

**ROMANIA**  
**JUDETUL ALBA**  
**COMUNA METES**  
**PRIMAR**

**DISPOZITIE**

**privind desemnarea doamnei Oancea Georgeta –Adriana-  
responsabil cu protecția datelor cu caracter personal**

Primarul comunei Metes, judetul Alba;

Vazand diploma de absolvire al cursului pentru pregatirea si calificarea responsabilului cu protectia datelor(DPO) al d-nei Oancea Gergeta Adriana;

Având în vedere temeiurile juridice prevăzute de dispozițiile:

- a) art. 15 alin. (2), art. 26, art. 28, art. 120 alin. (1) și art. 121 alin. (1) și alin. (2) din Constituția României, republicată;
- b) art. 3, art. 4 și art. 6 paragraful 1 din Carta europeană a autonomiei locale, adoptată la Strasbourg la 15 octombrie 1985, ratificată prin Legea nr. 199/1997;
- c) art. 7 alin. (2) din Legea nr. 287/2009 privind Codul civil, republicată, cu modificările ulterioare;
- d) art. 21, art. 24 și art. 28 din Legea cadru a descentralizării nr. 195/2006, cu modificările și completările ulterioare;
- e) art. 154 , art. 155 alin. (1) lit. d) raportat la alin. (5) lit.e) din OUG nr.57/2019-privind Codul administrative;
- f) Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare;
- g) Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare;
- h) art. 37-39 din Regulamentul Parlamentului European și Consilului Uniunii Europene nr. 679/2016 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 (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) - (General Data Protection Regulation - GDPR);
- i) Deciziei *Președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal* nr. 99/2018 privind încetarea aplicabilității unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date,

având în vedere că Regulamentele emise de organele UE au aplicabilitate generală, ca o lege internă, fiind obligatorii în toate părțile sale și cu aplicabilitate nemijlocită, fără să fie necesară adoptarea unei legi naționale de aplicare,

în temeiul prevederilor art. 155 alin. (1) lit.c) coroborat cu alin.(4) si ale art.196 alin.(1) lit."b" din OUG nr.57/2019 –privind Codul administrative emite următoarea

## **D I S P U N E**

**Art. 1.** –Se aproba Regulamentul privind protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date –conform anexa nr.1 la prezenta dispozitie;

**Art.2 (1) Se desemnează doamna OANCEA GEORGETA-ADRIANA, Inspector, grad profesional Principal** - compartimentului Agricol din cadrul aparatului de specialitate al primarului comunei, **responsabil cu protecția datelor cu caracter personal** pentru autoritățile administrației publice locale ale comunei Metes.

**Art. 3.** – Persoana prevăzută la art. 1 îndeplinește și următoarele sarcini, în calitate de reponsabil cu protecția datelor cu caracter personal:

a) informează și consiliază autoritățile administrației publice locale , precum și angajații care se ocupă cu prelucrările de date;

b) monitorizează respectarea Regulamentului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, a altor dispoziții de drept ale Uniunii sau de drept intern referitoare la protecția datelor;

c) consiliază autoritățile administrației publice locale, în ceea ce privește realizarea unei analize de impact asupra protecției datelor și monitorizează executarea acesteia;

d) cooperează cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal și reprezintă punctul de contact cu aceasta;

e) ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare a datelor cu caracter personal, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării, în îndeplinirea sarcinilor sale;

f) creează, conduce și păstrează o evidență a tuturor categoriilor de operațiuni de prelucrare efectuate în numele autorităților administrației publice locale.

**Art. 4.- (1)** Cu atribuțiile prevăzute la art. 3 se completează fișa postului, persoanei prevăzute la art. 1.

(2) Pentru îndeplinirea sarcinilor sale, responsabilul cu protecția datelor cu caracter personal, beneficiază de următoarele resurse:

a) sprijin activ al funcției din partea conducerii;

b) alocarea de timp pentru îndeplinirea atribuțiilor sale;

c) comunicare oficială, către toți angajații, a Dispoziției de desemnare;

d) sprijin, reacții și informații din partea tuturor compartimentelor ale aparatului de specialitate al primarului comunei;

e) perfecționarea pregătirii profesionale.

**Art. 5.** - Cu aducerea la îndeplinire a prezentei dispoziții se însărcinează *d-na Haragus Nicoleta Silvia*, consilier achizitii publice în cadrul aparatului de specialitate al primarului comunei, fiind desemnata si persoana responsabila cu resursele umane REVISAL si d-na Oancea Georgeta Adriana-Inspector in cadrul aparatului de specialitate al primarului;

**Art. 6. (1)-** Impotriva prezentei dispozitii ,persoana care se considera vatamata intr un drept al sau sau intr un interes legitim poate formula plangere prealabila la primarul comunei Metes,in termen de 30 de zile de la data comuncarii ;

**(2)** Prezenta dispozitie poate fi contestata la sectia de contencios administrativ a Tribunalului ,in termen de 6 luni de la data comunicarii raspunsului la plangerea prealabila depusa, in conformitate cu prevederile Legii nr.554/2004 ,cu modificarile si completarile ulterioare;

Prezenta dispoziție se comunică în mod obligatoriu, prin intermediul secretarului comunei, în termenul prevăzut de lege, INstitutiei prefectului-judetul Alba, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, persoanei menționate la art. 1 și se aduce la cunoștință publică prin publicarea pe pagina de internet .

Metes la 17.11 /2022

Nr 229 /2022

PRIMARUL COMUNEI METES,

SANZAIANA DANIEL

Sut



Contrasemnăza pentru legalitate:

SECRETAR GENERAL

ELENA MAN

*Elena Man*

ASOCIAȚIA

„CENTRUL PENTRU PROTECȚIA DATELOR”

În colaborare cu

S.C. AMPLUSNET S.R.L. (GDPR COMPLET)

oferă

## Diplomă de Absolvire

Curs pentru Pregătirea și Certificarea  
Responsabilului cu Protecția Datelor (DPO)

Regulamentul General pentru Protecția Datelor cu Caracter Personal

Cursant

**Oancea Georgeta-Adriana**

Asociația „Centrul pentru Protecția Datelor”

Darius Fărcaș



Responsabilul cu protecția datelor cu caracter personal (DPO)

cod COR: 242231

Conf. univ. dr. Nicolae PLOEȘTEANU

Iunie 2022



S.C. Amplusnet S.R.L.  
GDPR Complet

Ionel Orza

## REGULAMENT INTERN DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

### CAP. 1 DISPOZIȚII GENERALE

#### 1.1. Obiect și obiective

1.1.1. Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora;

1.1.2. Prezentul regulament asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal;

1.1.3. Exercițarea drepturilor prevăzute în prezentul regulament nu poate fi restrânsă decât în cazurile expres și limitativ prevăzute de lege.

1.1.4. Libera circulație a datelor cu caracter personal în interiorul Uniunii Europene nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

#### 1.2. Domeniul de aplicare

1.2.1. Prezentul regulament se aplică tuturor angajaților Primăriei comunei Metes cu atribuții de prelucrare a datelor cu caracter personal și/sau după caz persoanelor împuternicite ale Primăriei comunei Metes.

1.2.2. Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată 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.

