Aprobat:
Preşedinte interimar al Judecătoriei Cimişlia
_____Veronica CARAPIREA
„16" 01 2025

Politica de securitate

privind protecţia datelor cu caracter personal în cadrul Judecătoriei Cimişlia

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul Judecătoriei Cimişlia sunt aplicate principiile prevăzute de actele:

Internaţionale:

- Declaraţia universală a drepturilor omului;
- Convenţia 108 a Consiliului Europei;
- DIRECTIVA 2002/58/CE A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice (Directiva asupra confidenţialităţii şi comunicaţiilor electronice);
- REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);

Naţionale:

- Constituţia Republicii Moldova;
- Codul administrativ nr. 116/2018;
- Legea nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal;
- Legea nr. 158-XVI din 04.07.2008 cu privire la funcţia publică şi statutul funcţionarului public;
- Legea nr.148 din 09.06.2023privind accesul la informaţiile de interes public;
- Legea nr. 71-XVI din 22 martie 2007 cu privire le registre;
- Legea comunicaţiilor electronice nr. 241-XVI din 15.11.2007;
- Legea nr. 467-XV din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat;
- Legea nr. 142 din 19.07.2018 cu privire la schimbul de date şi interoperabilitate;
- Legea nr. 64 din 23.04.2010 cu privire la libertatea de exprimare;
- Legea nr. 91 din 29.05.2014 privind semnătura electronică şi documentul electronic;
- Legea integrităţii nr. 82 din 25.05.2017;
- Legea nr. 270 din 23.11.2018 privind sistemul unitar de salarizare în sectorul bugetar;
- Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal;
- Hotărârea Guvernului nr. 883 din 25 noiembrie 2011 cu privire la aprobarea Conceptului tehnic al sistemului informaţional automatizat „Registrul de stat al operatorilor de date cu caracter personal";
- Hotărârea Guvernului nr. 296 din 15 mai 2012 privind aprobarea Regulamentului Registrului de evidenţă a operatorilor de date cu caracter personal;
- Hotărârea Guvernului nr. 571 din 30 iulie 2013 cu privire la aprobarea proiectului de lege pentru aprobarea Strategiei naţionale de dezvoltare a domeniului protecţiei datelor cu caracter personal pentru anii 2013-2018 şi a Planului de acţiuni privind implementarea acesteia;
- Hotărârea Guvernului nr. 282 din 27 aprilie 2022 cu privire la lichidarea Registrului de evidenţă al operatorilor de date cu caracter personal şi abrogarea unor hotărâri ale Guvernului
- Hotărârea Consiliului Superior al Magistraturii nr. 457/29 din 18 octombrie 2023 cu privire la aprobarea Regulamentului privind standardele minime de calitate privind activitatea organizatorică şi administrativă a judecătoriilor şi curţilor de apel.

II. INTRODUCERE

Politica este aprobată de către președintele interimar care acționează în baza Hotărârii CSM nr. 669/41 din 2 decembrie 2024 referitor la cererea judecătorului Dumitru Cherdivara de demisie din funcția de președinte interimar al Judecătoriei Cimișlia.

Prezenta Politică este aprobată, inclusiv, în vederea conformării Judecătoriei Cimișlia cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal și Hotărârii Guvernului nr. 1123 din 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, având drept scop stabilirea regulilor minime de implementare de către deținătorii de date cu caracter personal a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale de date cu caracter personal și/sau registrelor ținute manual.

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta") și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

Directiva 95/46/CE a Parlamentului European și a Consiliului (4) vizează armonizarea nivelului de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește activitățile de prelucrare și asigurarea liberei circulații a datelor cu caracter personal între statele membre.

III. DISPOZIȚII GENERALE

În prezenta Politică de securitate, sânt definite/utilizate 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;

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;

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;

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 şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

terţ – persoană fizică sau persoană juridică de drept public ori de drept privat, alta decît subiectul datelor cu caracter personal, decît operatorul ori persoana împuternicită de către operator şi decît persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

destinatar – orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, căreia îi sînt dezvăluite date cu caracter personal, indiferent dacă este sau nu terţ. Nu sînt considerate destinatari organele din domeniul apărării naţionale, securităţii statului şi ordinii publice, organele de urmărire penală şi instanţele judecătoreşti cărora li se comunică date cu caracter personal în cadrul exercitării competenţelor stabilite de lege;

autentificare – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

control de securitate – acţiuni întreprinse de către deţinătorii de date cu caracter personal sau Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare – Centrul), în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute manual, în conformitate cu prezentele Cerinţe;

