



ROMANIA  
MUNICIPIUL TURDA  
S.P. POLITIA LOCALA  
Str. P-ța Romana, nr. 39, loc. Turda, jud. Cluj  
Tel./Fax: 0264-317303  
[office@politialocalaturda.ro](mailto:office@politialocalaturda.ro)

NR. 4055/11 05. AUG. 2020

Operator de date cu caracter personal 10309

APROB,  
DIRECTOR EXECUTIV,  
MOLDOVAN VALER



## **POLITICA PRIVIND GESTIONAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL POLIȚIEI LOCALE TURDA**

**ÎN CONTEXTEL PANDMIEI COVID -19**



## **POLITICA PRIVIND GESTIONAREA DATELOR CU CARACTER PERSONAL ÎN CONTEXTEL PANDMIEI ÎN CADRUL POLȚIEI LOCALE TURDA**

### **DEFINITII:**

„**GDPR**”, „**Regulamentul**” - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, în limba engleză General Data Protection Regulation);

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

„**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, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea,

„**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; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

„**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 (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;

„**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;

**„*consumămant*”** - 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;

**„*reprezentant*”** - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternică de operator, care reprezintă operatorul sau persoana împuternică în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

**„*reguli corporatiste obligatorii*”** - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternică 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 împuternică 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;

**„*autoritate de supraveghere*”** - înseamnă o autoritate publică independentă instituită de un stat membru;

**„*DPO*”** - responsabilul cu protecția datelor (în limba engleză, data protection officer);

**“*Contact*”** - În contextul unei aplicații de urmărire a contactelor, un contact este un utilizator care a participat la o interacțiune cu un utilizator confirmat ca fiind purtător al virusului, pe o durată și la o distanță care determină un risc de expunere semnificativă la infecția virală. Parametrii privind durata expunerii și distanța dintre persoane trebuie să fie estimați de autoritățile din domeniul sănătății și pot fi stabiliți în aplicație.

**”*date de localizare*”** - Înseamnă toate datele prelucrate într-o rețea de comunicații electronice sau de un serviciu de comunicații electronice care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu public de comunicații electronice (astfel cum este definit în directivă), precum și datele din alte surse potențiale referitoare la: • latitudinea, longitudinea sau altitudinea echipamentului terminal; • direcția de deplasare a utilizatorului sau • momentul în care au fost înregistrate informațiile de localizare.

**"interacțiune"** În contextul unei aplicații de urmărire a contactelor, o interacțiune este definită ca schimbul de informații dintre două dispozitive aflate în imediata apropiere (în spațiu și timp) în raza de acțiune a tehnologiei de comunicații utilizate (de exemplu, Bluetooth). Această definiție exclude localizarea celor doi utilizatori ai interacțiunii.

**"purtător al virusului"** - În documentul de față, sunt considerați purtători ai virusului utilizatorii care au fost depistați pozitiv în urma testării și care au primit un diagnostic oficial din partea unui medic sau a unui centru medical.

**"urmărirea contactilor – monitorizarea"** - Persoanele care au fost în contact apropiat (conform unor criterii care urmează a fi definite de epidemiologi) cu o persoană infectată cu virusul au un risc semnificativ de a fi la rândul lor infectate și de a infecta alte persoane. Urmărirea contactelor este o metodologie de control al transmisiei bolilor prin care se întocmește o listă cu toate persoanele care au fost în imediata apropiere a unui purtător al virusului, astfel încât să se verifice dacă acestea sunt expuse riscului de infecție și să se ia măsurile sanitare corespunzătoare.

## SCOPUL ȘI DOMENIUL DE APLICARE

### SCOPUL

Prezenta politică are în vedere reguli măsuri pentru a asigura faptul că orice persoană fizică care acionează sub autoritatea POLIȚIEI LOCALE TURDA gestionează (colectează/prelucrează) datele cu caracter personal ale persoanelor "Contact" sau "purtător al virusului" în contextul pandemiei de Covid 19, exclusiv la cererea motivată a autorităților publice care gestionează buna desfășurare a activităților necesare combaterii pandemiei de Covid 19.

**Poliția Locală Turda** utilizează/prelucrează datele cu caracter personal ale persoanelor "Contact" sau "purtător al virusului" în contextul pandemiei de Covid 19 în **scopul monitorizării acestora în vederea respectării măsurilor de carantină sau izolare/distanțare socială și sancționare pentru nerespectarea măsurilor impuse de legislație în acest sens.**

Angajații Poliției Locale Turda înțeleg și au reprezentarea deplină a faptului că încălcarea regulilor privind **gestionarea greșită a datelor cu caracter personal** poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, persoanei fizice în cauză.

## **DOMENIUL DE APLICARE**

Prezenta politică se aplică de către toți polițiștii locali, funcționari publici, personal contractual din structurile organizatorice ale Poliției Locale Turda:

- ❖ Serviciul Ordine și Siguranță Publică,
- ❖ Serviciul Baza de Date, Dispecerat și Relații Publice,
- ❖ Serviciul Disciplina în Construcții, Protecția Mediului și Control Comercial și
- ❖ Serviciul Finaciar Contabil, Resurse Umane și Juridic.