#### 1.3. Termeni și definiții

În sensul prezentului regulament:

1. **"Date cu caracter personal"** înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("**Persoana vizată**"). O persoana fizica 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;

**2. "Prelucrare"** înseamnă 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* - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale și din orice sursă;
- *înregistrarea* - consemnarea datelor cu caracter personal într-un sistem de evidență automat ori neautomat, care poate fi registru, fișier automat, baza 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;
- *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;
- *adaptarea* - transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;
- *modificarea* - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate, actualitate;
- *extragerea* - scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;
- *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 ulterioară;
- *utilizarea* - folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;
- *dezvăluirea/divulgarea* - a face disponibile date cu caracter personal către terți prin comunicare, transmitere, diseminare sau punerea la dispoziție în orice alt mod;
- *alăturarea* - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

- *combinarea/alinierea* - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
- *blocarea* - întreruperea prelucrării datelor cu caracter personal;
- *restricționarea* - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
- *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;
- *transformarea* - operațiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;
- *distrugerea* - aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

**3. "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 respectivă sau deplasările acesteia;

**4. "Pseudonimizare/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. "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;

**6. "Operator"** înseamnă 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; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ. *În sensul prezentului*

*regulament au calitatea de Operator, UAT comuna Metes / Primăria comunei Metes, cu toate entitățile funcționale/structurile organizatorice – direcții, departamente, servicii, birouri, compartimente, comisii, comitete, etc., dacă stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal.*

**7. "Persoana împuternicită de operator/procesator"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

**8. "Destinatar"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (cărui) 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 respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

**9. "Parte terță"** înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana 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;

**10. "Consimțământ"** al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

**11. "Încălcarea securității datelor cu caracter personal"** înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

**12. "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 biologic recoltate de la persoana în cauză;

**13. "Date biometrice"** 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;

**14. "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;

**15. "Întreprindere"** înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;

**16. "Grup de întreprinderi"** înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

**17. "Reguli corporatiste obligatorii"** înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

**18. "Autoritate de supraveghere/ANSPDCP"** înseamnă Autoritatea Națională de Supraveghere a Datelor cu Caracter Personal;

**19. „Codul numeric personal (CNP)”** 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;

**20. „Date cu caracter personal cu funcție de identificare de aplicabilitate generală (date cu caracter special)”** înseamnă numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;

**21. „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 – CCICJ sau al împuternicitului acestuia ale cărei atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.*

**22. „Responsabilul de protecția datelor”** înseamnă persoana din cadrul instituției cu sarcini/responsabilități specifice privind funcționarea corespunzătoare a sistemului de protecție a datelor cu caracter personal, în conformitate cu prevederile GDPR precum și elaborarea, implementarea și monitorizarea respectării prevederilor prezentului Regulament.

#### **1.4. Documente de referință**

- Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (GDPR);
- Legislația internă aplicabilă în domeniul protecției datelor cu caracter personal;
- OUG nr.57/2019-privind Codul administrativ;
- Regulamentul de organizare și funcționare;
- Regulamente și proceduri interne.

## **CAP.2 PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL**

- 2.1. Legalitate, echitate și transparență** – un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate *„în mod legal, echitabil și transparent față de persoana vizată.”*;
- 2.2. Limitări legate de scop** – datele personale trebuie să fie colectate *în scopuri bine determinate, explicite și legitime*, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică/ istorică ori în scopuri statistice nu se consideră incompatibilă de la scopurile inițiale;
- 2.3. Minimizarea/Reducerea la minimum a datelor** – orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie *cele mai adecvate, relevante și strict limitate* la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;
- 2.4. Exactitatea informațiilor** – datele cu caracter personal trebuie să fie exacte, și, în cazul în care este necesar, trebuie să fie actualizate; operatorii trebuie să ia toate măsurile 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;
- 2.5. Limitarea stocării** – datele trebuie păstrate fix atât timp cât sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepții asociate cu activități de prelucrare în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, conform art. 89, alin.1 din GDPR, sub rezerva punerii în aplicare a măsurilor tehnice și organizatorice adecvate prevăzute de GDPR în vederea garantării drepturilor și libertăților persoanei vizate;
- 2.6. Integritate și confidențialitate** – prelucrarea datelor personale trebuie făcută în cele mai adecvate condiții de siguranță, care să includă „protecția împotriva prelucrării

neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare”.

Nerespectarea acestui principiu expune direct la breșe de securitate și confidențialitate și, implicit, la penalitățile extrem de severe prevăzute de GDPR;

**2.7. Responsabilitate – Operatorul este responsabil de respectarea principiilor GDPR și de a demonstra această respectare.** GDPR impune nu numai respectarea principiilor GDPR – de exemplu, prin documentarea deciziilor luate cu privire la o activitate de procesare, ci și să se demonstreze oricând aceasta respectare (responsabilitate).

**În consecință:**

- *Orice prelucrare de date cu caracter personal trebuie să fie legală și echitabilă;*
- *Ar trebui să fie transparent pentru persoanele fizice vizate că sunt colectate, utilizate, consultate sau prelucrate datele cu caracter personal care le privesc și în ce măsură datele sunt sau vor fi prelucrate;*
- *Principiul transparenței prevede că orice informații și comunicări 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; acest principiu se referă în special la informarea persoanei vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care sunt prelucrate;*
- *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 să își exercite drepturile în legătură cu prelucrarea;*
- *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;*
- *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;*
- *Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace;*
- *Operatorul trebuie să stabilească termene pentru ștergere sau revizuirea periodică. Operatorul trebuie să ia toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse;*

- *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 neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.*

### **CAP. 3 LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

*Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:*

- a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;*
- b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;*
- c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;*
- d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;*
- e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;*
- f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.*

*Nota: „Interesele legitime ale unui operator”, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se afla în serviciul acestuia. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor poate constitui un interes legitim al operatorului de date în cauză.*

## **CAP. 4 CONSIMȚĂMÂNTUL PERSOANEI VIZATE ȘI CONDIȚIILE PRIVIND CONSIMȚĂMÂNTUL**

4.1. În cazul în care prelucrarea se bazează pe consimțământ, operatorul 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.

4.2. În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se refera și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

4.3. Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragera consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragera consimțământului se face la fel de simplu ca acordarea acestuia.

4.4. Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

4.5. *La nivelul Primăriei comunei Metes, ca Operator de date personale, consimțământul persoanelor vizate este acordat :*

- în cadrul procesului de recrutare/selecție de personal;
- în situația încheierii unor contracte;

4.6. În cadrul procesului de recrutare/selecție de personal, persoana responsabilă cu resursele umane va solicita acordarea consimțământului de către potențialul angajat prin semnarea de către acesta a unei *Note de Informare* prin care declară că a fost informat în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de Informare se vor păstra distinct în evidențele Compartimentului Contabilitate-Achiziții publice-Resurse Umane.

4.7. În cazul înregistrării unor date pentru achiziția de produse, lucrări, servicii/achitarea tarifelor online, accesarea unor servicii specifice, precum și în cazul invitațiilor online adresate vizitatorilor specialiști în vederea participării acestora la târguri, expoziții și alte asemenea evenimente etc., consimțământul persoanei vizate este dat prin completarea

formulelor Notă de informare / Declarație de consimțământ sau prin bifarea unor căsuțe dedicate din secțiunea website-ului / softului, acolo unde este posibil.

**4.8.** Dacă prelucrarea datelor personale se bazează pe consimțământ, prelucrarea datelor unui copil este legală dacă acesta are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri dacă titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile. Aceste dispoziții nu afectează dreptul general al contractelor aplicabil în statele membre UE, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

**4.9.** *În toate celelalte cazuri în care Primăria comunei Metes prelucrează date, acestea sunt colectate, procesate, stocate, transmise ca urmare a unor ingerințe legale, motiv pentru care acordul / consimțământul persoanei vizate nu este necesar. În schimb, în toate cazurile, persoana vizată trebuie să fie informată cu privire la drepturile sale, conform regulamentului GDPR.*

## **CAP. 5 REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL**

### **5.1. Prelucrarea unor categorii speciale de date cu caracter personal**

**5.1.1.** Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

#### **5.1.2. Prevederile anterioare nu se aplica în următoarele situații:**

- a) *când persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede că interdicția prevăzută anterior să nu poată fi ridicată prin consimțământul persoanei vizate;*
- b) *când prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat*

în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

c) *când prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se afla în incapacitate fizică sau juridică de a-și da consimțământul;*

d) *când prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și că datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;*

e) *când prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;*

f) *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;*

g) *când prelucrarea este necesară 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;*

h) *când prelucrarea este necesară în 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 asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute de lege; datele cu caracter personal pot fi prelucrate în scopurile menționate anterior în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.*

i) *când prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi 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, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

j) *când prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau al 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.*

## **5.2. Prelucrarea datelor cu caracter personal cu funcție de identificare generală**

Datele cu caracter personal cu funcție de identificare generală (Codul numeric personal - CNP, seria și numărul actului de identitate/pașaportului etc.) vor fi prelucrate, exclusiv în situațiile în care este necesară stabilirea identității persoanelor vizate și prelucrarea este prevăzută în mod expres de o dispoziție legală.