fişiere temporare – ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare – atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate – certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal– mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

nivel de protecţie – nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, stabilit conform Cerinţelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri (**N - 1** sau **N - 2**);

politica de securitate a datelor cu caracter personal – document, elaborat de către deţinătorul de date cu caracter personal, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sînt expuse acestea;

perimetru de securitate – zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

protecţia informaţiei contra acţiunilor neintenţionate – ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

purtător de date cu caracter personal – suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;

restaurarea datelor – procedurile cu privire la reconstituirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

tehnologie informaţională ((TI) eng. informational technology) – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

utilizator – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

sesiune de lucru – perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi pînă la momentul opririi acestora;

sistem informaţional de date cu caracter personal – totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

stocare – păstrarea pe orice fel de suport a datelor cu caracter personal;

consimţământul subiectului de date cu caracter personal – manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

depersonalizarea datelor – modificarea datelor cu caracter personal astfel încît detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condiţiile unei investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă;

creare de profiluri – formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte referitoare la o persoană fizică, în special pentru a analiza sau a stabili aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele, interesele, fiabilitatea, comportamentul, locul în care se află persoana respectivă şi deplasările acesteia.

III. Obiectivele

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Judecătoria Cimişlia, atât în cadrul prelucrării manual, cât şi sistemelor şi proceselor de tehnologie informaţională (în continuare IT).

Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe IT în cadrul Judecătoriei Cimişlia. Baza unei securităţi IT adecvate o constituie respectarea prezentei Politici. Acesta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor IT împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislaţiei.

Având în vedere că siguranţa IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură.

Judecătoria Cimişlia va proteja datele cu caracter personal atât a participanţilor la proces/vizitatori, cât şi a angajaţilor săi.

Reglementările prezentei Politici reprezintă un standard minim pentru Judecătoria Cimişlia, inclusiv toţi angajaţii Judecătoriei Cimişlia. Pornind de la această reglementare, toţi angajaţii instanţei urmează să respecte strict prevederile Politicii şi regulilor interne, privind protecţia datelor cu caracter personal şi sistemelor IT.

IV. Dispoziţii privind ierarhia şi responsabilităţile persoanelor responsabile de Politica de securitate

Operatorul de date cu caracter personal reieşind din specificul activităţii, prin prezenta Politică de securitate, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.

Politica de securitate a datelor cu caracter personal se va revizui la necesitate ca rezultat al modificărilor sau reevaluării competenţelor entităţii, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

Politica de securitate, în mod obligatoriu va fi adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

Responsabil de implementarea şi monitorizarea respectării prevederilor Politicii de securitate a datelor cu caracter personal, va fi desemnată persoana care conform Fişei de post şi/sau Ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoana responsabilă desemnată, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducătorului Judecătoriei Cimişlia sau persoanei care îndeplineşte interimatul funcţiei.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor persoanale sau alte împrejurări.

Persoana responsabilă de politica de securitate a datelor cu caracter personal:

- va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală;
- va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal;
- va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;
- va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

V. Misiunile de bază

Principiile şi normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor lor cu caracter personal ar trebui, indiferent de cetăţenia sau de locul de reşedinţă al persoanelor fizice, să respecte drepturile şi libertăţile fundamentale ale acestora, în special dreptul la protecţia datelor cu caracter personal. Prezenta politică urmăreşte să contribuie la realizarea unui spaţiu de libertate, securitate şi justiţie, la bunăstarea persoanelor fizice.

Legalitate – ceea ce presupune că, în toate acţiunile, angajaţii sunt obligaţi să respecte cu strictețe legea, drepturile, libertăţile constituţionale şi fundamentale ale subiecţilor datelor cu caracter personal, în corespundere cu Declaraţia Universală a Drepturilor Omului, Convenţia Europeană pentru Apărarea Drepturilor Omului şi a Libertăţilor Fundamentale, Constituţia Republicii Moldova, alte acte legislative şi normative în vigoare.

Transparenţă - este abilitatea de a pune la dispoziţia publicului informaţii relevante şi în timp util cu privire la activităţile desfăşurate în cadrul instituţiei. Prin acest principiu societatea civilă îşi realizează dreptul de a cunoaşte şi a avea acces la informaţiile de interes public, precum şi asupra activităţii autorităţilor publice.

Obiectivitate – presupune să nu permită ca prejudecăţile, conflictul de interese sau influenţa nedorită a altor persoane să intervină în raţionamentele profesionale ale angajaţilor din cadrul Judecătoriei.

