distanta (echipamente IT, camere de supraveghere, echipamente de securitate, echipamente Smart sau IOT, dispozitive sau echipamente de telecomunicaţii, GPS, etc);

4. Toate aceste dispozitive, ale angajaţilor ce au primit autorizare, vor trebui protejate corespunzător, prin limitarea accesului persoanelor neautorizate (colegi neautorizaţi, familie, prieteni, necunoscuţi), accesarea echipamentelor in baza unei parole puternice, criptarea dispozitivelor, activarea GPS si a posibilităţii de găsire a echipamentelor in caz de pierdere sau furt, activarea posibilităţii de ştergere si formatare de la distanta a echipamentului in caz de pierdere sau furt, atunci când construcţia si posibilităţile tehnice ale echipamentelor o permit.

5. In situaţiile foarte limitate in care, doar cu titlu de excepţie, sunt autorizaţi, in baza unei necesitaţi de importanta majora privind operaţiunile instituţiei, unii angajaţi din conducere sau administratorii sistemelor informatice, au necesitatea de a accesa de la distanta sistemele informatice sau au de a avea instalate aplicaţii de gestionare a sistemului informatic de posta electronica, ori alte aplicaţii sau programe informatice (contabilitate, salarizare, situaţii de urgenta, etc), pe dispozitive informatice fixe (calculator desktop, server) personale aflate in locaţii personale, se vor evalua riscurile si se vor securiza cibernetic acele dispozitive de către administratorul IT al instituţiei, asigurându-se ca

6. Dispozitivele accesează doar securizat sau prin VPN sistemele autorizate si au instalate sisteme hardware sau software adecvate pentru o securizare maxima. Aceste operaţiuni fiind efectuate cu supervizarea DPO Responsabilului cu Protecţia Datelor si aprobarea conducerii primariei;

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 instituţionala, ce vor trebui sa reducă orice risc privind protejarea datelor cu caracter personal;

8. Astfel, se recomanda ca pe lângă sistemele de securitate antiefracţie instalate, sa se implementeze in instituţie sisteme de monitorizare si control;

9. In punctele foarte sensibile precum Centrul de Date unde sunt locate echipamentele esenţiale din instituţie, precum si in Arhiva instituţiei unde se afla toate documentele arhivate, precum si in alte puncte sensibile, se vor implementa sisteme de supraveghere video, sisteme antiefracţie, sisteme de control al accesului, sisteme anti incendiu, sisteme de monitorizare a temperaturii si sisteme anti inundaţie, etc.;

10. Toate încăperile din instituţie, vor fi prevăzute cu sisteme de închidere, control al accesului si sisteme antiefracţie (grilaje la parter sau etaje inferioare ori sisteme de alarmare anti efracţie);

11. Staţiile de lucru fixe si mobile, vor fi securizate prin parola puternica de acces, iar staţiile ce prelucrează date cu caracter personal sau confidenţiale in măsura in care posibilităţile tehnice o permit, vor fi securizate prin criptare integrala sau parţiala si nu vor împărtăşi in reţeaua locala discuri sau dosare, iar instalarea programelor va fi limitata, putând fi efectuata doar de către administratorul IT;

12. Toate staţiile de lucru vor avea instalate doar sisteme de operare si programe de calculator licenţiate si vor fi securizate prin instalarea de programe de securitate informatica de tip antivirus si firewall configurate corespunzător, încât sa asigure securitatea staţiei de lucru, in timpul prelucrării datelor, a accesării internetului precum si a utilizării suporturilor informatice (cd, dvd, memorii externe);

anonimiza datele cu caracter personal ale persoanelor fizice si pentru a îndeplini obligaţiile prevăzute de Regulamentul U.E. 679/2016;