Prin legislația națională se pot detalia condițiile specifice de prelucrare a unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate.

## **5.3. Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni**

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. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

## **5.4. Prelucrarea care nu necesită identificarea**

**5.4.1.** În cazul în care scopurile pentru care Primăria comunei Metes (operatorul) prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării legislației specifice.

**5.4.2.** Dacă, în cazurile menționate anterior, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, prevederile legale privind

dreptul de acces, de rectificare, de ștergere, la restricționarea prelucrării, dreptul la portabilitatea datelor nu se aplica, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale menționate anterior, oferă informații suplimentare care permit identificarea sa.

### **5.5. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video**

**Primăria comunei Metes**, prin intermediul sistemelor de supraveghere video, prelucrează datele cu caracter personal, respectiv imaginea și alte informații ce permit identificarea persoanelor vizate.

Imaginile referitoare la persoane identificate sau identificabile, prelucrate prin mijloace de supraveghere video, constituie date cu caracter personal:

- a) chiar dacă nu sunt asociate cu datele de identificare ale persoanei sau
- b) chiar dacă nu conțin imaginea persoanei filmate, ci alte informații de natură să conducă la identificarea acesteia (ex: numărul de înmatriculare al vehiculului)

Scopul prelucrării datelor personale consta în: monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor, îndeplinirea obligațiilor legale și realizarea intereselor legitime.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate de **Primăria comunei Metes**.

Informațiile înregistrate sunt destinate utilizării de către instituție și pot fi comunicate numai următorilor destinatari: persoana vizată, reprezentanții legali/împuțerniciții persoanei vizate, organele de urmărire/cercetare penală, instanțe judecătorești, în conformitate cu prevederile legislației interne și comunitare aplicabile activității desfășurate de **instituție**.

Informările în cauză, precum și indicatoarele de marcare a existenței sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video-CCTV. *Personalul de pază din cadrul Direcției Administrative va verifica periodic starea fizică a informărilor și a indicatoarelor anterior menționate și va răspunde de siguranța și confidențialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.*

### **5.6. Prelucrarea în contextul ocupării unui loc de muncă**

**5.6.1.** Prin lege sau prin acorduri colective, se pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii,

al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

**5.6.2.** Aceste norme includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce privește transparența prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună și sistemele de monitorizare la locul de muncă.

## **CAP.6 DREPTURILE PERSOANEI VIZATE ÎN CONTEXTUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

### **6.1. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate**

**6.1.1.** OPERATORUL ia măsuri adecvate pentru a furniza persoanei vizate informațiile legale solicitate, precum și orice notificări și comunicări (în situația exercitării drepturilor de care beneficiază potrivit legii) referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

**6.1.2.** Operatorul facilitează exercitarea drepturilor persoanei vizate.

**6.1.3.** Operatorul *furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri prin care își exercită drepturile de care beneficiază în baza legii, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii.* Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor.

**6.1.4.** Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

6.1.5. Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

6.1.6. Informațiile furnizate în temeiul legislației specifice și orice comunicare și orice măsuri luate în baza exercitării drepturilor de care beneficiază, potrivit legii, persoana vizată, sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

- a) fie să perceapă o taxa rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
- b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

6.1.7. În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea prin intermediul căreia își exercită drepturile de care beneficiază, potrivit legii, persoana vizată, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

6.1.8. Informațiile care urmează să fie furnizate persoanelor vizate în temeiul legislației specifice, pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

*6.1.9. Pentru exercitarea drepturilor prevăzute de legislația specifică și de prezentul Regulament, persoanele vizate se pot adresa Responsabilului cu protecția datelor din cadrul Primăriei orașului Hațeg, cu o cerere scrisă, datată și semnată.*

## **6.2. Dreptul la informare**

### **6.2.1. Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate direct de la persoana vizată**

6.2.1.1. În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate următoarele informații:

- a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- b) datele de contact ale responsabilului cu protecția datelor, după caz;

- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) interesele legitime urmărite de operator sau de o parte terță, după caz;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal în afara Spațiului UE și al Zonei Economice Europene și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție sau, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

**6.2.1.2.** *În plus*, față de informațiile menționate anterior, în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate *următoarele informații suplimentare* necesare pentru a asigura o prelucrare echitabilă și transparentă:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- b) 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;
- c) atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- d) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- f) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

**6.2.1.3.** În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante;

6.2.1.4. Prevederile precedente nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

### **6.2.2. Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată**

6.2.2.1 În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

- a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- b) datele de contact ale responsabilului cu protecția datelor, după caz;
- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) categoriile de date cu caracter personal vizate;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal în afara Spațiului UE și al Zonei Economice Europene și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție sau, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

6.2.2.2. *Pe lângă informațiile menționate anterior*, operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- b) interesele legitime urmărite de operator sau de o parte terță, după caz;
- c) 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 și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- d) atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- e) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;

g) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

#### **6.2.2.3. Operatorul furnizează informațiile menționate anterior:**

a) **într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;**

b) **dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau**

c) **dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.**

6.2.2.4. În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante.

#### **6.2.2.5 Prevederile precedente nu se aplică dacă și în măsura în care:**

a) persoana vizată deține deja informațiile;

b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute de lege, sau în măsura în care obligația furnizării informațiilor este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;

c) obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii Europene sau de dreptul intern sub incidența căruia intra operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.

#### **6.2.3. Informarea persoanelor vizate în contextul activităților specifice:**

**Informarea persoanelor vizate se poate realiza, după cum urmează:**

- În cadrul procesului de recrutare/selecție de personal și în contextul derulării raporturilor de muncă, Compartimentului Contabilitate-Achizitii publice- Resurse Umane va pune la dispoziția potențialului angajat / angajatului o *Notă de Informare și o declarație de consimțământ*, pe care acesta/aceasta le va citi și le va semna și prin care declară că a fost informat/a în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de Informare se vor păstra distinct în evidențele Compartimentului Contabilitate-Achizitii publice-Resurse Umane. *Modelul Declarației de consimțământ este prevăzut în Anexa nr.1. Modelul Notei de Informare este prevăzut în Anexa nr. 2;*

- Persoanele vizate, respectiv angajații, clienții/potențialii clienți, vizitatorii și alte persoane care intră în sediul Primăriei comunei Metes, ale căror date sunt prelucrate prin intermediul sistemelor de supraveghere video, sunt informate în acest sens prin intermediul unor *Note de Informare sub forma unor indicatoare de marcarea a existenței sistemului de supraveghere video ce trebuie să fie aplicate în locurile unde sunt amplasate camere de supraveghere video-CCTV. Prevederile se aplică și în cazul sistemului de supraveghere video de la nivelul comunei Metes. Personalul cu atribuții specifice în aceste privințe va verifica periodic starea fizică a informărilor și a indicatoarelor anterior menționate și va răspunde de siguranța și confidențialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.*

- În cadrul derulării activităților contractuale, compartimentul responsabil cu inițierea contractării va pune la dispoziția potențialului contractant o Notă de Informare și o declarație de consimțământ, pe care acesta le va citi și le va semna și prin care declară că a fost informat/a în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de Informare se vor păstra distinct în evidențele compartimentului responsabil. Modelul Declarației de consimțământ este prevăzut în Anexa nr.1. Modelul Notei de Informare este prevăzut în Anexa nr.2.

### **6.3. Dreptul de acces al persoanei vizate**

**6.3.1.** Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

- a) scopurile prelucrării;
- b) categoriile de date cu caracter personal vizate;

- c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;
- d) acolo unde este posibil, perioada pentru care se preconizează ca vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioadă;
- e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
- f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
- h) existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

**6.3.2.** În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate, prevăzute de lege referitoare la transfer.

**6.3.3.** Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

**6.3.4.** Dreptul de a obține o copie menționată anterior nu aduce atingere drepturilor și libertăților altora.

#### **6.4. Dreptul la rectificare**

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

#### **6.5. Dreptul la ștergerea datelor ("dreptul de a fi uitat")**

**6.5.1.** Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a

șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplica unul dintre următoarele motive:

- a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- b) persoana vizată își retrace consimțământul pe baza căruia are loc prelucrarea, și nu există niciun alt temei juridic pentru prelucrarea;
- c) persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării, în cazul prelucrării în scop de marketing direct;
- d) datele cu caracter personal au fost prelucrate ilegal;
- e) 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 afla operatorul;
- f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate în legislația specifică.