Confidenţialitate – determină obligaţia funcţionarului instanţei de a garanta prelucrarea, utilizarea, securizarea datelor şi a informaţiilor obţinute în exercitarea atribuţiilor prevăzute de lege prin nedivulgarea lor unor terţe persoane.

Profesionalism – angajaţii instanţei au obligaţia să-şi îndeplinească atribuţiile de serviciu cu responsabilitate, competenţă, eficienţă şi corectitudine, aplicând experienţa şi abilităţile dobândite.

Respect – acest principiu presupune obligaţia angajaţilor de a avea un comportament onorabil şi politicos faţă de justiţiabili, subiecţii datelor cu caracter personal, dar şi alte persoane în exercitarea funcţiei.

Integritate morală – funcţionarii instanţei trebuie să aibă un comportament care să asigure onestitatea şi integritatea exercitării funcţiei.

VI. Locaţia şi descrierea sistemului de evidenţă

Datele cu caracter personal conţinute în cadrul Judecătoria Cimişlia se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic;
- softuri, programe, aplicaţii.

VII. Mijloacele supuse principiilor de protecţie a datelor cu caracter personal

Protecţia datelor cu caracter personal în cadrul Judecătoriei Cimişlia (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

Sînt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe:

- suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
- sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

VIII. Durata de stocare

Prelucrarea datelor cu caracter personal de către Judecătoria Cimişlia se efectuează în baza acţiunilor prevăzute de actele legislative.

IX. Măsurile de protecţie a datelor cu caracter personal sunt asigurate în scopul:

- preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
- respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
- asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
- păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal;
- neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată;
- eficientizarea resurselor informaţionale atât pe suport de hârtie cât şi cel în format electronic.

X. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

- preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim (utilizarea canalelor VPN).
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal, sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă;
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale;
- stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atât pentru utilizatorii interni cît şi pentru cei externi.

XI. Procedurile organizatorice şi tehnice care urmează a fi respectate în cadrul Judecătoriei Cimişlia la prelucrarea datelor cu caracter personal

1. Măsurile generale de administrare a securităţii informaţionale

a) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.
b) Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.
c) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.
d) Trebuie administrat accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.
e) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine 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 deţinătorului de date cu caracter personal.
f) Scoaterea şi introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează în registru.
g) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
h) Este interzisă instalarea programelor de tip shareware sau freeware, fără aprobarea administratorului sistemului informatic.

2. Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

a) Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare, cartele cu microprocesoare).

b) Se asigură administrarea şi 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 al Judecătoriei Cimişlia reprezintă perimetrul oficiilor în care se prelucrează/stochează datele cu caracter personal.
d) Perimetrul clădirii sau încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să fie integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte, mijloace de control al accesului, semnalizare, la ferestrele sunt instalate gratii.
e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să răspundă necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor şi altor posibile riscuri.
f) Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajații.
g) Computerele, serverele, alte terminale de acces trebuie amplasate în locuri cu acces limitat pentru persoane străine.
h) Accesul în perimetrul de securitate a clădirii Judecătoriei Cimişlia unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținînd cont de necesitatea asigurării regimului de confidențialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 şi art. 30 ale Legii nr. 133/2011 privind protecția datelor cu caracter personal, precum şi pct. 26 din CERINȚELE față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobat prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010. (Anexă nr. 1)
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 şi autentificarea utilizatorilor

a) Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.
b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.
c) Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.
d) Se efectuează modificarea parolelor de fiecare dată când sunt depistați indicii unei eventuale compromiteri a sistemului sau parolei.
e) Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sunt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.
f) În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi 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 primite în
scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de către *deținătorul de date cu caracter personal.*

4. Identificarea şi autentificarea echipamentului

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal.

5. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:
1) identificarea univocă a fiecărui utilizator;
2) verificarea autenticităţii fiecărui utilizator;
3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;
4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (inacţiune în perioada de maximum 2 luni);
6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

6. Utilizarea parolelor în procesul asigurării securităţii informaţionale

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor, care includ:
1) păstrarea confidenţialităţii parolelor;
2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;
3) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri ale sistemului sau parolei;
4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;
5) modificarea parolelor peste intervale de maximum 3 luni;
6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7. Controlul administrării accesului

Este efectuat controlul sistematic al acţiunilor utilizatorilor în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

8. Accesul de la distanţă

a) Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.
b) Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Limitarea folosirii tehnologiilor fără fir

a) Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării şi controlului.
b) Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.
c) Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale deţinătorului de date cu caracter personal.

