

Regulamentul

privind politica de securitate a protecției datelor cu caracter personal la prelucrarea acestora gestionate de către Primăria Cojușna

Prezentul regulament privind politica de securitate a protecției datelor cu caracter personal la prelucrarea acestora gestionate de către Primăria Cojușna (în continuare Regulament) este aprobat, inclusiv, în vederea conformării APL-ului cu prevederile Hotărârii Guvernului Republicii Moldova nr. 1123 din data de 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal” și Legii Republicii Moldova nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

I. Noțiuni Generale

În prezentul Regulament sînt definite următoarele noțiuni:

- *date cu caracter personal* - orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;
- *categorii speciale de date cu caracter personal* - datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale;
- *operator* - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;
- *persoană împuternicită de către operator* - persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;
- *autentificare* - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;
- *control de securitate* - acțiuni întreprinse de către APL în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale sau registrelor ținute;
- *fișiere temporare* - ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat pînă la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;
- *identificare* - atribuirea unui identificator subiecților și obiectelor de acces sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

- *integritate* - certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;
- *mijloace de protecție criptografică a informației care conține date cu caracter personal* - mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;
- *nivel de protecție* - nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;
- *politica de securitate a datelor cu caracter personal* - document, elaborat de către operatorul de date - APL, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sunt expuse acestea;
- *perimetru de securitate* - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;
- *persoana responsabilă de politica de securitate a datelor cu caracter personal* - 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;
- *protecția informației contra acțiunilor neintenționate* - ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;
- *purător de date cu caracter personal* - suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;
- *restaurarea datelor* - procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;
- *tehnologie informațională* - totalitatea metodelor, procedeele și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;
- *utilizator* - persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;
- *sesiune de lucru* - perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și pînă la momentul opririi acestora;
- *sistem informațional de date cu caracter personal* - totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;
- *prelucrarea datelor cu caracter personal* - orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau

neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

- *stocare* - păstrarea pe orice fel de suport a datelor cu caracter personal;
- *sistem de evidență a datelor cu caracter personal* - orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;
- *consimțământul subiectului datelor cu caracter personal* - orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;
- *depersonalizarea datelor* - modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

II. Obiectivele Politicii de Securitate

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de Primăria Cojușna, atât în cadrul prelucrării manuale, cât și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul APL. Baza unei securități IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datele cu caracter personal, sistemelor și proceselor IT împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Avînd în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.

APL va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a angajaților săi.

Reglementările prezentei Politici, reprezintă un standard minim inclusiv pentru toți angajații primăriei. Pornind de la această reglementare, toți angajații urmează să respecte strict prevederile Politicii și regulile interne ale APL privind protecția datelor cu caracter personal și sistemelor IT.

III. Mijloacele supuse principiilor de protecție a datelor cu caracter personal

Protecția datelor cu caracter personal în cadrul primăriei este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal. Sînt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;

- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

Măsurile de protecție a datelor cu caracter personal sînt asigurate în scopul:

- preîntîmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atît pe suport de hîrtie cît și cel în format electronic.

Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

- preîntîmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntîmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntîmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntîmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații;
- preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;
- preîntîmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.
- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atît pentru utilizatorii interni cît și pentru cei externi.

IV. Procedurile organizatorice și tehnice care urmează a fi respectate la prelucrarea datelor cu caracter personal

1. Măsurile generale de administrare a securității informaționale

- a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
- b) Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru.

- c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
- d) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.
- e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
- f) Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.
- g) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

2. Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

- a) Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare);
- b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces;
- c) Perimetrul de securitate a primăriei reprezintă perimetrul oficiilor în care se prelucrează/stochează date cu caracter personal;
- d) Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare;
- e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri;
- f) Ușile și ferestrele se încuie în cazul în care în încăperea lipsesc membrii.
- g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
- h) Accesul în perimetrul de securitate a clădirii unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținînd cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal;
- i) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii.

3. Identificarea și autentificarea utilizatorilor

- a) Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
- b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnamentele nivelului de accesibilitate al utilizatorului;
- c) Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.

- d) În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile permise în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul I.T.

4. Utilizarea parolelor în procesul asigurării securității informaționale

Sunt respectate regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- păstrarea confidențialității parolelor,
- interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia,
- modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei,
- alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere,
- modificarea parolelor peste intervale de 3 luni,
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

5. Accesul de la distanță

a) Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului.

b) Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale primăriei și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

6. Limitarea folosirii tehnologiilor fără fir

a) Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.

b) Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.

c) Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile.

7. Drepturile subiecților de date cu caracter personal

a) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art. 12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptând cazul în care el deține deja informațiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);

- privind scopul concret al prelucrării datelor cu caracter personal colectate;

- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor (în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a caror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluzării sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale (alte materiale), cu excepția cazurilor în care solicitantii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură mentenanța sistemului și sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.

d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaționale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

8. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

a) Accesul în spațiile unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale, regulamentelor departamentale aprobate.

b) Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.

c) Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul primăriei.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

9. Asigurarea protecției contra programelor dăunătoare (virusurilor)

Este asigurată protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate anti-virus.

10. Marcarea documentelor

Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea parafei de atenționare.

Model: „Atenție! Acest act conține date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133/2011 privind protecția datelor cu caracter personal”

11. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 741 Cod contravențional) și penală (art. 177, 178, 180 Cod penal).