**6.5.2.** Alineatele anterioare nu se aplică în măsura în care prelucrarea este necesară:

- a) pentru exercitarea dreptului la liberă exprimare și la informare;
- b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul;
- c) din motive de interes public în domeniul sănătății publice;
- d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în măsura în care dreptul la ștergere este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
- e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

## **6.6. Dreptul la restricționarea prelucrării**

**6.6.1.** Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării *în cazul în care se aplică unul din următoarele cazuri:*

- a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;

c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau

d) persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

**6.6.2.** În cazul în care prelucrarea a fost restricționată conform prevederilor anterioare, astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau 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.

**6.6.3.** O persoană vizată care a obținut restricționarea prelucrării este informată de către operator înainte de ridicarea restricției de prelucrare.

### **6.7. Obligația de notificare cu privire la rectificarea, ștergerea datelor cu caracter personal sau restricționarea prelucrării**

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate.

Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

### **6.8. Dreptul la portabilitatea datelor**

**6.8.1.** Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- a) prelucrarea se bazează pe consimțământ sau pe un contract; și
- b) prelucrarea este efectuată prin mijloace automate.

**6.8.2.** În exercitarea dreptului său la portabilitatea datelor, persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

**6.8.3.** Exercițarea dreptului la portabilitatea datelor nu aduce atingere dreptului la ștergerea datelor. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

**6.8.4.** Dreptul la portabilitatea datelor nu aduce atingere drepturilor și libertăților altora.

## **6.9. Dreptul la opoziție și procesul decizional individual automatizat**

### **6.9.1. Dreptul la opoziție**

**6.9.1.1.** În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se afla, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează ca 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.

**6.9.1.2.** Dacă prelucrarea datelor cu caracter personal are scop marketingul direct, persoana vizată are dreptul de a se opune prelucrării în acest scop a datelor care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

**6.9.1.3** În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

**6.9.1.4.** Cel târziu în momentul primei comunicări cu persoana vizată, dreptul la opoziție menționat este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

**6.9.1.5.** În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situația sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

### **6.9.2. Procesul decizional automatizat, crearea de profiluri**

**6.9.2.1.** Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

#### **6.9.2.2. Prevederile anterioare nu se aplică în cazul în care decizia:**

- a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplica operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

c) are la baza consimțământul explicit al persoanei vizate.

**6.9.2.3.** În cazurile în care decizia este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date sau are la bază consimțământul explicit al persoanei vizate, operatorul de date 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.

**6.9.2.4.** Deciziile menționate anterior nu au la baza categoriile speciale de date cu caracter personal, cu excepțiile prevăzute de lege (ex: persoana vizată și-a dat consimțământul explicit) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

## **CAP. 7 RESTRICȚII**

Prin legislația specifică care se aplică operatorului de date sau persoanei împuternicite de operator se poate restricționa domeniul de aplicare al obligațiilor și al drepturilor prevăzute în actuala legislație în măsura în care dispozițiile acesteia corespund drepturilor și obligațiilor menționate anterior, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

- a) securitatea națională;
- b) apărarea;
- c) securitatea publică;
- d) prevenirea, investigarea, depistarea sau urmărirea penală sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
- e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
- f) protejarea independenței judiciare și a procedurilor judiciare;
- g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
- h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale;

- i) protecția persoanei vizate sau a drepturilor și libertăților altora;
- j) punerea în aplicare a pretențiilor de drept civil.

## **CAP. 8 OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR**

### **8.1. Responsabilitatea Operatorului**

**8.1.1.** Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, costurile implementării precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, *Primăria comunei Metes pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu legislația specifică.*

De asemenea, măsurile tehnice și organizatorice adoptate de instituție sunt necesare protejării datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Respectivul măsuri se revizuiesc și se actualizează dacă este necesar.

*Pentru îndeplinirea cerințelor legale specifice protecției datelor cu caracter personal , Primăria comunei Metes implementează măsuri tehnice și organizatorice orientate pe diferite direcții de acțiune, precum: alocarea/stabilirea responsabilităților pentru Responsabilul de protecția datelor, alocarea/responsabilităților pentru angajații care prelucrează date cu caracter personal, elaborarea regulamentului privind protecția datelor, adaptarea activităților organizației la cerințele legale specifice, elaborarea/implementarea unor politici/proceduri IT adecvate pentru securitatea datelor personale, instruirea personalului, monitorizarea conformității, etc.*

**8.1.2.** Măsurile tehnice și organizatorice *includ punerea în aplicare de către instituție a unor politici/proceduri IT adecvate de protecție/securitate a datelor cu caracter personal. Biroul IT al Primăriei comunei Metes are responsabilitatea/obligativitatea elaborării/actualizării și implementării politicilor/procedurilor adecvate de protecție/securitate a datelor cu caracter personal.*

**8.1.3.** Suplimentar măsurilor anterior precizate, în vederea asigurării unui nivel adecvat de protecție/securitate a datelor cu caracter personal, la nivelul instituției se adoptă/stabilesc măsuri organizatorice și reguli, precum:

- *Toate documentele care conțin date cu caracter personal se înregistrează și urmează regulile de păstrare, procesare, multiplicare, transport, distrugere și arhivare stabilite prin Legea Arhivelor Naționale, legislația internă și internațională privind protecția datelor cu caracter personal, și prin proceduri interne;*

- *Personalul este instruit în legătură cu aspectele legale privind protecția datelor personale și cu privire la riscurile pe care le comportă prelucrarea datelor personale;*

- *Utilizatorul/angajatul instituției poate prelucra date cu caracter personal doar pe perioada în care ocupa funcția respectivă. Extinderea sau restrângerea atribuțiilor de prelucrare a datelor cu caracter personal se dispune de instituție atunci când utilizatorul/angajatul se afla în una dintre următoarele situații:*

- a) *la modificarea raporturilor de muncă;*
- b) *la modificarea atribuțiilor privind prelucrarea datelor cu caracter personal, prevăzute în fișa postului.*

Dreptul de acces al utilizatorului la sistemul de evidență a datelor cu caracter personal se suspendă pe perioada în care acesta se afla în una dintre următoarele situații:

- a) *se află în concediu fără plată, concediu medical, concediu pentru creșterea sau îngrijirea copilului minor, pentru o perioadă mai mare de 3 luni;*
- b) *se afla în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;*
- c) *urmează un curs sau o specializare cu scoatere din program, pentru o perioadă mai mare de 3 luni;*
- d) *pe perioada cercetării disciplinare, în situația în care față de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispozițiilor legale;*
- e) *alte cazuri prevăzute de lege.*

- *Cu ocazia proiectării, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, se interzice accesul providerilor/programatorilor/personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal deținute/create/accesate de personalul din structura respectivă a instituției. În aceste situații, se pun la dispoziția providerilor/programatorilor/personalului de întreținere numai date anonime/pseudonimizate;*

- *Pentru cazuri excepționale, numai pe durata intervenției și circumstanțiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezența unui utilizator desemnat de operator, în această situație, răspunderea pentru păstrarea confidențialității datelor aparține persoanelor în cauză, sens în care trebuie să semneze un Angajament de confidențialitate;*