10. Securitatea electroenergetică

a) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.
b) În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.
c) Sunt implementate sisiteme automatizate de depistare şi semnalizare a incediilor în birourile unde sunt amplasate sistemele informaţionale de date cu cracter personal şi mijloacele de prelucrare a datelor cu caracter personal.
d) Sunt prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sînt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

11. Controlul instalării şi scoaterii componentelor TI

a) Este exercit controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.
b) Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

12. Dezvăluirea datelor cu caracter personal

a) Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de dastinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmânarea personal, etc.).
b) Dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor, (spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.) sunt interzise.
c) Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Judecătoria Cimişlia şi alte entităţii care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.
d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie şi/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituţional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.
e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul

internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

f) Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidenţei instanţei, este limitat la strictul necesar pentru realizarea scopurilor declarate.

g) Acces la sistemele informaţionale gestionate în cadrul Judecătoriei Cimişlia, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă pentru cauză, (inclusiv informaţia stocată în auditul sistemelor informaţionale şi de evidenţă), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art. 214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate.

Urmează a ţine cont de faptul că în conformitate cu prevederile art. 8, alin. (1), lit. (f) al Legii privind accesul la informaţiile interes public nr. 148 din 09 iunie 2023, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fişa personală a clientului, aceştia urmează a fi informaţi în scris despre obligaţiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 741 Cod contravenţional. (Declaraţia de a lua cunoştinţa cu materialele cauzei) (Anexa nr. 2)

13. Drepturile subiecţilor de date cu caracter personal

a) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecţia datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptînd cazul în care el deţine deja informaţiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidenţă 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;
- existenţa drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

b) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi 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 alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigură mentenanţa sistemului şi 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 intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaţionale şi de evidenţă gestionate.

14. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

a) Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.

b) Stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului - este interzisă.

c) Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Judecătoriei Cimişlia.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi 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.

15. Auditul sistemelor informaţionale gestionate

a) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

b) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii);
- denumirea (identificatorul) aplicaţiei sau procesului, a ID-ul utilizatorului;

- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

- data şi timpul modificării competenţelor;
- ID-ul administratorului care a efectuat modificările;
- ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

d) Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

- data şi timpul eliberării;
- denumirea informaţiei şi căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
- ID-ul utilizatorului, care a solicitat informaţia.

16. Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

Este asigurată protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existenţa programelor licenţiate anti-virus.

17. Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

18. Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.
b) Personalul Judecătoriei Cimişlia informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.
c) Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.
d) Anual, către 31 ianuarie, deţinătorii de date cu caracter personal prezintă Centrului raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecţia datelor cu caracter personal.

19. Marcarea documentelor

Informaţia ieşită din instanţă, care conţine date cu caracter personal, se marchează, indicîndu-se prescripţii pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deţinătorului de date cu caracter personal. Anexă nr. 3

20. Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal precum şi a informaţiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe după caz, semnatari a anexei nr. 3, pentru nerespectarea dispoziţiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravenţională (art. 741 Cod contravenţional) şi penală (art.art. 177, 178, 180 Cod penal).

XII. Informarea subiectului datelor cu caracter personal

În cazul în care datele cu caracter personal sânt colectate direct de la subiectul datelor, persoana împuternicită este obligată să-i furnizeze următoarele informaţii, exceptând cazul în care acesta deţine deja informaţiile respective:

- identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;
- scopul prelucrării datelor colectate;

Informaţii suplimentare, precum:

- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenţa drepturilor de acces la date, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care acestea pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sânt obligatorii sau voluntare, precum şi consecinţele posibile ale refuzului de a răspunde.

În cazul în care datele cu caracter personal nu sânt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informaţia privind categoriile de date care urmează a fi colectate sau dezvăluite.

XIII. Responsabilitatea personalului instanţei

Operatorul de date cu caracter personal reieşind din specificul activităţii, prin prezenta Politică, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul instanţei.

Politica de securitate a datelor cu caracter personal se va revizui la necesitate ca rezultat al modificărilor sau reevaluării competenţelor entităţii, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

Politica de securitate, în mod obligatoriu, va fi adus la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

Responsabil de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, vor fi desemnaţi şefii subdiviziunilor care conform fişei postului şi/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară în subdiviziunea sa pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoanele responsabile desemnate, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit preşedintelui/vicepreşedintelui (managerul) Judecătoriei Cimişlia sau persoanei care îndeplineşte interimatul funcţiei.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

IX. Atribuțiile angajaților Judecătoriei Cimișlia

1. SECRETARIATUL JUDECĂTORIEI

Sarcinile de bază al șefului de secretariat prin prisma respectării legislației în vigoare privind datelor cu caracter personal sunt:

