

PRIMARIA COMUNEI RADOVAN

JUDETUL DOLJ

POLITICA DE SECURITATE A PRELUCRARIII DATELOR CU CARACTER PERSONAL

1. OBIECTIV:

Obiectivul acestei politici este de a stabili masurile necesare si responsabilitatile angajatilor PRIMARIEI RADOVAN, pentru îndeplinirea obligațiilor referitoare la garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal.

2. DOMENIUL DE APLICARE :

Prezenta politica se aplica tuturor angajatilor PRIMARIEI RADOVAN cu atributii de prelucrare a datelor cu caracter personal si/sau dupa caz persoanelor imputernicite.

3. TERMENI ȘI DEFINIȚII:

ANSPDCP: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

Date cu caracter personal: orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale ale acelei persoane; ;

Date anonime: date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

Operator: orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul 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 aceluși act normativ; dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Stocarea : păstrarea pe orice fel de suport a datelor cu caracter personal culese;

Utilizator: 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.

Persoana responsabilă de politica de securitate a datelor cu caracter personal(DPO): persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

Prelucrarea datelor cu caracter personal: orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea ,

Restricționarea prelucrării înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

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 află persoana fizică respectivă sau deplasările acesteia;

Persoană împuternicită de operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

Destinatar înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță;

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;

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

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;

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;

4. DOCUMENTE DE REFERINȚĂ:

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului .

5. PRECIZĂRI:

5.1. REGULI GENERALE

PRIMARIA RADOVAN a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat.

În acest sens au fost desemnate, la nivelul PRIMARIA RADOVAN, persoane responsabile cu respectarea dispozițiilor **Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului**.

PRIMARIA RADOVAN a luat măsuri de stocare în siguranță a informațiilor privind date cu caracter personal, astfel încât să fie asigurat un nivel adecvat de protecție și securitate, în sensul **Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului**.

Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor, societatea a elaborat și implementat măsuri organizatorice și tehnice orientate pe anumite direcții de acțiune:

- Identificarea și autentificarea utilizatorului
- Tipul de acces
- Colectarea datelor
- Computerele și terminalele de acces
- Fișierele de acces
- Instruirea personalului

5.2. PROCEDURI SPECIFICE

5.2.1. Identificarea și autentificarea utilizatorului

Pentru a căpăta acces la date cu caracter personal, utilizatorii trebuie să se autentifice în sistemele informatice ale PRIMARIA RADOVAN .

Autentificarea în cadrul sistemelor informatice ale PRIMARIA RADOVAN se face prin introducerea credențialelor de autentificare unice și netransmisibile dobândite în urma procesului de înrolare și management al identității electronice, guvernate de politicile de securitate în vigoare.

Fiecare utilizator are propriul său cod de identificare (nume de utilizator).

Niciodată nu este alocat același cod de identificare mai multor utilizatori și acesta nu poate fi partajat de către mai multe persoane.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată sunt dezactivate și distruse după un control prealabil. Perioada după care codurile trebuie dezactivate și distruse este stabilită prin politica PRIMARIEI RADOVAN.

Orice cont de utilizator este însoțit de o modalitate de autentificare, prin introducerea unei chei de autentificare precum o parolă. Parolele sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție. La introducerea parolelor acestea nu sunt afișate în clar pe monitor. Parolele sunt schimbate periodic conform politicilor de securitatea ale PRIMARIEI RADOVAN.

Schimbarea periodică a parolelor se face numai de către utilizatori autorizați. Sistemul informațional blochează automat accesul unui utilizator după un număr fix de introduceri greșite ale cheii de autentificare.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare este obligat prin fișa postului să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului. Este stabilită o procedură proprie de administrare și gestionare a conturilor de utilizator.

Sunt autorizați anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile permise sau dacă va absenta o perioadă îndelungată stabilită de entitate.

5.2.2. Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu.

Pentru aceasta trebuie să fie stabilite tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea incidentelor și a problemelor aparute în utilizarea sistemelor informatice.

5.2.3. Colectarea datelor

PRIMARIA RADOVAN desemnează utilizatori autorizați pentru operațiile de colectare și introducere de date cu caracter personal în sistemele informaționale.

Orice modificare a datelor cu caracter personal trebuie sa se poate face numai de către utilizatori autorizați desemnați.