36. Supravegherea video, înregistrările audio, video si fotografierea

1. Intrucât, dezvoltarea tehnică în domeniul IT, telecomunicaţii şi echipamente tehnice, permite acum înregistrare şi difuzarea în orice moment, a imaginilor, a vocii, a comportamentului, precum şi a alor elemente ce pot duce la identificarea persoanelor, fiind în esenţă prelucrări de date cu caracter personal, se va avea în vedere gestionarea situaţiilor, precum şi încadrarea acestor situaţii în regulamente si proceduri, care săgaranteze respectarea Regulamentului U.E. 679/2016, precum şi a drepturilor persoanelor vizate;
2. Specialistul IT(serviciul extern), precum şi Responsabilul cu date cu caracter personal, vor avea un rol cheie în identificarea tuturor situaţiilor, ce necesită înregistrări audio, video sau fotografiere, precum: supravegherea video CCTV a instituţiei, a imobilelor si a spatiilor publice, înregistrări (video-foto) şi difuzări ale: şedinţelor, investiţiilor (construcţii noi, modernizări, amenajări), festivităţilor, evenimentelor culturale sau de orice natura, din primărie, din instituţiile subordonate sau colaboratoare si de pe raza localităţii, în vederea mediatizării si popularizării localităţii şi/sau a instituţiei, în mass media, radio, tv, publicaţii, precum si în mediul internet, cu respectarea Regulamentului U.E. 679/2016 GDPR;
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 şi difuzările realizate de către instituţie prin personalul responsabil sau de către operatorii împuterniciţi, respectă in totalitate drepturile persoanelor vizate precum şi Regulamentul U.E. 679/2016;
4. Angajaţii instituţiei vor fi instruiţi în legătură cu aspectele legale privind protecţia datelor personale şi cu privire la riscurile pe care le comportă prelucrarea datelor personale;
5. Se va asigura monitorizarea instituţiei, a centrului de date şi a obiectivelor importante prin sistemul CCTV de supraveghere video;
6. Personal specializat va asigura monitorizarea permanentă şi intervenţia în cazul situaţiilor ce ţin de securitatea instituţionala, a infrastructurii informatizate, echipamentelor IT&C şi a datelor;
7. Se vor respecta cu stricteţe procesele privind circuitul documentelor, începând cu înregistrarea, regulile de păstrare, procesare, multiplicare, transport, distrugere şi arhivare conform Nomenclatorului Arhivistic, stabilite şi prin Legea Arhivelor Naţionale sau legislaţia internă şi internaţională privind protecţia datelor cu caracter personal, urmându-se şi procedurile interne în acest scop;
8. Se vor stabili pentru fiecare angajat tipurile de acces la date, încăperi, infrastructură informatizată şi operaţiunile permise doar pentru îndeplinirea atribuţiilor de serviciu, conform fisei postului;
9. Se vor lua măsuri de salvare a bazelor de date ale instituţiei, prin copii de siguranţă la un interval necesar să asigure siguranţa acestor baze de date în situaţii neprevăzute, pentru a se elimina orice risc de pierdere a datelor; în acest sens se va desemna un specialist care să aibă atribuţii de serviciu şi executarea copiilor de siguranţă ale bazelor de date ale sistemelor informatice sau staţiilor de lucru;
10. Angajaţii care prelucrează date cu caracter personal sunt obligaţi să îşi închidă sesiunea de lucru sau să blocheze ecranul terminalelor de acces atunci când părăsesc biroul iar la sfârşitul programului de lucru să închidă computerele;
11. Imprimarea prin intermediul imprimantelor a datelor cu caracter personal se va realiza numai de angajaţii autorizaţi, iar unde tehnologia o permite, imprimantele vor tine evidenţa imprimărilor sau se vor proteja cu o parole;
12. Angajaţii vor avea dreptul să prelucreze date cu caracter personal doar pe perioada în care ocupă funcţia respectivă, cu extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal atunci când intervin situaţii precum modificarea raporturilor de muncă sau a atribuţiilor, prevăzute în fişa postului, cu impact asupra DCP;
13. Astfel, se va suspenda dreptul de acces al angajaţilor la sisteme ce presupun prelucrarea datelor cu caracter personal, pe perioada în care acesta se afla în una dintre următoarele situaţii:

a. S-au stabilit cu exactitate cerinţele referitoare la produsele sau serviciile ce se doresc a fi achiziţionate, sau specificul colaborării ce urmează a fi perfectate;
b. Dacă, deja persoana împuternicită prelucrează datele cu caracter personal în numele Operatorului, sau urmează să prelucreze după încheierii contractului cu Operatorul;
c. Este indicat, ca această procedură să fie utilizată de fiecare dată când instituţia are în vedere, externalizarea sau achiziţionarea unor servicii, produse ce implică prelucrări de date cu caracter personal aparţinând Operatorului, de către persoane juridice în calitate de împuterniciţi;