- Monitorizarea bazei de date computerizată (Registrului electronic al angajaților, Registrul al funcționarilor publici) privind funcțiile și personalul autorității publice Judecătoria Cimișlia;
- Asigurarea activității administrativă și organizatorică a instanței;
- Coordonarea procesului de elaborare a planurilor de activitate și a programelor de dezvoltare strategică ale instanței;
- Asigurarea gestionarea mijloacelor financiare alocate instanței judecătorești;
- (aplicațiile e-alocații, e- docplat, SIMF) respectând Legea privind protecția datelor cu caracter personal;
- Coordonarea procesului de asigurare a instanței judecătorești cu personal, menținerea și dezvoltarea acestuia;
- Datele cu caracter personal conținute în cadrul secretariatului Judecătoriei Cimișlia se prelucrează/stochează:
  - pe suport de hârtie;
  - în format electronic.

Calculator de birou cu nr. de inventariere - 31460052, aflându-se în biroul (șef al secretariatului) din sediul central al Judecătoria Cimișlia ;

La expirarea termenului datele din cadrul secretariatului sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor -tip a termenelor de păstrare a acestora în instanțele judecătorești aprobat prin Hotărârea Consiliului Superior al Magistraturii nr. 377/19 din 31 iulie 2018.

Orice utilizare a datelor cu caracter personal parvenite în cadrul instanței în alte scopuri este interzisă.

2. GREFA SECRETARIATULUI JUDECĂTORIEI

2.1. ASISTENȚI JUDICIARI

Sarcinile de bază și atribuțiile asistentului judiciar prin prisma respectării datelor cu caracter personal sunt:

- Pregătirea actelor normative și a informației necesare judecătorului pentru examinarea cauzelor;
- Verificarea actelor prezentate și anexate la dosar de către participanții la proces;
- Elaborarea proiectelor de acte procesuale;
- Asigurarea depersonalizării actelor procesuale judecătorești salvarea acestora în PIGD și publicarea pe pagina web a instanței judecătorești.

În cazul în care datele cu caracter personal nu sânt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu în momentul primei dezvăluiri, să furnizeze

subiectului datelor cu caracter personal informația privind categoriile de date care urmează a fi colectate sau dezvăluite.

Orice utilizare a datelor cu caracter personal parvenite în cadrul ședinței și/sau introdusă în Programul Integrat de Gestionarea a Dosarelor în alte scopuri este interzisă.

La expirarea termenului datele din cadrul secretariatului sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor -tip a termenelor de păstrare a acestora în instanțele judecătorești aprobat prin Hotărârea Consiliului Superior al Magistraturii nr. 377/19 din 31 iulie 2018.

2.2. GREFIERI

Sarcinile de bază și atribuțiile grefierului prin prisma respectării datelor cu caracter personal sunt:

- prelucrarea și actualizarea prin certificare datele cu caracter personal din PIGD și din dosare.
- înștiințarea justițiabilii și participanții la proces despre efectuarea actelor de procedură și alte informații ce țin de competența sa;
- Înregistrarea corectă în SRS „FEMIDA„ ședințele de judecată.

La expirarea termenului datele din cadrul secretariatului sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor -tip a termenelor de păstrare a acestora în instanțele judecătorești aprobat prin Hotărârea Consiliului Superior al Magistraturii nr. 377/19 din 31 iulie 2018

Orice utilizare a datelor cu caracter personal parvenite în cadrul ședinței și/sau introdusă în Programul Integrat de Gestionarea a Dosarelor în alte scopuri este interzisă.

3. SERVICIUL GENERALIZARE, SISTEMATIZARE, MONITORIZARE A PRACTICII JUDICIARE ȘI RELAȚII CU PUBLICUL

Sarcinile de bază și atribuțiile SGMPJRP prin prisma respectării datelor cu caracter personal sunt:

- elaborarea și asigurarea plasării informației pe website-ul instanței și panoul informativ pentru publicul larg;
- organizarea conferințelor de presă, întocmirea comunicatelor de presă sub coordonarea președintelui instanței și a purtătorului de cuvânt comunicate despre activitatea instanței, cauze de rezonanță, ținând cont de principiul confidențialității datelor cu caracter personal, cu publicarea acestora pe pagina web;
- colaborarea cu mass-media, instituțiile de drept, societatea civilă și justițiabilii în sensul furnizării informației de interes public;
- oferirea informațiilor justițiabililor, subiecți ai dosarului, doar la prezentarea actului de identitate, astfel evitând expunerea informațiilor din dosar unei alte persoane decât cea pe cauză;
- examinarea și întocmirea, în limitele competenței, a răspunsurilor la demersurile, sesizările și petițiile înregistrate, prezentându-le președintelui instanței pentru coordonare și semnare;
- gestionarea poștei electronice a instanței de judecată;
- coordonarea și asigurarea funcționalității Centrului de informare și a Liniei Instituționale din cadrul instanței.