PRIMARIA RADOVAN va lua măsuri pentru ca sistemele informaționale să înregistreze cine a făcut modificarea datelor cu caracter personal, data și ora modificării.

Pentru o mai bună administrare, vor fi implementate măsuri pentru ca sistemele informaționale să mențină datele șterse sau modificate.

5.2.4. Computerele și terminalele de acces

Computerele și alte terminale de acces la date cu caracter personal aflate în sediul PRIMARIA RADOVAN punctele de lucru , vor fi instalate în încăperi cu acces restricționat

Unde nu pot fi asigurate aceste condiții, computerele vor fi instalate în încăperi care se pot încuia.

Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilita de către PRIMARIA RADOVAN , sesiunea de lucru se va închide automat.

Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate. Serverele care găzduiesc date cu caracter personal pot fi accesate doar în mod controlat, pe baza de drepturi de acces.

Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD) care contin date cu caracter personal, decât cu aprobare prealabilă din partea conducerii societății.

5.2.5. Fișierele de acces :

PRIMARIA RADOVAN ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată . Pentru prelucrările automate, aceste informații sunt stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

PRIMARIA RADOVAN păstrează fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.

Fișierele de acces fac posibilă identificarea de către PRIMARIA RADOVAN sau de către persoana împuternicită, a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

5.2.6. Instruirea personalului

Personalul PRIMARIA RADOVAN este informat cu privire la prevederile **Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului** pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor

de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal.

Utilizatorii care au acces la date cu caracter personal vor fi instruiți asupra confidențialității acestora (angajamentele de confidentialitate) și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.

5.2.7. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) trebuie luate măsuri privind:

- interzicerea folosirii de către utilizatori a programelor software care provin din surse neverificate;
- informarea utilizatorilor în privința pericolului privind virusii informatici;
- implementarea unor sisteme automate de tip antivirus și protective malware și de securitate a sistemelor informațice;
- dezactivarea posibilității de copiere sau imprimare a datelor cu caracter personal afisate pe ecran în afara fluxurilor normale de lucru.

5.2.8. Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați de către PRIMARIA RADOVAN pentru această operațiune.

5.2.9. Prelucrarea manuala de date cu caracter personal

Documentele care conțin date cu caracter personal vor fi ținute în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare. 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.

5.3. PRELUCRAREA DATELOR CU CARACTER PERSONAL AVÂND O FUNCȚIE DE IDENTIFICARE DE APLICABILITATE GENERALĂ, inclusiv dezvăluirea acestora către terți, se face numai în următoarele condiții:

a) persoana vizată și-a dat în mod expres consimțământul;

sau

b) prelucrarea este prevăzută în mod expres de o dispoziție legală;

sau

c) în alte cazuri, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

PRIMARIA RADOVAN respectă principiul caracterului adecvat, pertinent și neexcesiv, precum și măsurile de confidențialitate și de securitate a prelucrărilor.

În cazul prevăzut la punctul c) de mai sus, se au în vedere următoarele aspecte:

- scopul prelucrării să fie determinat, explicit și legitim;
- stabilirea și aplicarea unor măsuri prin care să se asigure exercitarea drepturilor persoanelor vizate;
- durata de stocare a datelor să fie pe perioada strict necesară îndeplinirii scopului, după care datele vor fi șterse sau distruse, după caz;
- stabilirea modalităților de acces la sistemele de evidență în vederea colectării datelor, în funcție de care se vor stabili și respecta măsuri tehnice și organizatorice adecvate pentru protejarea datelor;
- utilizarea datelor numai în limitele scopului stabilit;

5.4. DREPTURILE PERSOANELOR ALE CĂROR DATE PERSONALE SUNT COLECTATE ȘI/ SAU PRELUCRATE

5.4.1. Dreptul de a fi informat

În cazul în care datele cu caracter personal sunt obținute direct de la persoana vizată, PRIMARIA RADOVAN este obligat să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care această persoană posedă deja informațiile respective:

- a) scopul în care se face prelucrarea datelor;
- b) existența drepturilor prevăzute de lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;
- c) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

Înainte de completarea datelor cu caracter personal se solicita consimțământul persoanelor vizate, pentru prelucrarea acestora;

Numărul de înregistrare a notificării comunicat de Autoritatea Națională de supraveghere se menționează în orice document prin care se colectează, stochează sau dezvăluie date cu caracter personal;

Datele de contact ale DPO-Responsabil cu protecția datelor cu caracter personal.