- Operațiunile de colectare, introducere, modificare și actualizare a datelor cu caracter personal se realizează numai de personalul anume desemnat de către conducătorii operatorului, conform actelor de reglementare internă;
- Primăria comunei Metes dispune măsurile tehnice necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele cu caracter personal;
- Bazele de date cu caracter personal deținute/create și programele folosite de operatori/utilizatori sunt salvate, prin copii de siguranță, la un interval de timp stabilit de conducere, în funcție de mărimea, volumul și importanța acestor baze de date;
- Accesul în încăperile în care se află documente ce conțin date cu caracter personal și/sau terminale de acces/echipamente care prelucrează date cu caracter personal este limitat la utilizatorii stabiliți de conducătorii operatorului și numai pentru îndeplinirea atribuțiilor de serviciu (acces restricționat/controlat);
- Documentele, terminalele de acces/echipamentele care conțin date cu caracter personal vor fi ținute/păstrate în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare și/sau în încăperi/spații care se pot încuia. Documentele care conțin date cu caracter personal, folosite pentru realizarea anumitor operațiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora. Terminalele de acces/echipamentele se securizează cu parolă;
- 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 stabilită, prin proceduri de lucru/diagrame flux, în funcție de operațiunile care trebuie executate.
- Terminalele de acces trebuie să aibă setate funcția de închidere automată a ecranului și funcția „lock screen - screen saver” la o temporizare prestabilită, prin proceduri de lucru/diagrame flux, iar dacă acest lucru nu este posibil din punct de vedere tehnic, după trecerea intervalului de timp stabilit, datele afișate trebuie ascunse sau sesiunea de lucru va fi închisă. Terminalele de acces folosite în relația cu publicul se poziționează astfel încât datele afișate să fie vizualizate numai de către utilizatori;
- Accesul utilizatorilor/angajaților la datele cu caracter personal care se regăsesc în Rețeaua instituției – serverele și stațiile de lucru, se face controlat/restricționat pe bază de user și parolă, setate exclusiv de Biroul IT, utilizatorii având drept de acces limitat, conform procedurilor interne (ex: read only, write, execute, modify, full control etc.);

- *Nu este permisă scoaterea din organizație a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD etc.) care conțin date cu caracter personal, decât cu aprobarea prealabilă a conducerii;*

- Se interzice utilizarea serviciului de e-mail în orice mod ce ar avea drept consecința transmiterea, distribuirea și livrarea de mesaje nesolicitate de poștă electronică în volum mare sau de mesaje comerciale nesolicitate ("Spam"). Prin spam înțelegem trimiterea de mesaje (comerciale) nesolicitate în urma cărora se primesc plângeri din partea celor care le primesc, folosirea sau distribuirea de liste de e-mailuri care aparțin unor persoane care nu și-au exprimat consimțământul anterior.

- *Utilizatorii/angajații nu vor deschide email-uri de tip SPAM/Malware și/sau orice alte comunicații electronice care nu au legătură cu activitatea desfășurată în calitate de angajat. Totodată, angajații CCICJ nu au voie să găzduiască sau să permită găzduirea site-urilor sau informațiilor a căror publicitate este făcută prin emailuri SPAM. **Nerespectarea politicii anti-spam constituie abatere disciplinară și se sancționează potrivit Regulamentului Intern.***

- *Utilizatorii/angajații care prelucrează date cu caracter personal sunt obligați să își închidă sesiunea de lucru, să blocheze ecranul terminalelor de acces atunci când părăsesc locul de muncă, iar la sfârșitul programului de lucru să închidă terminalele de acces;*

- *Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați, și, acolo unde echipamentul de imprimare permite, aceasta operațiune se va realiza controlat, pe bază de parolă.*

***Prezentele reguli și măsuri se completează cu prevederile politicilor și procedurilor elaborate/implementate , reglementări interne necesare pentru asigurarea adecvată a protecției/securității datelor cu caracter personal.***

**8.1.4.** Aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat, menționat de legislația specifică, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

**8.2. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit**

**8.2.1.** Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare (mijloace manuale și/sau automate - ex: sisteme de operare, servere, stații de lucru, soluții de

securitate, de backup, de stocare, programe/soluții software/aplicații IT achiziționate sau dezvoltate in-house etc.), cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate (ex: pseudonimizarea), care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

**8.2.2.** Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

**8.2.3.** Un mecanism de certificare aprobat menționat de legislația specifică poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute anterior.

### **8.3. Persoana împuternicită de Operator**

**8.3.1.** În cazul în care prelucrarea urmează să fie realizată în numele operatorului, acesta contractează exclusiv persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

**8.3.2.** Persoana împuternicită de operator nu recrutează o alta persoană împuternicită fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.

**8.3.3.** Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului.

Respectivul contract sau act juridic prevede în special ca persoana împuternicită de operator:

- a) *prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care aceasta obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;*
- b) *se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;*
- c) *adoaptă toate măsurile tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor personale corespunzător, în conformitate cu cerințele legislației specifice;*
- d) *respectă condițiile menționate privind recrutarea unei alte persoane împuternicite de operator;*
- e) *ținând seama de natura prelucrării, oferă asistența operatorului prin măsuri tehnice și organizatorice adecvate, în măsură în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute de legislația specifică;*
- f) *ajută operatorul să asigure respectarea obligațiilor privind securitatea prelucrării, notificarea Autorității/informarea persoanei vizate în cazul încălcării securității datelor, evaluarea impactului asupra protecției datelor, consultarea prealabilă, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;*
- g) *la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;*
- h) *pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.*
- i) *Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.*

**8.3.4.** În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum sunt prevăzute anterior, revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate.

În cazul în care aceasta a doua persoană împuternicită nu își respecta obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor persoanei împuternicite subsecvent.

**8.3.5.** Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, sau la un mecanism de certificare aprobat, menționate de legislația specifică, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate anterior.

**8.3.6.** Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celalalt act juridic încheiat între persoana împuternicită de operator și o altă persoană împuternicită, se poate baza, integral sau parțial, pe clauze contractuale standard prevăzute/adoptate de Comisia Europeană/ de o autoritate de supraveghere, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul legislației specifice;

**8.3.7.** Contractul sau celalalt act juridic menționat anterior se formulează în scris, inclusiv în format electronic.

**8.3.8.** În cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

**8.3.9.** În situațiile în care sunt prelucrate date cu caracter personal în numele instituției de către persoane împuternicite (procesatori de date - ex: instituții de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariați, companii de curierat etc.) derulatorii de contract ai Primăriei comunei Metes vor avea responsabilitatea/obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite

**8.3.10. 8.4.** Desfășurarea activității de prelucrare sub autoritatea Operatorului sau a Persoanei Împuternicite de Operator

Persoana împuternicită de operator și orice persoana care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucreză decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

## **8.5. Evidențele activităților de prelucrare**

**8.5.1.** Organizațiile care au mai puțin de 250 de angajați nu au obligația de a ține evidența prelucrării de date cu caracter personal, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum sunt prevăzute în legislația specifică.

**8.5.2.** În situația în care, operatorul va intra sub incidența prevederilor anterior menționate, acesta păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde următoarele informații:

- a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- b) scopurile prelucrării;
- c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existența unor garanții adecvate;
- f) acolo unde este posibil, termenele-limita preconizate pentru ștergerea diferitelor categorii de date;
- g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate adecvate;

**8.5.3.** Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

- a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează aceasta persoana (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

- b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
- c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existența unor garanții adecvate;
- d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate adecvate.

**8.5.4. Evidențele menționate anterior se formulează în scris, inclusiv în format electronic.**

**8.5.5.** Operatorul sau persoana împuternicită de acesta, precum și, sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia, cu notificarea prealabilă a Operatorului;

**8.6. Cooperarea cu Autoritatea de supraveghere**

Primăria comunei Metes, în calitate de Operator și persoana împuternicită de operator și, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

**8.7. Măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal**

**8.7.1. Aspecte generale privind securitatea prelucrării**

**8.7.1.1.** Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, *operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:*

- a) pseudonimizarea și criptarea datelor cu caracter personal;
- b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;
- c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- d) un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

**8.7.1.2.** La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

**8.7.1.3.** Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, menționate în legislația specifică, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute anterior.