39. Procedură de evaluare a persoanelor juridice împuternicite

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.
2. Evaluarea GDPR a persoanei împuternicite ar trebui făcută utilizând chestionarul de evaluare şt păstrată ca dovadă a evaluării, precum şi în baza dovezilor puse la dispoziţie de către persoana împuternicită;
3. In prima faza a evaluării, va înmâna persoanei juridice „ Scrisoarea de conformitate cu GDPR, către persoanele juridice împuternicite" anexând şi „Formularul de verificare a persoanelor juridice împuternicite", aceasta având obligaţia de al înapoia Operatorului, completat cu acurateţe conform cerinţelor din formular;
4. In a doua fază, se vor solicita persoanei juridice împuternicite dovezi că dispun de resursele necesare şi are capacitatea de a proteja datele cu caracter personal ale Operatorului, este aliniat[la Regulamentul U.E. 679/2016 şi la legislaţia privind securitatea cibernetică;
5. Dovezile pot fi: proceduri, politici, regulamente, analize GAP, analize DPIA, dovezi ale conformării cu GDPR, audituri, certificări ale firmei şi ale specialiştilor, ISO 27001, dovezi de conformare cu legislaţia securităţii cibernetice, privind infrastructura informatizată, sistemele informatice, metode de prevenţie, criptare, copii de protecţie şi securizare date, precum şi echipamentele unde se vor prelucra şi stoca datele cu caracter personal în numele Operatorului;
6. In a treia fază se vor cerceta în detaliu, „Formularul de verificare a persoanelor juridice împuternicite", completat de către persoana juridică împuternicită şi se vor verifica informaţiile privind persoana juridică împuternicită;
7. Compania care face obiectul evaluării, serviciile sau produsele furnizate, şi identificarea datelor cu caracter personal care sunt sau pot fi împărtăşite cu împuternicitul;
8. Se vor face cercetări în privinţa companiei care furnizează serviciile sau produsele, precum data înfiinţării, sediul social, sediile secundare, sediul unde sunt locate sistemele informatice ce vor prelucra datele Operatorului, administratori, numărul de angajaţi, serviciile sau produsele, portofoliul de clienţi, situaţia juridică, economică, solvabilitatea şi rezultatele financiare ale companiei;
9. Se vor verifica în detaliu, oferta tehnică şi comercială, termenii contractuali, durata, legea aplicabilă, reînnoirea şi rezilierea, precum şi termenii sau clauzele privind protecţia datelor;
10. Din dovezile puse la îndemână de către persoana juridică, verificaţi cu acurateţe, politicile, procedurile, responsabilizarea angajaţilor, subcontractanţii (dacă este cazul cu serviciile subcontractate), auditările, certificările, ISO, privind GDPR, confidenţialitatea şi securitatea cibernetică;
11. Ca urmare a unui contract între părţi, definiţi ce date cu caracter personal ale Operatorului sunt prelucrate, stocate de către împuternicit şi care este scopul prelucrărilor. Specificaţi dacă sunt prelucrate şi categorii de date speciale şi care ar fi volumul total al prelucrărilor;
12. Va trebui stabilită cu exactitate, locaţia 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;
13. Este de preferat ca locaţia echipamentelor să fie la sediul împuternicitului, sau în Romania într-un centru de date securizat care să garanteze protecţia datelor şi să fie conforme cu Regulamentul U.E. 679/2016;

6. De asemeni, partenerii comerciali si colaboratorii, vor fi informaţi prin orice mijloc de corespondenta, in privinţa alinierii de către instituţie cu Regulamentul UE 679/2016.