Birou SGMPJRP – calculator de inventariere nr. 31460060, – calculator de inventariere 031400006.
telefon 0236 26905.

Prelucrarea informațiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în safeuri și dulapuri, care sunt amplasate fizic în biroul SGMPJRP din sediul Judecătoriei Cimișlia.

Orice utilizare a datelor cu caracter personal parvenite în cadrul SGMPJRP, în alte scopuri este interzisă.

La expirarea termenului datele din cadrul secției sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip a termenelor de păstrare a acestora în instanțele judecătorești aprobat prin Hotărârea Consiliului Superior al Magistraturii nr. 377/19 din 31 iulie 2018.

4. DIRECȚIA EVIDENȚĂ ȘI DOCUMENTARE PROCESUALĂ

Sarcinile de bază și atribuțiile DEDP prin prisma respectării datelor cu caracter personal sunt:

- Asigurarea procesului de înregistrare operativă şi gestionare a documentelor la nivelul instanţei respectând Legea privind protecţia datelor cu caracter personal;
- Asigurarea circulaţiei operative a documentelor intrate în instanţă respectând Legea privind protecţia datelor cu caracter personal;
- Pregătirea răspunsurilor la interpelările cetăţenilor şi altor instanţe respectând Legea privind protecţia datelor cu caracter personal;
- Introducerea toată informaţia despre dosare parvenite în instanţa în Programul Integrat de Gestionare a Dosarelor;
- Primirea toate dosarele şi materiale de la grefieri verificând şi respectând normele de procedură şi Legea privind protecţia datelor cu caracter personal.

În cazul în care datele cu caracter personal nu sânt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informaţia privind categoriile de date care urmează a fi colectate sau dezvăluite.

Orice utilizare a datelor cu caracter personal parvenite în DEDP şi introduse în Programul Integrat de Gestionarea a Dosarelor în alte scopuri este interzisă.

Datele cu caracter personal conţinute în DEDP în cadrul Judecătoriei Cimişlia se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic;
- în PIGD

Calculator de birou nr. de inventariere - 31460015, 257(1I), 119, 31460016, 31460039, 31460017 calculatoarele aflându-se în birourile DEDP al Judecătoriei Cimişlia;

Prelucrarea informaţiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în safeuri şi dulapuri, care sunt amplasate fizic birourile DEDP al Judecătoriei Cimişlia.

Orice utilizare a datelor cu caracter personal parvenite în şedinţa de judecată sau în cadrul secţiei în alte scopuri este interzisă.

5. SERVICIUL INTREPREȚI ȘI TRADUCĂTORI

Sarcinile de bază și atribuțiile SIT prin prisma respectării datelor cu caracter personal sunt:

- Contribuirea la realizarea drepturilor şi libertăţilor justiţiabililor şi vizitatorilor instanţei, asigurând traducerea în/din limba rusă etc. a actelor judecătoreşti şi interpretarea la cererea participanţilor la proces în şedinţele de judecată.

Calculator de birou nr. de inventariere - 31460018 calculatoarul aflându-se în biroul SIT din sediul Central al Judecătoriei Cimişlia;

Orice utilizare a datelor cu caracter personal parvenite în şedinţa de judecată sau în cadrul SIT în alte scopuri este interzisă.

6. SERVICIUL FINANCIAR – ECONOMIC

Sarcinile de bază și atribuțiile SFE prin prisma respectării datelor cu caracter personal sunt:

In cadrul sistemului de evidenţă contabilă sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele şi patronimicul;