Clădirile care sunt supravegheate video vor avea, la intrare, afișat în loc vizibil, informarea privind preluarea și stocarea de imagini.

5.4.2. Dreptul de acces la date

Orice persoană vizată are dreptul de a obține de la PRIMARIA RADOVAN (în calitate de operator), la cerere și în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc, sunt sau nu sunt prelucrate de acesta.

5.4.3. Dreptul de intervenție asupra datelor

Orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte;

b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă legii.

5.4.4. Dreptul de opoziție

Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca datele care o vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale contrare.

În caz de opoziție justificată prelucrarea nu mai poate viza datele în cauză.

5.4.5. Dreptul de a se adresa justiției

(1) Fără a se aduce atingere posibilității de a se adresa cu plângere autorității de supraveghere, persoanele vizate au dreptul de a se adresa justiției pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate.

(2) Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanței competente pentru repararea acestuia.

5.5. COMUNICAREA DATELOR CU CARACTER PERSONAL

(1) Datele cu caracter personal se pot comunica între PRIMARIA RADOVAN și împuterniciții acestuia sau între / sau PRIMARIA RADOVAN și împuterniciți ai acestuia și alte instituții ori organisme publice sau entități de drept public sau privat în una dintre următoarele situații:

- a) dacă persoana vizată și-a dat consimțământul expres și neechivoc pentru comunicarea datelor sale;
- b) fără consimțământul persoanei vizate în cazurile prevăzute de lege.

(2) Comunicarea datelor cu caracter personal se poate face și on-line, cu respectarea dispozițiilor alin.

(1) și asigurarea securității sistemelor de comunicații a datelor cu caracter personal.

(3) Datele cu caracter personal asupra cărora persoanele vizate au exercitat și li s-a recunoscut dreptul de opoziție nu pot face obiectul prelucrării.

(4) Cererile pentru comunicarea datelor cu caracter personal adresate PRIMARIA RADOVAN, trebuie să conțină datele de identificare a solicitantului, precum și motivarea și scopul cererii, conform prevederilor legale.

(5) Cererile care nu conțin aceste elemente se restituie pentru completare, iar cele care nu se încadrează în condițiile prevăzute de lege se resping, menționându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.

(6) Înainte de comunicarea datelor cu caracter personal, PRIMARIA RADOVAN verifică dacă acestea sunt exacte și, dacă este cazul, actualizate.

(7) În situația în care se constată că au fost transmise date incorecte sau neactualizate PRIMARIA RADOVAN, are obligația de a informa destinatarul respectivelor date asupra neconformității acestora, cu menționarea datelor care au fost modificate.

(8) La comunicarea datelor cu caracter personal PRIMARIA RADOVAN atenționează destinatarul asupra interdicției de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

6. CONFIDENȚIALITATEA PROCESĂRII

Datele personale sunt considerate informații confidențiale și vor fi tratate ca atare. Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajați este interzisă. Prelucrarea datelor cu caracter personal este confidențială. Ea va fi efectuată numai de persoanele care acționează sub autoritatea operatorului și numai pe baza instrucțiunilor acestuia. Orice procesare de date efectuată de un angajat, care nu a fost autorizată să fie desfășurată ca parte a îndatoririlor sale legitime, este considerată ca fiind neautorizată. Se aplică principiul "necesitatea de a cunoaște". Angajații pot avea acces la informații personale în funcție de adecvarea acestui acces la tipurile de date și de scopul determinat. Acest lucru se bazează pe defalcarea și separarea atentă a atribuțiilor angajaților operatorului și presupune punerea în aplicare a rolurilor și responsabilităților pentru fiecare angajat. Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod. Superiorii ierarhici își informează angajații la începutul relației de muncă cu privire la obligația de a proteja secretul datelor. În

cazul utilizării neautorizate a datelor personale, angajații pot fi sancționați în conformitate cu legislația aplicabilă și cu reglementările în vigoare în cadrul operatorului. Obligația menținerii confidențialității datelor personale rămâne în vigoare și după încheierea perioadei de angajare, sancțiunile aplicabile în caz de încălcare a obligației de confidențialitate fiind cele prevăzute de cadrul legislativ în vigoare.