7. Se aprobă şi se introduce în circuitul documentelor din cadrul UAT Comuna Girov, documentaţia specifică implementării GDPR din Anexa 1 „Documentaţie specifică implementării Regulamentului UE 679/2016", parte integrantă a prezentului Regulament.

8. Documentaţia specifică GDPR din Anexa 1 „Documentaţie specifică implementării Regulamentului UE 679/2016", se introduce in circuitul documentelor UAT Comuna Girov precum şi a instituţiilor subordonate, in vederea utilizării, pentru alinierea si conformarea instituţiei cu Regulamentul UE 679/2016 si a Directivei UE 680/2016 ale Parlamentului European şi a Consiliului Europei cu privire la protecţia datelor cu caracter personal;

9. Elemente ale documentaţiei, în funcţie de fiecare situaţie specifică, se vor pune la dispoziţia angajaţilor, de către şefii de direcţii, servicii, compartimente, etc., la indicaţia si cu supervizarea DPO Responsabilului cu Protecţia Datelor, spre informare si consultare, pe suport electronic si tipărit, disponibile in mod permanent in fiecare departament;

10. Toate documentele aprobate, sunt obligatorii in toate elementele sale, pentru întreg personalul din cadrul UAT Comuna Girov şi a instituţiilor subordonate, fiecare document in funcţie de specificul sau, va fi asumat si utilizat in direcţia, serviciul, compartimentul, biroul, adecvat, sub îndrumarea DPO - Responsabil cu Protecţia Datelor;

11. Planul de masuri, in vederea alinierii instituţiei la Regulamentul U.E. 679/2016 GDPR, verificat si aprobat, se adoptă in cadrul UAT Comunei Girov, începând cu implementarea imediata a procedurilor si masurile operaţionale si in cel mai scurt timp cu implementarea soluţiilor 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 fişiere, sisteme de criptare, copii de siguranţa ale datelor, redundant si independent energetic, in vederea alinierii complete la Regulamentul U.E. 679/2016 GDPR;

12. Toate documentele enumerate mai sus, sunt anexate la prezentul Regulament şi sunt obligatorii in toate elementele sale, pentru întreg personalul din cadrul Aparatului de specialitate al U.A.T Comuna Girov;

13. Politicile şi procedurile menţionate, asumate de către instituţie, reprezintă ansamblul de reguli ce se vor respecta de către toţi angajaţii instituţiei, ca si regulament intern, fiind dovada către terţi a alinierii instituţiei cu Regulament UE 679/2016;

14. DPO Responsabilul cu Protecţia Datelor, va transmite prezentul regulament, precum şi documentaţia adecvată, conducătorilor de compartimente, care la rândul lor le vor comunica tuturor angajaţilor instituţiei, respectiv către terţi, la indicaţiile DPO DPO - Responsabilul cu protecţia datelor, va face demersurile in vederea informării prin intermediul portalului de internet al instituţiei astfel:

15. Crearea unei secţiuni distincte denumita GDPR, vizibila si accesibila dîn prima pagina a portalului;

16. 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;

17. Tot in aceasta secţiune se vor afişa documentele:

a. Nota de informare persoane vizate, privind prelucrarea datelor cu caracter personal;
b. Politica privind confidenţialitatea a portalului de internet;
c. Politica privind supravegherea video prin sistem CCTV;

18. La prima accesare a portalului, va trebui sa apară o opţiune vizibila in prin plan ce sa conţină următoarele doua elemente principale:

a. Un link prin accesarea căruia vizitatorii vor avea acces la Politica privind confidenţialitatea a portalului de internet (se va introduce formularul POL03);
b. Un buton de „Accept" prin care vizitatorii portalului îşi vor da acceptul referitor la aceasta politica;

2. Operatorul este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prevederile legislaţiei GDPR. Persoana împuternicită de operator este răspunzătoare numai în cazul în care nu a respectat obligaţiile din legislaţia sau nu s-a conformat acordului cu operatorul.