- numărul personal de identificare de stat (IDNP);
- data naşterii şi domiciliul;
- codul personal de asigurări sociale (CPAS):
- datele privind locul de muncă şi funcţia ocupată;
- mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;
- datele privind situaţia familială (la cererea solicitantului);
- numele, prenumele (după caz patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);
- datele pentru transferul pe contul bancar a plăţilor salariale şi a altor sume datorate cu titlu de indemnizaţii, compensaţii sau alte beneficii, după caz;
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizaţiei corespunzătoare;
- mărimea concretă a drepturilor salariale calculate, taxele şi impozitele aferente, inclusiv contribuţiile de asigurări sociale obligatorii de asistenţă medicală şi socială, şi alte sume datorate în virtutea legii sau contractului;
- după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.
- Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii şi care au impact asupra calculării plăţilor salariale, de exemplu: modificarea gradului de calificare a funcţionarilor publici, avansarea în treptele de salarizare, evaluarea performanţelor profesionale ale subdiviziunilor cu acordarea sporului pentru performanţă, vechimea în muncă în serviciul public;
- Calcularea salariilor lunare, în conformitate cu legislaţia în vigoare a Republicii Moldova (Legea nr. 270 din 23.11.2018 privind sistemul unitar de salarizare a în sectorul public);
- Prelucrarea certificatelor de concedii medicale ale angajaţilor în vederea stabilirii indemnizaţiilor corespunzătoare;
- Prelucrarea copiilor ordinelor preşedintelui/vicepreşedintelui referitoare la personal;
- Calcularea şi reţinerea taxelor ce ţin de plăţile salariale aferente angajaţilor: primele de asigurare obligatorie de asistenţă medicală, contribuţiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;
- Calcularea şi virarea primelor de asigurare obligatorie de asistenţă medicală şi a contribuţiilor la bugetul asigurărilor sociale de stat, aferente plăţilor salariale - obligaţie a angajatorului;
- Prezentarea trimestrială a rapoartelor la Biroul Naţional de Statistică privind efectivul de personal şi remunerarea muncii acestuia. Anual se prezintă rapoarte privind formarea profesională a angajaţilor şi cheltuielile efectuate în acest scop. Anual se prezintă rapoarte ce reflectă cheltuielile executate pentru întreţinerea mijloacelor de transport, TFD 19, precum şi cele de întreţinere a clădirii instituţiei(cheltuielile pentru energie electrică şi a gazelor naturale, consumul de combustibil), raportul Balanţa Energetică. - Prezentarea la Biroul Naţional de Statistică se prezintă de două ori pe an rapoarte privind fluxul de angajări şi eliberări ale personalului pe parcursul anului bugetar.

La Inspectoratul Fiscal se prezintă lunar rapoartele IPC-21,

- Prezentarea anuală raportul IALS14, privind salariul şi impozitul pe venit, precum şi calcularea primelor de asigurare obligatorie de asistenţă medicală şi calcularea contribuţiilor de asigurări sociale de Stat pentru fiecare angajat în parte.
- Prezentarea lunară a informaţiei privind creanţele cu termen expirat şi datoriile cu termen de prescripţie expirat formate în instanţa (Forma FD -049).
- raportul operativ privind statele şi efectivul de personal din instituţie (Forma FD-050).
- De asemenea serviciul financiar-economic întocmeşte şi prezintă instituţiei ierarhic superioare, CSM, trimestrial şi anual raportul activităţii serviciului. Acest raport conţine informaţii despre cheltuielile operaţionale şi efective ale instituţiei în această perioadă de gestiune. Rapoartele financiare sunt întocmite conform Normelor metodologice privind evidenţa contabilă şi raportarea financiară în sistemul bugetar, aprobat prin Ordinul ministrului finanţelor nr. 216 din 28.12.2015, cu modificările operate ulterior. Totodată se solicită să se asigure întocmirea şi prezentarea rapoartelor financiare în

termenele şi componenţa stabilite, să se reflecte integral în evidenţa contabilă a operaţiunilor economice efectuate în perioada de raportare, atât prin sistemul trezorerial, cât şi în afara acestuia (după caz), să se verifice raportul financiar cu Fişa executării contului curent(forma FD-037).

- Se întocmesc şi se prezintă inclusiv şi raportul narativ privind executarea bugetului conform ordinului ministrului de finanţe nr.164 din 30 decembrie 2016 cu privire la aprobarea Cerinţelor la întocmirea Raportului narativ privind executarea bugetelor în instituţiile bugetare. Rapoartele se prezintă în modulul CNFD şi pe suport de hârtie (imprimat din program). Prelucrarea cererilor şi a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reţinut din salariu. în conformitate cu capitolul 4. titlul II din Codul Fiscal;
- Eliberarea certificatelor de salariu, la cererea angajaţilor.

Datele cu caracter personal ce fac obiectul reglementării prezentei Politici vor fi stocate de către Serviciul Financiar Economic astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/şterge, în funcţie de suportul pe care au fost efectuate, în cazul obligaţiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.

Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidenţă contabilă în alte scopuri decât cele menţionate mai sus este interzisă.

