



ROMÂNIA
CONSILIUL LOCAL AL MUNICIPIULUI TIMIȘOARA
DIRECȚIA GENERALĂ A POLIȚIEI LOCALE
Număr operator de date cu caracter personal: 5082
Str. Avram Imbroane, nr. 54, 300129 Timișoara; C.I.F. 27872311
Tel.: +40-256-306822; Fax : 0256-306.819
E-mail : contact@politialoctm.ro ; Web : www.polcomtim.ro



Nr. 7118/31.05.2023

APROB
DIRECTOR GENERAL
HAJDU APTILA

POLITICA PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL LA NIVELUL DIRECȚIEI GENERALE A POLIȚIEI LOCALE TIMIȘOARA

Poliția locală s-a înființat în scopul exercitării atribuțiilor privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea și descoperirea infracțiunilor, în următoarele domenii:

- a) ordinea și liniștea publică, precum și paza bunurilor;
- b) circulația pe drumurile publice;
- c) disciplina în construcții și afișajul stradal;
- d) protecția mediului;
- e) activitatea comercială;
- f) evidența persoanelor;
- g) alte domenii stabilite prin lege.

În scopul îndeplinirii atribuțiilor sale, Poliția Locală prelucrează date cu caracter personal în activitățile de: prevenire, constatare și sancționare a contravențiilor, menținere și asigurare a ordinii publice, ținere evidență cu persoanele care săvârșesc contravenții, gestionare resurse umane, gestionare resurse economico – financiare și administrative.

Datele cu caracter personal pot fi obținute în mod direct de la persoane fizice în diferite moduri, incluzând următoarele modalități: contact direct, în cadrul întâlnirilor de la sediul instituției, telefonic, primirea de date pe email/fax, trimiterea de cereri, petiții și completarea unor documente necesare furnizării serviciilor, completarea unor formulare online, vizitarea sediului sau depunere de dosare pentru angajarea pe posturile vacante din cadrul instituției;

De asemenea, datele cu caracter personal pot fi obținute indirect, din alte surse: prin dezvăluiri făcute de alte instituții (transfer de date), dezvăluiri efectuate într-un interes legitim, prin interogarea bazelor de date naționale, dezvăluiri ale altei persoane vizate.

Prelucrarea datelor cu caracter personal 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.

Poliția Locală Timișoara prelucrează date cu caracter personal, prin mijloace automatizate/manuale pentru următoarele scopuri:

- relații publice/petiționare;
- resurse umane;
- creșterea siguranței și prevenirea criminalității în municipiul Timișoara
- controlul activ al parcului auto, reducerea uzurii, reducerea consumului de combustibil, verificarea și optimizarea rutelor vehiculelor, generarea de rapoarte în timp real pentru toate componentele parcului auto precum și dirijarea de către dispecerul de serviciu a celui mai apropiat echipaj la intervenție
- prevenire, constatare și sancționare a contravențiilor;
- menținere și asigurare a ordinii și liniștii publice;
- formulare de acțiuni și reprezentare în instanță;
- organizare/derulare evenimente;
- îndeplinirea atribuțiilor legale de control;
- gestiunea financiar-contabilă;
- gestiunea logistico-administrativă;
- achiziții publice;
- verificări pe linie de fenomene epidemiologice;
- triajul persoanelor pentru accesul în clădirea instituției

În raport cu scopurile de mai sus, Poliția Locală Timișoara prelucrează următoarele categorii de date cu caracter personal:

- Numele și prenumele
- Numele și prenumele membrilor de familie
- Sexul
- Data și locul nașterii
- Cetățenia
- Caracteristici fizice/antropometrice
- Telefon/fax
- Adresă domiciliu/reședință
- E-mail
- Funcție/Profesie
- Loc de muncă
- Denumirea angajatorului
- Imagine
- Calitatea deținută în societăți comerciale (asociat, administrator)
- Cod unic de înregistrare
- Voce
- Semnătura
- Date privind formarea profesională – diplome – studii
- Date privind starea de sănătate

- Date privind infracțiuni, condamnări penale, cazier,
- Date privind originea etnică
- Date privind apartenența la sindicate
- Date privind sancțiuni disciplinare/administrative
- Date privind sancțiuni contravenționale
- CNP – codul numeric personal
- Seria și numărul actului de identitate
- Seria și numărul pașaportului/permisului de conducere
- Date din certificatul de înmatriculare
- Marca, modelul autoturismului și numărul de înmatriculare
- Date privind bunuri pierdute

Direcția Generală a Poliției Locale Timișoara își rezervă dreptul de a solicita alte date necesare pentru îndeplinirea atribuțiilor, strict în conformitate cu prevederile legale.

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

Informațiile înregistrate sunt destinate utilizării de către operator/împuternicit al operatorului și sunt comunicate numai următorilor destinatari: operatorului, persoanei vizate/reprezentanților legali ai acesteia, autorități publice de aplicare a legii, autorități de colactare a debitelor/ recuperare creanțe, autoritatea judecătorească, organe de urmărire penală și alte instituții abilitate de lege să solicite informații.

Perioada de stocare a datelor cu caracter personal – ca regulă generală datele cu caracter personal sunt stocate doar pentru perioada necesară atingerii scopului pentru care sunt colectate putând fi stabilite termene maxime de păstrare prin acte normative, regulamente, dispoziții interioare.

În ceea ce privește datele din evidențele letrice perioada de stocare este conform Nomenclatorului Arhivistic.

Întreg personalul Direcției Poliția Locală Timișoara care prelucrează date cu caracter personal va semna un acord de confidențialitate cu privire la prelucrarea acestui tip de date.

În cadrul procesului de recrutare/selecție de personal, Serviciul Resurse Umane va solicita acordarea consimțământului de către candidat 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 Direcției Generale a Poliției Locale Timișoara, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de Informare se vor păstra în evidențele Serviciului de Resurse Umane.