44. Condiţii generale pentru impunerea amenzilor administrative

1. Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislaţiei specifice este, în fiecare caz, eficace, proporţional şi disuasiv;
2. în funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menţionate de legislaţia GDPR.
3. Autoritatea poate sa ia următoarele masuri:
   a. Să emită avertizări, să emită mustrări, să dea dispoziţii
   b. Să oblige operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor;
   c. Să limiteze sau să interzică prelucrarea;
   d. Să dispună rectificarea sau ştergerea datelor sau restricţionarea prelucrării.
4. în cazul în care operatorul va fi sancţionat administrativ pentru nerespectarea legislaţiei privind protecţia datelor cu caracter personal, Responsabilul de protecţia datelor va analiza oportunitatea contestării sancţiunii administrative şi va formula propuneri în legătură cu promovarea căii de atac, precum şi, dacă este cazul, va elabora contestaţia, urmând să analizeze cel puţin următoarelor aspecte:
   a. Natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;
   b. Dacă încălcarea a fost comisă intenţionat sau din neglijenţă;
   c. Orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
   d. Gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia;
   e. Eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
   f. Gradul de cooperare cu Autoritatea de Supraveghere pentru a remedia încălcarea sau a atenua posibilele efecte negative ale încălcării;
   g. Categoriile de date cu caracter personal afectate de încălcare;
5. Modul în care încălcarea a fost adusă la cunoştinţa Autorităţii de Supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
6. In cazul în care măsurile menţionate de legislaţia specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauza cu privire la acelaşi obiect, obligarea la respectarea respectivelor masuri;
7. Aderarea la coduri de conduită sau la mecanisme de certificare aprobate;
8. Responsabilul de date personale va reprezenta operatorul în cadrul procedurii administrative în fata Autorităţii cât şi în situaţia în care se va contesta decizia Autorităţii în fata instanţelor judecătoreşti;
9. In situaţia neconformării fata de Regulamentul UE 679/2016 GDPR, se poate atrage aplicarea de amenzi administrative cuprinse între 10.000.000 EUR şi 20.000.000 EUR sau între 2% si 4% din cifra de afaceri total anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul valoarea cea mai mare.

CAP. XIV RESPONSABILITĂŢI

45. Responsabilităţi in cadrul UAT Comuna Girov

1. Prezentul Regulament este obligatoriu întregului personal al UAT Comuna Girov, iar cunoaşterea şi aplicarea corespunzătoare a prezentului regulament reprezint obligaţia tuturor angajaţilor;

1. Conducătorii structurilor organizatorice ale UAT Comuna Girov sunt responsabili cu protecţia datelor cu caracter personal pentru activităţile coordonate şi au următoarele responsabilităţi:

a. Stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal în următoarele situaţii: în vederea desfăşurării curente a activităţi instituţiei, în vederea îndeplinirii obligaţiilor legale, pentru derularea activităţii comerciale, contractuale, participarea le evenimente, etc.;
b. Asigură implementarea GDPR, coordonând şi monitorizând activitatea personalului din subordine în vederea respectării Regulamentului;
c. Asigură desfăşurarea pregătirii de specialitate şi instruirea utilizatorilor conform GDPR;
d. Dispun măsuri de completare sau, dup caz, de modificare a fişei posturilor angajaţilor;
e. Analizează şi dispun suspendarea sau revocarea dreptului de acces al utilizatorilor la sistemele informatice ce conţin date cu caracter personal, la arhiva sau la documentaţie specific;
f. Dispun măsuri organizatorice in vederea exercitării drepturilor de către persoana vizată;
g. Coordonează procesul de furnizare a datelor şi informaţiilor necesare în vederea soluţionării cererilor persoanelor vizate;
h. Analizează periodic activitatea angajaţilor în privinţa GDPR si a securităţii cibernetice;
i. Informează operativ Responsabilul de protecţia datelor despre vulnerabilităţile şi riscurile semnalate în sistemele informatice sau riscuri de securitate a prelucrărilor DCP şi orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate şi propune măsuri pentru înlăturarea acestora;