**8.7.1.4.** Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care aceasta obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

### **8.7.2. Aspecte specifice privind securitatea prelucrării.**

La nivelul instituției, în calitate de Operator de date cu caracter personal, *masurile tehnice IT și organizatorice menționate în legislația specifică, necesare asigurării unui nivel adecvat de protecție sunt implementate prin:*

**- Identificarea, ca urmare a unor activități de audit de specialitate și implementarea/utilizarea în activitatea instituției a unor soluții tehnice IT adecvate, ținând cont de costurile implementării, natura, domeniul de aplicare, contextul, scopurile prelucrării și riscurile aferente, soluții care să acopere aspecte prevăzute de legislația specifică, precum:**

- ✓ Cerințe de securitate de bază: testarea securității sistemului, întărirea sistemului, codificarea securizată, protecția împotriva programelor malware;
- ✓ Politica privind parolele: autentificarea utilizatorului, autentificare cu doi factori;
- ✓ Managementul schimbării: separarea mediilor de testare, testarea schimbărilor, accesul dezvoltatorilor;
- ✓ Controlul accesului: controlul accesului bazat pe roluri, securitatea conturilor de utilizator, revizuirea privilegiilor, Audit logs, conturi neutilizate, privilegiile utilizatorilor tehnici, consola de securitate, informații despre utilizatori;
- ✓ Managementul evenimentelor: log format documentation, log information, log protection and monitoring, log format, evenimente auditate;
- ✓ Securitatea datelor: criptarea datelor, securitatea datelor în ciclul lor de viață;
- ✓ Back-up: back-up copies, programul de back-up, back-up security, verificarea back-up-urilor, viabilitatea back-up-urilor;
- ✓ Pseudominimizarea, minimizarea, integritatea datelor personale (computere, servere, terminale de acces, imprimarea datelor), disponibilitatea datelor, ștergerea și portabilitatea datelor, evidențele activităților de prelucrare etc.

- **Elaborarea/implementarea/monitorizarea permanentă a unor politici/proceduri specifice de protecție/securitate a datelor cu caracter personal.**

### **8.7.3. Cartografierea datelor cu caracter personal**

Cartografierea datelor se realizează de către persoana desemnata responsabila cu protectia datelor cu caracter personal la nivelul Primariei comunei Metesiar modificarea acestor date sau actualizează ori de câte ori intervin modificări cu privire la natura activităților desfășurate, structurii organizatorice, datele prelucrate, categoriile vizate, introducerea unor noi măsuri de securitate etc. Conducătorul locului de muncă este responsabil de corectitudinea și completitudinea informațiilor furnizate prin acest formular și implicit de asigurarea implementării măsurilor de securitate la nivelul biroului, inclusiv de urmărirea ducerii la îndeplinire a Planurilor de măsuri aferente biroului/structurii de conformare cu regulamentul 2016/679 și instruirea personalului din subordine cu privire la aplicarea legislație privind protecția datelor cu caracter personal. Formularul completat se păstrează în format electronic și fizic de către fiecare conducător al locului de muncă.

În cazul în care măsurile de securitate implementate nu sunt adecvate, în funcție de riscurile asupra protecției datelor din punctul de vedere al persoanelor vizate, Conducătorul locului de muncă împreună cu funcțiile responsabile de aplicarea măsurilor propune *Planuri de măsuri* de conformare. Pentru estimarea riscurilor se ia în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii.

### **8.7.4. Reguli gestionare baze de date din punct de vedere GDPR**

Se interzice realizarea de comunicări comerciale în scop de marketing direct (ex. Newslettere) către persoanele vizate care se regăsesc la nivelul CCICJ în diverse evidente, baze de date, aplicații IT, utilizând adrese de e-mail de tipul nume.prenume@gmail.com, nume.prenume@yahoo.com sau nume.prenume@societateaX.ro sau alte adrese care conțin date cu caracter personal ori numere de telefon personale (SMC) care se regăsesc în aceste evidente, în lipsa consimțământului expres, neechivoc, liber exprimat anterior dar și informat al persoanelor vizate și evidențiat distinct.

Comunicările comerciale în scop de marketing direct se vor putea realiza utilizând adrese de email de tipul nume.prenume@gmail.com, nume.prenume@yahoo.com sau nume.prenume@societateaX.ro sau alte adrese care conțin date cu caracter personal ori numere de telefon personale (SMC) care se regăsesc în evidențele, aplicațiile, bazele de date utilizate la nivelul instituției, numai în măsura în care:

- avem consimțământul expres neechivoc, liber exprimat anterior dar și informat al persoanelor vizate, și

- evidențele, aplicațiile, bazele de date utilizate vor fi adaptate în sensul evidențierii în mod distinct a consimțământului persoanelor vizate, pentru controlul efectiv al acestui proces dpdv GDPR, indiferent de modalitatea de obținere a acestuia.

Datele trebuie să fie adecvate, relevante și strict limitate la ce este absolut necesar pentru scopurile în care sunt necesare pentru prelucrarea asumată.

Fiecare conducător al compartimentului, cu suportul persoanei responsabile cu protecție a datelor va identifica și inventaria, menține în rețeaua organizației, inclusiv în stațiile de lucru individuale, doar bazele de date care sunt utile în mod efectiv pentru desfășurarea activității curente a organizației, precum și eliminarea acelor care nu mai au relevanță pentru activitatea instituției și/sau a expirat termenul de arhivare. Lista bazelor de date gestionate de fiecare birou va conține minim: denumirea bazei de date, locația de păstrare, responsabilul de gestionare (elaborare, modificare), persoanele cu drepturi de acces, perioada de păstrare, frecvența back-up-ului etc.

Fiecare conducător al compartimentului care gestionează baze de date în rețeaua organizației și pe stațiile de lucru individuale, va stabili reguli de acces controlat/restricționat (ex. Read only, write, execute, modify etc.) pentru utilizatorii acestor baze de date, revizuite în sensul celor de mai sus, pe bază de user și parola, la niveluri de acces (dacă este posibil).

Bazele de date trebuie grupate în foldere dedicate, atât a celor utilizate pentru activități comerciale/relații de afaceri cât și a bazei de date utilizată în scop de marketing direct pentru persoane fizice.

În rețeaua organizației conducătorii locurilor de muncă, cu suportul unui specialist IT, se vor menține doar documentele care conțin date cu caracter personal care sunt relevante, utile în mod efectiv pentru desfășurarea activității curente și eliminarea tuturor acelor care nu au relevanță, sau sunt documente personale.

Specialistul IT va realiza/asigura în permanență, conform programelor aprobate, salvarea bazelor de date cu caracter personal precum și a altor documente ce conțin date cu caracter personal în rețeaua organizației, prin copii de siguranță (backul), la intervalul stabilit.

## **8.8. Notificarea Autorității de Supraveghere în cazul încălcării securității datelor cu caracter personal**

**8.8.1.** În cazul în care are loc o încălcare a securității datelor cu caracter personal, instituția, prin Responsabilul de protecția datelor, notifică acest lucru Autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea

Autorității nu are loc în termen de 72 de ore, aceasta va fi însoțită de o explicație motivată a întârzierii în cauză.

**8.8.2.** Persoana împuternicită de operator înștiințează operatorul (informează Responsabilul cu protecția datelor al operatorului) fără întârzieri nejustificate după ce ia la cunoștință de o încălcare a securității datelor cu caracter personal.

**8.8.3.** Notificarea adresată Autorității cu privire la încălcarea securității datelor personale, conține cel puțin, următoarele elemente:

- a) descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- c) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- d) descrierea măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

**8.8.4.** Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

**8.8.5.** Operatorul, prin Responsabilul de protecția datelor, păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acestora și a măsurilor de remediere întreprinse. Aceasta documentație permite autorității de supraveghere să verifice conformitatea cu legislația specifică.

**8.8.6.** *Angajații au obligația de a informa de îndată șeful ierarhic și Responsabilul cu protecția datelor (Ex: se va utiliza adresa de e-mail oficială a instituției) în cazul identificării unei situații de încălcare a securității datelor cu caracter personal.*

*Responsabilul cu protecția datelor analizează informațiile comunicate, iar dacă este cazul, solicită entităților funcționale date și informații suplimentare.*

*În cazul în care situația de încălcare a securității datelor cu caracter personal este fundamentată rezonabil, Responsabilul cu protecția datelor întocmește Notificarea și solicită avizul avizul Directorului General sau Secretarului General și acordul Președintelui pentru a fi transmisă la Autoritatea de Supraveghere.*

*Notificarea se transmite către Autoritatea de Supraveghere pe suport de hârtie sau în format electronic, conform cerințelor stabilite de Autoritate.*

## **8.9. Informarea Persoanei vizate cu privire la încălcarea securității datelor cu caracter personal**

**8.9.1.** În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul, prin Responsabilul de protecția datelor, informează persoana vizată fără întârzieri nejustificate cu privire la aceasta încălcare.