Prezenta politică va fi considerată ca având *caracter special* și se va aplica prelucrărilor de personale gestionate de Poliția Locală Turda, în activitățile conexe în contextul pandmiei COVID 19.

În cazul în care se constată existența anumitor aspecte legate de gestionarea datelor cu caracter general pentru care prezenta politică nu oferă directive corespunzătoare, angajații trebuie să solicite imediat consiliere din partea Ofițerului responsabil cu protecția datelor (DPO), doamna Mureșan Ioana.

## **REGULI GENERALE**

### **Principii privind prelucrarea.**

Desfășurarea activității curente a Poliției Locale Turda, presupune efectuarea de către angajați a unor prelucrări de date care se supun următoarelor principii:

- datele sunt prelucrate în mod legal, echitabil și transparent;
- datele sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public.
- datele sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- datele sunt exacte și, în cazul în care este necesar, să fie actualizate; se vor lua toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- datele sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal sunt stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;
- datele sunt prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

## **Informații referitoare la datele personale reținute:**

În cadrul Plenarei Comitetului European pentru Protecția Datelor, s-a adoptat Declarația referitoare la interoperabilitatea aplicațiilor de localizare în contextul pandemiei Covid 19, care are la bază Ghidul nr. 4/2020 privind utilizarea datelor de localizare și a instrumentelor de depistare în contextul pandemiei Covid-9. (*afișat spre consultare la avizierele instituțieie*).

Ghidul adoptat este urmare a numeroaselor probleme ridicate de guverne și entități private și evidențiază **condițiile și principiile de utilizare proporțională a datelor de localizare în scopul monitorizării răspândirii virusului**, respectiv a instrumentelor de depistare pentru a anunța persoanele aflate în apropierea altor persoane depistate ca infectate.

Ca urmare a acestei Declarații prin care subliniază: **necesitatea respectării transparenței și legalității prelucrărilor implicate, a drepturilor utilizatorilor și personelor cu respectarea principiului minimizării datelor și asigurării confidențialității datelor cu caracter personal** în Conextul pandemiei COVID 19, astfel:

**Poliția Locală Turda**, reiterează faptul că este Operator de date cu caracter personal și prelucrează toate datele cu caracter personal cu respectarea:

- prevederilor Regulamentului (UE)nr.679/2016,
- a Legii nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și
- a Politicii Poliției Locale Turda privind confidențialitatea datelor nr.6444/16.07.2018.

In contextul pandemiei Covid 19, prezic că Poliția Locală Turda ca operator de date persoanele interacționează atât cu date de localizare cât și identificare a persoanelor, prin schimb de informații cu DSP Cluj, Poliția Municipiului Turda, autorități publice locale Direcția Asistență Socilă și Spitalul Municipal Turda, astfel:

- **date de localizare:** adresa de domicilu sau adresa declarată conform FISEI de verificare
- **date de identificare contact sau purtător al virusului** (vezi definiții Ghid 4/2020): nume, prenume, data nașterii (CNP), portret - foto, număr telefon.

## **Reducerea la minimum a datelor**

Poliția Locală Turda respectă principiul reducerii la minimum a datelor potrivit GDPR, respectiv reține și stochează numai datele relevante și necesare îndeplinirii scopului prelucrării datelor cu caracter personal. Prelucrează aceste date numai și numai în scopul definit, cu respectarea transparenței și legalității prelucrărilor implicate, drepturilor persoanelor și respectarea principiului minimizării datelor

și asigurării confidențialității acestora pentru a sprijini evaluarea eficacității globale a măsurilor de izolare și urmărirea contactelor astfel încât să se rupă cât mai rapid lanțurile de contaminare.

Se interzice interoperabilitatea să fie folosită ca motiv pentru a extinde colectarea sau prelucrarea datelor mai mult decât este necesar, Poliția Locală Turda interechionând strict cu datele furnizate de DSP Cluj și Poliția Municipiului Turda și persoana vizată fie "contact" sau "purtător al virusului".

### **Exactitate**

Datele personale prelucrate de Poliția Locală Turda sunt exacte și actualizate la momentul gestionării/prelucrării efectuând verificări pentru a asigura acest aspect în cazul în care este necesar.

### **Termenele de stocare**

Poliția Locală Turda ia măsuri adecvate privind eliminarea datelor cu caracter personal atunci când acestea nu mai sunt necesare atingerii scopului prelucrării. Acest lucru reduce riscul stocării unor date inexakte, inutile sau irelevante. Această obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

Prelucrarea ulterioară a acestor date în alte scopuri care nu au legătură cu gestionarea crizei sanitare generate de COVID19 fiind interzise, acestea fiind păstrate numai pe perioada crizei generate de pandemia Covid19. Ulterior ca regulă generală aceste date sunt șterse.

Operatorul va asigura ștergerea/distrugerea datelor personale, cu excepția cazului în care legislația EU sau cea națională prevăd obligația păstrării acestora pe o perioadă mai îndelungată.