49. Responsabilităţi ale angajaţilor UAT Comuna Girov

1. Să cunoască şi să aplice prevederile Regulamentului precum şi a legislaţiei GDPR.
2. Să aplice procedurile de informare a persoanelor vizate şi să le pună la dispoziţie notele de informare şi după caz declaraţiile de consimţământ, atunci când datele cu caracter personal sunt colectate direct de la aceştia.
3. Vor oferi peroanelor vizate informaţii cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, conidiile în care pot fi exercitate aceste drepturi etc.;
4. Să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin şefilor ierarhici, conducerii instituţiei, pentru realizarea activităţilor specifice ale acestora;
5. Să păstreze confidenţialitatea datelor prelucrate, a datelor de acces la sistemele informatice prin care sunt gestionate date cu caracter personal;
6. Să respecte masurile de securitate, precum şi celelalte reguli stabilite la nivelul instituţiei
7. Să informeze de imediat şeful ierarhic şi Responsabilul cu protecţia datelor DCP, în situaţii precum: breşe informatice, atacuri informatice, vulnerabilităţi, pierderi de date,
8. defecţiuni tehnice ale sistemelor informatice, accesări neautorizate, pierderi sau diseminări de date DCP, etc.

50. Răspunderi ale structurilor Achiziţii Publice, Juridic, şi DPO

1. Au responsabilitatea şi obligativitatea încheierii de acorduri sau adăugarea de clauze contractuale în contractele încheiate şi gestionate de către aceştia privind GDPR, la indicaţia DPO;
2. In situaţiile în care sunt prelucrate date cu caracter personal în numele UAT Comuna Girov de către persoane împuternicite ,vor avea responsabilitate şi obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite, acorduri de prelucrare a datelor cu caracter personal;
3. Au responsabilitatea şi obligativitatea încheierii de acorduri în contractele încheiate şi gestionate de către aceştia privind GDPR, cu operatorii IT cu acces la sistemele informatice ale instituţiei;
4. In funcţie de situaţiile ce se impun, derulează achiziţiile de 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

52. Responsabilităţi ale Compartimentului Resurse Umane

1. Asigură informarea potenţialilor angajaţi şi a angajaţilor instituţiei cu privire la prelucrarea datelor cu caracter personal şi la drepturile de care beneficiază potrivit legii;
2. Participă la organizarea programelor de pregătire continuă a angajaţilor în GDPR;
3. Asigură responsabilizarea angajaţilor cu privire la GDPR, iar la angajarea salariaţilor în cadrul instituţiei, pune la dispoziţia acestora în documentele în vederea informării şi luării la cunoştinţă cu privire la prevederile prezentului Regulament şi a legislaţiei GDPR şi se asigură de semnarea de către salariaţi a acordurilor de confidenţialitate.
4. Se va avea totodată în vedere pentru fiecare angajat, completarea fisei postului şi a contractelor de muncă cu responsabilităţile privind GDPR şi a prezentului Regulament. în acest sens se vor semna acte adiţionale la contractual de muncă sau anexe la fisa postului, după caz, în funcţie de angajat, funcţionar public sau contractual.
5. Va informa Conducerea Unităţii si va face toate demersurile necesare pentru a asigura resursele umane necesare asigurării securităţii cibernetice, precum si a implementării Regulamentului UE 679/2016 GDPR.
6. In situaţia in care resursele umane interne nu sunt disponibile sau se verifica situaţii de incompatibilităţi, se vor face demersurile necesare in vederea angajării, transferului intre departamente, a calificării personalului sau se va propune externalizarea serviciilor către operatori economici specializaţi, cu experienţa, care sa întrunească condiţiile si sa poată oferi serviciile la standarde cat mai superioare.

53. Responsabilităţi ale Compartimentului IT/Responsabil IT

1. Luarea măsurilor tehnice şi organizatorice, specifice zonei IT&C, prevăzute de prezentul Regulament;
2. Elaborarea, implementarea şi monitorizarea permanentă a politicilor şi a procedurilor specifice de protecţie şi securitate a datelor cu caracter personal la nivelul instituţiei;
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;
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;
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;
6. Evaluarea fiecărui serviciu al terţilor pe care compania îl consideră că utilizează sau stochează date, precum Cloud sau SaaS;
7. Implementează măsuri pentru pseudonimizarea şi criptarea datelor DCP;
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;
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;
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;
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.