**8.9.2.** În informarea transmisă persoanei vizate, prevăzută anterior, se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin următoarele informații și măsuri:

- numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- descrierea măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

**8.9.3.** Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

- a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
- b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;
- c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

## **CAP.9 EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI CONSULTAREA PREALABILĂ**

### **9.1. Evaluarea impactului asupra protecției datelor**

**9.1.1.** Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul, prin Responsabilul de protecția datelor, efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

**9.1.2.** Responsabilul cu protecția datelor elaborează, la solicitarea operatorului, în colaborare cu angajații instituției, evaluarea impactului asupra unui anumit tip de prelucrare de date cu caracter personal.

**9.1.3.** *Evaluarea impactului asupra protecției datelor se impune mai ales în cazul:*

a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni menționate în legislația specifică; sau

c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

**9.1.4.** *Autoritatea de supraveghere întocmește și publică o lista a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor.*

**9.1.5.** *Autoritatea de supraveghere poate, de asemenea, sa stabilească și sa pună la dispoziția publicului o lista a tipurilor de operațiuni de prelucrare pentru care nu este necesara o evaluare a impactului asupra protecției datelor.*

**9.1.6.** *Evaluarea conține cel puțin:*

a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate; și

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

9.1.7. La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate în legislația specifică, în special în vederea unei evaluări a impactului asupra protecției datelor.

9.1.8. *Operatorul, prin Responsabilul de protecția datelor, solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.*

9.1.10. Atunci când prelucrarea are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, prevederile anterioare nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înainte desfășurării activităților de prelucrare.

9.1.11. Acolo unde este necesar, operatorul, prin Responsabilul de protecția datelor, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

## **9.2. Consultarea prealabilă a Autorității de Supraveghere**

9.2.1. *Operatorul, prin Responsabilul de protecția datelor, consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.*

9.2.2. Atunci când consultă autoritatea de supraveghere, operatorul, prin Responsabilul de protecția datelor, îi furnizează acesteia:

- a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;
- b) scopurile și mijloacele prelucrării preconizate;
- c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;
- d) datele de contact ale specialistului de date personale ;

- e) evaluarea impactului asupra protecției datelor; și
- f) orice alte informații solicitate de autoritatea de supraveghere.

9.2.3. Dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

## **CAP.10 RESPONSABILUL DE PROTECȚIA DATELOR**

### **10.1. Alocarea responsabilităților/sarcinilor aferente Responsabilului de protecția datelor**

La nivelul instituției, sarcinile/responsabilitățile Responsabilului cu protecția datelor au fost alocate unei persoane care a participat la un curs de pregătire profesională;

**Responsabilitățile** alocate/stabilite prin Fisa de post sunt următoarele:

- Participă la procesul de tranziție către conformitatea cu Regulamentul privind Protecția Datelor cu Caracter Personal (GDPR);
- informează și consiliază reprezentanții sau persoane împuternicite de instituție, precum și angajații organizației care se ocupă de prelucrare datelor cu caracter personal privind obligațiile (naționale și europene) referitoare la prelucrarea datelor cu caracter personal, precum și cu privire la orice aspect legat de protecția datelor cu caracter personal;
- acordă consiliere și se implică în mod direct în efectuarea evaluărilor de impact asupra protecției datelor, monitorizează funcționarea acestora, inclusiv privind consultarea prealabilă a autorității de supraveghere, dacă este cazul;
- monitorizează respectarea prevederilor legale (naționale și europene) și ale reglementărilor interne referitoare la protecția datelor personale la nivelul Primăriei comunei Metes;
- monitorizează alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- participă la instruirea angajaților implicați în operațiunile de prelucrare a datelor personale;
- participă la activitatea de actualizare a evidenței operațiunilor de prelucrare a datelor personale și monitorizează corectitudinea acesteia;
- monitorizează, utilizând metoda eșantionului, modul în care persoanele ale căror date cu caracter personal se procesează, au fost informate de drepturile pe care le au;

- asigură asistența privind gestionarea prelucrării de date cu caracter personal, menținerea registrului de prelucrare a datelor personale precum și registrul privind incidentele de securitate și efectuează notificările privind încălcarea securității datelor personale;
- cooperează cu autoritatea de supraveghere (ANSPDCP) și acționează ca punct de contact în relația cu autoritatea de supraveghere, persoanele vizate, precum și în cadrul Primăriei, în legătură cu aspecte de prelucrare;

## **10.2. Responsabilitățile instituției față de Responsabilul de protecția datelor**

- Conducerea instituției și conducătorii entităților funcționale din cadrul Organizației vor acorda întregul sprijin Responsabilului de date personale, asigurându-i resursele necesare pentru executarea atribuțiilor sale, precum și pentru accesarea datelor cu caracter personal și a operațiunilor de prelucrare și pentru menținerea cunoștințelor sale de specialitate;
- Responsabilul cu protecția datelor își desfășoară activitatea în cadrul instituției. În desfășurarea activității, Responsabilul de protecția datelor nu va primi niciun fel de instrucțiuni în ceea ce privește îndeplinirea atribuțiilor sale în legătură cu GDPR.
- Persoanele vizate pot contacta și solicita asistența de specialitate din partea Responsabilului cu protecția datelor cu privire la toate aspectele legate de prelucrarea datelor și de exercitarea drepturilor lor.

## **CAP.11 TRANSFERURILE DE DATE CU CARACTER PERSONAL CATRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE**

**11.1. Orice decizie de a transfera date în afara spațiului UE și al Zonei Economice-Europene va fi supusă, anterior transferului și în timp util, analizei Responsabilului de protecția datelor.**

**Transferurile de date în afara spațiului UE și al Zonei Economice-Europene se pot face:**

- În temeiul unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție;
- În baza unor garanții adecvate oferite de instituție.

Garanțiile adecvate pot fi furnizate prin:

- a) un instrument obligatoriu dpdv juridic și executoriu între autoritățile sau organismele publice;
- b) reguli corporatiste obligatorii;
- c) clauze standard de protecție a datelor adoptate de Comisia Europeană;

d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisia Europeană;

e) un angajament obligatoriu și executoriu din partea instituției sau a persoanei împuternicite din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat, însoțit de un angajament obligatoriu și executoriu din partea instituției din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

**11.2. Sub rezerva autorizării din partea autorității de supraveghere, garanțiile adecvate pot fi furnizate, în special, prin:**

a) clauze contractuale între Primăria orașului Hațeg și operator, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau

b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

**11.3. În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer de date către o țara terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:**

a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transfer, după ce a fost informată asupra posibilelor riscuri pe care transferurile le pot implica pentru persoana vizată;

b) transferul este necesar pentru executarea unui contract între persoana vizată și instituție sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea sau pentru executarea unui contract încheiat în interesul persoanei vizate între instituție și o alta persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului UE sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat de public în general, sau de orice persoană care poate face dovada unui interes legitim.

**11.4. In lipsa unei decizii a Comisiei, a unor garanții adecvate dar și în lipsa condițiilor precizate anterior, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care:**

- transferul nu este repetitiv;
- se referă doar la un număr limitat de persoane vizate;
- este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și
- operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer.

## **CAP.12 CĂI DE ATAC, RĂSPUNDERI, MĂSURI ȘI SANCTIUNI SPECIFICE**

### **12.1. Dreptul de a depune o plângere la o autoritate de supraveghere**

**12.1.1.** Fără a aduce atingere oricăror alte cai de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul sau de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încălca prezentul regulament.

**12.1.2.** Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul legislației specifice.

### **12.2. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere**

**12.2.1.** Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

**12.2.2.** Fără a aduce atingere oricăror alte cai de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă 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.

**12.2.3.** Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.

**12.2.4.** În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a Comitetului european pentru protecția datelor în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

### **12.3. Dreptul la o cale de atac eficientă împotriva unui operator sau a unei persoane împuternicite de operator**

**12.3.1.** Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă 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.

**12.3.2.** Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu. Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competențelor sale publice.

### **12.4. Dreptul la despăgubiri și răspunderea operatorului sau a persoanei împuternicite de operator**

**12.4.1.** Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a legislației specifice are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

**12.4.2.** Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prevederile legislației specifice. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din legislația specifică care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale/contractuale ale operatorului.