7. SECURITATEA PRELUCRĂRII

Datele personale sunt protejate împotriva accesului neautorizat și împotriva prelucrării sau divulgării ilegale, precum și pierderii accidentale, modificării sau distrugerii. Acest lucru se aplică indiferent dacă datele sunt prelucrate electronic, pe suport de hârtie sau prin alte mijloace. Înainte de introducerea noilor metode de prelucrare a datelor, în special a noilor sisteme informatice, sunt definite și implementate măsuri tehnice și organizatorice de protecție a datelor cu caracter personal. Aceste măsuri trebuie să se bazeze pe stadiul tehnicii, pe riscurile procesării și pe necesitatea de a proteja datele (determinate de procesul de clasificare a informațiilor). În special, structura organizatorică responsabilă se poate consulta cu Ofițerul de Securitate a Informației și cu DPO. Măsurile tehnice și organizatorice pentru protecția datelor personale fac parte din managementul securității informațiilor și sunt adaptate în mod continuu la evoluțiile tehnice și schimbările organizaționale. Accesul la datele cu caracter personal este oferit numai acelor angajați ai operatorului care au nevoie de astfel de date cu caracter personal pentru a-și îndeplini sarcinile legate de oricare dintre scopurile prelucrării menționate mai sus (inclusiv departamentul resurse umane, departamentul Juridic, departamentul Financiar, IT, Administrativ). Orice acces la datele cu caracter personal pentru alți angajați care nu au drepturi de accesare în conformitate cu prezenta Politică este interzis. Angajații operatorului care au acces la datele cu caracter personal au dreptul să prelucreze numai acele date de care au nevoie pentru a-și îndeplini responsabilitățile specifice de muncă legate de oricare dintre scopurile de prelucrare menționate mai sus. Documentele care conțin date cu caracter personal sunt stocate în departamentele structurale ale operatorului ai căror angajați au acces la datele cu caracter personal legat de îndeplinirea atribuțiilor lor oficiale și sunt responsabili de interacțiunea datelor relevante ale persoanei vizate. O persoană care prelucrează date cu caracter personal în numele operatorului respectă principiile și regulile de prelucrare a datelor cu caracter personal stabilite prin prezenta Politică. Dacă operatorul autorizează o altă persoană cu prelucrarea datelor cu caracter personal, operatorul este responsabilă față de persoana vizată de prelucrarea datelor cu caracter personal pentru faptele sau omisiunile acelei persoane. O persoană care prelucrează date cu caracter personal în numele operatorului este responsabilă față de acesta.

Toate datele cu caracter personal trebuie să fie tratate cu cea mai înaltă securitate și trebuie păstrate:

- într-o cameră închisă cu cheia cu acces controlat; și/sau
- într-un sertar sau dulap închis cu cheia; și/sau
- dacă sunt computerizate, parola protejată conform cerințelor din politica de control al accesului; și/sau
- stocate în medii de calculator (detașabile) care sunt criptate în conformitate standardele în domeniu;

8. CONTROLUL PROTECTIEI DATELOR

Respectarea politicii de protecție a datelor și a legilor aplicabile privind protecția datelor este verificată în mod regulat prin intermediul auditurilor de protecție a datelor precum și al altor controale. Realizarea acestor controale este responsabilitatea DPO. Rezultatele controalelor privind protecția datelor sunt raportate managementului organizației.

La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția autorității responsabile de protecția datelor.

Autoritatea responsabilă cu protecția datelor poate efectua propriile controale de conformitate cu reglementările din această politică, conform legislației naționale.

9. REȚINEREA ȘI ELIMINAREA DATELOR

Operatorul nu va păstra datele personale într-o formă care permite identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar, în legătură cu scopurile pentru care datele au fost colectate inițial. Operatorul poate stoca datele perioade mai lungi conform termenelor imperative de prescripție aplicabile și cu implementarea unor măsuri tehnice și organizaționale adecvate pentru a proteja drepturile și libertățile Persoanelor vizate. Datele personale trebuie să fie eliminate în siguranță în conformitate cu al șaselea principiu al GDPR – prelucrate într-un mod adecvat pentru a menține securitatea, cu protejarea „drepturilor și libertăților” persoanelor vizate. Orice eliminare a datelor va fi efectuată în conformitate cu procedura de eliminare sigură.