## **REGULI SPECIFICE PRIVIND GESTIONAREA DATELOR**

### **Sfera datelor personale**

#### **Datele persoanelor vizate:**

- În contextul combaterii pandemiei de Covid 19, Poliția Locală Turda prelucrează următoarele date cu caracter personal ale contactului/ților sau purtător al virusului: **date de localizare** (adresa de domiciliu sau adresa declarată) și **date de identificare** nume, prenume, data nașterii (CNP), portret -foto, număr telefon, comunicate după cum urmează:

- prin intermediul formularelor, fișelor de verificare privind monitorizarea persoanei și prin intermediul comunicărilor transmise Poliției Locale Turda în formă scrisă, în formă electronică, completări la întrebările formulate telefonic de autorități publice abilitate din cadrul M.A.I sau Ministerului Sanătatii.

#### **Datele angajaților**

Poliția Locală Turda colectează și utilizează datele personale ale angajaților în temeiul legii și numai în scopuri relevante, corespunzătoare și uzuale.

Poliția Locală Turda, recunoaște și respectă drepturile de confidențialitate ale angajaților săi, nu limitează colectarea, accesul și utilizarea datelor de către autoritățile abilitatea DSP, Poliția penrtu a lúa ia măsuri preventive în contextul Pandemiei de Covid 19. Respectivele divulgări pot avea loc numai în condițiile în care există înțelegerea deplină a faptului că accesul și utilizarea datelor sunt limitate, și că datele trebuie să fie protejate.

### **Soluții de organizare**

Poliția Locală Turda în calitate de Operator, a adoptat următoarele soluții de organizare în ceea ce privește gestionarea datelor cu caracter personal:

- ✓ Responsabilitatea privind **prelucrarea datelor** în acord cu prezenta politică revine tuturor angajaților, Operatorul va asigura măsurile organizatorice necesare implementării prevederilor GDPR, astfel încât prelucrările datelor cu caracter personal să fie efectuate în conformitate cu legislația europeană și națională;
- ✓ DPO-ul va instrui angajații astfel încât aceștia să respecte gestionarea corectă a datelor personale;
- ✓ Angajații sunt obligați să respecte măsurile de prelucrare a datelor cu caracter personal, asigurându-se un nivel adecvat de protecție a datelor astfel prelucrate.

Poliția Locală Turda în contextul pandemiei Covid 19, utilizează datele cu caracter personal ale persoanelor Contact/purtator al virusului în mod responsabil, în scopul general anume cel de gestionare a sănătății în scopul principal menționat și asigurându-se în același timp că nu se restrâng drepturile și libertățile individuale ale persoanei, fiind interzisă cu desăvârșire dezvăluirea publică a datelor persoanele ale persoanei și/sau a stării de sănătate a acestora fie contact sau purtător al virusului.

### **Verificarea corectitudinii datelor cu caracter personal**

Toți angajații au obligația să verifice datele personale gestionate din perspectiva acurateței și integralității informațiilor relevante și trebuie să gestioneze corespunzător conform regulilor de protecție a datelor personale, a principiilor generale de prelucrare, în special a principiului asigurării securității și confidențialității și a principiului responsabilității.

## **REGULI PRIVIND PROCEDURA DE RAPORTARE ȘI TRATARE INCIDENTE DE SECURITATE**

### **Aspecte generale.**

„ Incidentul de securitate înseamnă o încălcare a securității care duce la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal, în mod

accidental sau ilegal. Aceasta include încălcările cauzate atât în mod accidental, cât și în mod intenționat.

În momentul raportării unei încălcări, trebuie incluse următoarele informații:

- ✓ descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil: categoriile și numărul aproximativ al persoanelor vizate în cauză; categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- ✓ 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 pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Încălcările securității datelor cu caracter personal pot cuprinde:

- ✓ accesul unui terț neautorizat;
- ✓ acțiunea (sau inacțiunea) intenționată sau accidentală a unui operator sau unei persoane împuernicite de operator;
- ✓ trimitera unor date cu caracter personal către un destinatar greșit;
- ✓ pierderea sau furtul unor dispozitive informative care conțin date cu caracter personal;
- ✓ modificarea datelor cu caracter personal fără permisiune;
- ✓ pierderea disponibilității datelor cu caracter personal.

Pentru transmiterea Notificării către Autoritatea de supraveghere se va folosi modelul pus la dispoziție [Formular de notificare a încălcării securității datelor către ANSPDCP].

Persoana responsabilă de transmiterea Notificării către Autoritatea de supraveghere este Mureșan Ioana. Termenul de transmitere a notificării este 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

În măsura în care decizia este de a nu informa persoanele vizate, trebuie notificată ANSPDCP, dacă nu se poate demonstra că încălcarea nu este susceptibilă să genereze un risc pentru drepturi și libertăți. În orice caz, trebuie păstrate documente cu privire la procesul de luare a deciziei în conformitate cu cerințele principiului responsabilității.

Întocmit,

D.P.O – MUREȘAN IOANA