**12.4.3.** Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

### **12.5. Condiții generale pentru impunerea amenzilor administrative**

**12.5.1.** Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislației specifice este, în fiecare caz, eficace, proporțională și disuasivă.

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

*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 în legătură promovarea căii de atac, precum și, dacă este cazul, va elabora contestația, urmând să analizeze cel puțin următoarele aspecte:*

- a) 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;
- b) dacă încălcarea a fost comisă intenționat sau din neglijență;
- c) orice acțiuni 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 ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia;
- 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 și a atenua posibilele efecte negative ale încălcării;
- g) categoriile de date cu caracter personal afectate de încălcare;
- h) 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;
- i) în cazul în care măsurile menționate de legislația specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;
- j) aderarea la coduri de conduită sau la mecanisme de certificare aprobate; și
- k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

Responsabilul de date personale va reprezenta operatorul în cadrul procedurii administrative în fața autorității cât și în situația în care se va contesta decizia autorității în fața instanțelor judecătorești.

**12.5.3.** Neconformarea față de prevederile GDPR poate atrage aplicarea de amenzi administrative cuprinse între 10.000.000 EUR și 20.000.000 EUR sau între 2% și 4% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul valoarea cea mai mare.

## **CAP.13 RESPONSABILITĂȚI ÎN CADRUL PRIMĂRIEI COMUNEI METES**

**13.1.** Cunoașterea și aplicarea corespunzătoare a prezentului Regulament reprezintă obligația întregului personal al instituției, potrivit limitelor de autoritate aprobate;

**13.2.** Responsabilitățile privind protecția datelor cu caracter personal revin gradual întregului personal;

**13.3.** Responsabilitățile în ceea ce privește elaborarea, avizarea, aprobarea, implementarea, supravegherea și evaluarea aplicabilității prezentului Regulament, precum și dispunerea măsurilor care se impun revin, după cum urmează:

### **13.3.1. Primăria comunei Metes (cu toate structurile organizatorice), în calitate de Operator:**

- a) asigură implementarea legislației comunitare-UE și naționale privind protecția datelor cu caracter personal la nivelul instituției, prin prezentul regulament sau alte acte interne ;
- b) asigură conformarea tuturor activităților de prelucrare cu prevederile legislației comunitare-UE și naționale privind protecția datelor cu caracter personal;
- c) asigură informarea persoanelor vizate și respectă drepturile acestora;
- d) ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;
- e) asigură respectarea prezentului regulament privind măsurile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal.

### **13.3.2. Primarul comunei Metes**

- a) aprobă Regulamentul privind prelucrarea datelor cu caracter personal, prin dispoziție;
- b) aprobă prin acte de reglementare internă/acte decizionale măsuri de implementare a prevederilor legale incidente și ale Regulamentului privind prelucrarea datelor cu caracter personal;
- c) asigură prin instrumentele de control și/sau audit intern/extern evaluarea proceselor aferente prezentului Regulament și aplicarea legislației în domeniul protecției datelor;

d) aprobă modificări ale prezentului Regulament, în situația în care schimbările legislative impun acest lucru în regim de urgență.

**13.3.4. Organele de Conducere ale instituției și conducătorii structurilor sale organizatorice -compartimente sunt responsabili cu protecția datelor cu caracter personal pentru activitățile coordonate**

**13.3.5. Utilizatorii, respectiv angajații** care prelucrează date cu caracter personal au următoarele responsabilități specifice:

- a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentului regulament;
- b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, 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, condițiile în care pot fi exercitate aceste drepturi etc.;
- c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin șefilor ierarhici, organelor de conducere, pentru realizarea activităților specifice ale acestora;
- d) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
- e) să respecte măsurile de securitate, precum și celelalte reguli stabilite;
- f) să informeze de îndată seful ierarhic și Responsabilul de protecția datelor despre împrejurări de natura a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință.

**13.3.6. Derulatorii de contracte**

- a) au responsabilitatea/obligativitatea inserării în contractele încheiate și gestionate de către aceștia a clauzelor specifice (elaborate de/împreună cu Responsabilul de protecția datelor, cu titlu general) cu privire la protecția datelor cu caracter personal și/sau cu privire la respectarea Condițiilor Generale, Tehnice și de Participare;
- b) în situațiile în care sunt prelucrate date cu caracter personal în numele instituției de către persoane împuternicite (procesatori de date-ex: instituții de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariați, companii de curierat etc.) derulatorii de contract vor avea responsabilitatea/obligativitatea de

încheia cu fiecare dintre aceste persoane împuternicite Acorduri de prelucrare a datelor cu caracter personal, care vor avea în conținut elementele prevăzute în prezentul Regulament și legislația specifică, stabilite în prealabil de Responsabilul de protecția datelor și aprobate de conducere.

e) în situația prelucrării datelor personale în scop de marketing direct, derulatorii de contract, precum și salariații responsabili de operațiunile de marketing direct (inclusiv serviciile aferente IT) vor avea în vedere în mod obligatoriu consimțământul exprimat anterior prelucrării de către persoana vizată, pentru evitarea unor situații de neconformare față de prevederile legale privind protecția datelor personale.

**13.3.7. Responsabilul de protecția datelor** responsabil cu elaborarea Regulamentului și controlul procesului, incluzând: monitorizarea și controlul aplicării unitare a Regulamentului, testarea conformității, audituri de specialitate și informarea conducerii; participă la organizarea și administrarea programelor de pregătire continuă a angajaților în domeniul cunoașterii prevederilor GDPR; responsabilitățile acestuia sunt menționate în prezentul regulament și în Fișa de post.

## **CAP.14 ANGAJAMENTUL DE CONFORMARE A ANGAJAȚILOR FAȚĂ DE LEGISLAȚIA SPECIFICĂ ȘI REGULAMENTUL PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL**

14.1. La angajare, înainte de începerea activităților de prelucrare a datelor cu caracter personal, dar și ulterior, cu ocazia derulării raporturilor de muncă, organizării de instruiți profesionale specifice, toți angajații care prelucrează date cu caracter personal trebuie să semneze un *Angajament individual de conformare* față de legislația specifică și a prezentului Regulament privind protecția datelor cu caracter personal.

## **CAP. 15 TRAINING**

15.1. Planurile anuale de pregătire continuă, elaborate în condițiile legii, 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.

15.2. Periodic, conducătorii structurilor funcționale din cadrul instituției organizează cu sprijinul Responsabilului de protecția datelor instruiți cu utilizatorii/angajații pentru cunoașterea procedurilor specifice de lucru instituite la nivelul instituției și cu privire la

riscurile generate de vulnerabilități și amenințări informatice la adresa datelor cu caracter personal prelucrate.

15.3. Instruirile se efectuează periodic și în mod obligatoriu la modificarea cadrului legal în materie, iar prelucrarea incidentelor se va realiza cu întregul personal implicat în activitatea de prelucrare a datelor cu caracter personal.

## **CAP.16 DISPOZIȚII FINALE**

16.1. Nerespectarea prevederilor prezentului Regulament reprezintă un risc major de conformare care poate atrage pentru Primăria comunei Metes sancțiuni din partea organelor de reglementare/supraveghere competente, în condițiile legii.

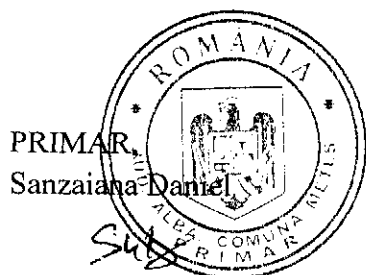
16.2. Prezentul Regulament reprezintă proprietatea intelectuală a instituției și intră sub incidența Legii nr. 8/1996 privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare.

16.3. Prezentul Regulament are caracter „Uz intern”, difuzarea acestuia neautorizată de către salariați către terțe persoane intră sub incidența *Angajamentului de conformare* și se sancționează conform legislației în vigoare.

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

16.5. Prezentul regulament completează: regulamentele, procedurile interne, diagramele flux, precum și orice alte acte de reglementare internă.

16.6. Dacă ulterior datei intrării în vigoare a prezentei reglementări, o prevedere legală modifică/completează/abrogă prevederi ale prezentului regulament, se vor aplica prevederile legale în vigoare.



Contrasemneaza pentru legalitate-Secretar general,

Mar Elena