10. INCIDENTE DE PROTECȚIE A DATELOR

Toți angajații sunt obligați să informeze imediat superiorul sau DPO cu privire la cazurile de încălcare a acestei politici de protecție a datelor sau alte reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor), indiferent dacă este vorba despre o încălcare a confidențialității, a integrității datelor sau a disponibilității acestora.

Conducătorul structurii organizatorice este obligat să informeze imediat DPO cu privire la incidentele de protecție a datelor.

În cazurile de:

- Transmitere necorespunzătoare a datelor cu caracter personal către terțe părți,
- Acces neadecvat la datele cu caracter personal sau
- Pierdere, distrugere sau alterare a datelor cu caracter personal,

conducătorul structurii organizaționale în cauza întocmește, de urgență, rapoartele de sesizare, conform regulilor de stabilite pentru Gestionarea Incidentelor de Securitate a Informațiilor, astfel încât să poată fi luate măsurile urgente pentru limitarea afectării titularilor de date cu caracter personal și pentru respectarea obligațiilor de raportare și notificare a incidentelor către autoritatea de supraveghere.

11. RESPONSABILITĂȚI ȘI SANCTIUNI

Conducerea operatorului precum și angajații și prepușii acestora sunt responsabili de prelucrarea datelor în zona lor de responsabilitate. Prin urmare, acestia sunt obligați să se asigure că sunt îndeplinite cerințele legale pentru protecția datelor și cele conținute în politica de protecție a datelor (de exemplu, obligațiile naționale de raportare). Organele de conducere au responsabilitatea de a se asigura că există măsuri organizaționale, resurse umane și tehnice pentru ca orice prelucrare a datelor să fie efectuată în

conformitate cu protecția datelor. Respectarea acestor cerințe reprezintă responsabilitatea conducătorilor de structuri organizatorice. DPO este informat de îndată despre controalele efectuate de autoritățile de supraveghere cu privire la protecția a datelor.

DPO poate efectua verificări și familiarizează angajații operatorului cu conținutul politicilor de protecție a datelor. Pentru planurile de prelucrare a datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, DPO este informat înainte de începerea procesării. Acest lucru se aplică în mod obligatoriu datelor cu caracter personal sensibile. Managerul organizației se asigură că angajații sunt suficient de instruiți în protecția datelor. Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor pot conduce la cereri de despăgubire pentru prejudicii. Încălțările pentru care angajații individuali sunt responsabili pot conduce la sancțiuni prevăzute în dreptul muncii.

12. OFIȚERUL DE PROTECȚIA DATELOR (DPO)

Ofiterul de Protecția Datelor (DPO) fiind independent din punct de vedere al ordinilor profesionale, își desfășoară activitatea pentru respectarea legislației în vigoare privind protecția datelor. El este responsabil pentru politica de protecție a datelor și supraveghează respectarea acesteia. Ofiterul de Protecția Datelor are linie de raportare directă către managerul organizației.

Orice persoană vizată poate aborda DPO, în orice moment, să ridice preocupări, să pună întrebări, să solicite informații sau să depună plângeri legate de protecția datelor sau de problemele de securitate a datelor. Dacă se solicită, preocupările și plângerile vor fi tratate în mod confidential.

Deciziile luate de Ofiterul de Protecția Datelor (DPO) pentru remedierea încălcărilor privind protecția datelor trebuie să fie susținute de conducerea organizației. Anchetele autorităților de supraveghere sunt întotdeauna raportate DPO.

Datele de contact ale DPO sunt următoarele:

Telefon 0251/359223; e-mail doljprimariaradovan@gmail.com

13. RELATIA CU ANSPDCP

Persoanele vizate, din orice categorie ar face ele, pot sesiza sau face reclamații referitoare la situații de încălcare a cerințelor Regulamentului nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) adresate Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal care are sediul în București, str. General Gheorghe Magheru nr. 28-30, sector 1 și poate fi contactată la telefon 0318059211 sau adresa de mail anspdcp@dataprotection.ro.

14. DISPOZIȚII FINALE

Pentru mai multe informații, orice persoană se poate adresa PRIMARIA RADOVAN la telefon 0251/359223; e-mail doljprimariaradovan@gmail.com