În cazul procesului de recrutare/selecție de personal se procedează la pseudonimizarea datelor cu caracter personal prin atribuirea unui cod unic de identificare a candidaților.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate de către Direcția Generală a Poliției Locale Timișoara.

Informațiile înregistrate sunt destinate utilizării de către Direcția Generală a Poliția Locală Timișoara și pot fi comunicate numai următorilor destinatari: persoana vizată, reprezentanții legali/împuterniciții persoanei vizate, reprezentanții autorizați ai Direcției Generale a Poliției Locale Timișoara, organele de urmărire/cercetare penală, instanțe judecătorești, în conformitate cu prevederile legislației interne și comunitare aplicabile activității desfășurate de Direcția Generală a Poliției Locale Timișoara.

Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de 30 de zile, cu excepția situațiilor temeinic justificate (ex. existența unei solicitări din partea instituțiilor abilitate). La expirarea termenului înregistrările se distruge sau se șterg.

Persoanele vizate, respectiv angajații, vizitatorii și alte persoane care intră în sediul Direcției Generale a Poliției Locale Timișoara vor fi informate în legătură cu prelucrarea datelor personale prin intermediul sistemelor de supraveghere video. Indicatoarele de marcarea a existenței sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video - CCTV.

Accesul persoanelor care nu fac parte din efectivul instituției se face pe la poarta 1. Toate documentele/ sistemele electronice care conțin date cu caracter personal vor fi poziționate/ orientate astfel încât să nu fie accesibile/ vizibile personalului neautorizat.

Sistemul GPS are ca scop controlul activ al parcului auto, reducerea uzurii, reducerea consumului de combustibil, verificarea și optimizarea rutelor vehiculelor, generarea de rapoarte în timp real pentru toate componentele parcului auto precum și dirijarea de către dispecerul de serviciu a celui ai apropiat echipaj la intervenție. Accesul la acest tip de date cu caracter personal este permis doar persoanelor autorizate/ nominalizate în acest sens.

Sistemul GPS tetra are ca scop creșterea operativității și gestionarea eficientă a patrulelor în teren de către dispeceratul Direcției Generale a Poliției Locale Timișoara, practic coordonarea activității personalului propriu și intervenția la evenimente pe principiul „cel mai apropiat polițist de locul evenimentului intervine”, monitorizarea traseului parcurs în vederea executării atribuțiilor de serviciu și asigurării respectării buletinului postului și deconectarea, în caz de necesitate.

Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, Direcția Generală a Poliției Locale Timișoara 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 sunt necesare protejării datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Măsurile se revizuiesc și se actualizează dacă este necesar.

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

Măsurile tehnice și organizatorice cuprind sisteme de supraveghere video și sisteme antifracție; monitorizarea și intervenția în caz de alarmă asigurată în permanență de personalul autorizat; 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; instruirea personalului în legătură cu aspectele legale privind protecția datelor personale și cu privire la riscurile pe care le comportă prelucrarea datelor personale; stabilirea pentru fiecare utilizator a tipului de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu; etc

Personalul Poliției Locale Timișoara 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 atunci când 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.

Operațiunile de colectare, introducere, modificare și actualizare a datelor cu caracter personal se realizează numai de personalul anume desemnat conform actelor de reglementare internă;

- Poliția Locală Timișoara 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, în funcție de mărimea, volumul și importanța acestor baze de date;
- Poliția Locală Timișoara desemnează/stabilește utilizatori care să aibă atribuții de serviciu și executarea copiilor de siguranță ale bazelor de date deținute/create și ale programelor folosite;
- 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 și numai pentru îndeplinirea atribuțiilor de serviciu (acces restricționat/controlat);
- Documentele, terminalele de acces/echipamentele care conțin date cu caracter personal vor fi păstrate în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare și/sau în încăperi 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 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 la datele cu caracter personal care se regăsesc în rețeaua Poliției Locale Timișoara – serverele și stațiile de lucru, se face controlat pe bază de user și parolă, setate exclusiv de responsabilul IT desemnat, utilizatorii având drept de acces limitat, conform procedurilor interne (ex: read only, write, execute, modify, full control etc.);
- Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD etc.) care conțin date cu caracter personal, decât cu aprobarea prealabilă a conducerii;
- Utilizatorii 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

– Utilizatorii 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;

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.

Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic 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. Contractul sau actul juridic prevede în special ca persoana împuternicită de operator: prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului; 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; adoptă toate măsurile tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor personale corespunzător, în conformitate cu cerințele legislației specifice; respecta condițiile menționate privind recrutarea unei alte persoane împuternicite de operator; 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; 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; pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

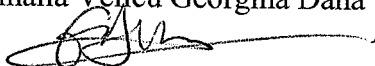
În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator 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.

Drepturile persoanelor vizate conform Regulamentului General privind Protecția Datelor, sunt:

- dreptul la informare (art. 13, 14, 34)
- dreptul de acces al persoanei vizate (art. 15)
- dreptul la rectificare (art. 16)
- dreptul la ștergerea datelor - "dreptul de a fi uitat" (art. 17)
- dreptul la restricționarea prelucrării (art. 18)
- dreptul la notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării (art. 19)
- dreptul la portabilitatea datelor (art. 20)
- dreptul la opoziție (art. 21)

- dreptul de a nu face obiectul unei decizii individuale automatizate, inclusiv crearea de profiluri (art. 22)
- dreptul de a depune o plângere la o autoritate de supraveghere (art. 77)
- dreptul de a se adresa justiției (art. 79)

Sef Serviciul Dispecerat
Mihailă Velicu Georgina Dana



Avizat Juridic

Şef BCEJ

Tănase Dan