Datele cu caracter personal conţinute în serviciu Serviciul Financiar Economic în cadrul Judecătoria Cimişlia se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic;
- Software - Sistemul de evidenţă contabilă în sfera bugetară l C: Buget, care este instalat la computerul central – „Contabil Şef", computerul aflându-se în biroul Serviciului Financiar Economic din sediul central al Judecătoriei Cimişlia.

Mentenanţa programului contabil IC: este efectuată de către „Centrul de tehnologii Informaţionale în Finanţe", fiind încheiat anual contract de voloare mică, privind prestarea serviciilor de deservire între Judecătoria Cimişlia şi „Centrul de tehnologii Informaţionale în Finanţe" cu următoarele atribuţii stabilite companiei prestatoare:

- Efectuarea ajustărilor în program, în baza modificărilor legislaţiei Republicii Moldova;
- Eliminarea erorilor în funcţionarea programului;
- Consultarea în rezolvarea dificultăţilor apărute în utilizarea programului ;
- Examinarea solicitărilor parvenite din partea Autorităţii Publice Judecătoria Cimişlia;
- Examinarea şi nedivulgarea informaţiei cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

Prelucrarea informaţiilor în sistemul de evidenţă contabilă pe suport de hârtie este structurată după criteriu "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în biroul Serviciului Financiar Economic din sediul central al Judecătoriei Cimişlia.

Calculator de birou nr. de inventariere-31460053, 31460135, computerul aflându-se în biroul Serviciului Financiar Economic din sediul central al Judecătoriei Cimişlia.

Prelucrarea informaţiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în biroul Serviciului Financiar Economic din sediul central al Judecătoriei Cimişlia.

Orice utilizare a datelor cu caracter personal în cadrul serviciu în alte scopuri este interzisă.

7. SERVICIUL RESURSE UMANE

Prin prisma respectării datelor cu caracter personal sunt în cadrul serviciului resurse umane sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele şi patronimicul;
- numărul personal de identificare de stat (IDNP);

- data naşterii şi domiciliul;
- codul personal de asigurări sociale (CPAS);
- datele privind locui de muncă şi funcţia ocupată;
- mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;
- datele privind situaţia familială (la cererea solicitantului);
- numele, prenumele (după caz. patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);
- certificatele de concediu medical acordate;
- certificate/copii ale actelor cu privire la datele personale ale personalului;
- baza de date computerizată privind funcţiile şi personalul autorităţii publice Judecătoria Cimişlia;
- după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.

Prelucrarea datelor cu caracter personal menţionate va fi efectuată pentru realizarea următoarelor scopuri:

- Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii şi care au impact asupra activităţii desfăşurate de funcţionarii publici de execuţie şi conducere de personalul ce deţine posturi în serviciu administrativ, de exemplu: modificarea gradului de calificare a funcţionarilor publici, avansarea în treptele de salarizare, evaluarea performanţelor profesionale ale subdiviziunilor cu acordarea sporului pentru performanţă, vechimea în muncă în serviciul public, acordarea premiului anual personalului care efectuează deservirea tehnică: Anual se prezintă rapoarte privind formarea profesională a angajaţilor.
- Calcularea salariilor lunare, în conformitate cu legislaţia în vigoare al Republicii Moldova (Legea nr. 270 din 23.11.2018 privind sistemul unitar de salarizare în sectorul bugetar);
- Înregistrarea certificatelor de concedii medicale ale angajaţilor;
- Elaborarea proiectelor de ordine preşedintelui/vicepreşedintelui referitoare la personal;
- Proiectele de acte administrative cu privire la angajare modificare/suspendare/încetarea raporturilor de serviciu/de muncă, evaluarea personalului;
- actualizarea dosarelor personale;
- certificate/copii ale actelor cu privire la datele personale ale personalului;
- completarea bazei de date computerizată (Registrului electronic al angajaţilor, Registrul al funcţionarilor publici) privind funcţiile şi personalul autorităţii publice Judecătoria Cimişlia;

Datele cu caracter personal ce fac obiectul reglementării prezentei Politici vor fi stocate de către specialistul principal al serviciului resurse umane, astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/şterge, în funcţie de suportul pe care au fost efectuate, în cazul obligaţiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.

Orice utilizare a datelor cu caracter personal, de către serviciul resurse umane în alte scopuri decât cele menţionate mai sus este interzisă.

Datele cu caracter personal conţinute în serviciul resurse umane în cadrul Judecătoriei Cimişlia se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic;
- Registru electronic al angajaţilor
- Registrul electronic al funcţionarilor publici.

Calculator de birou nr. de inventariere -31460021, computerul aflându-se în biroul Serviciului resurse umane din sediul central al Judecătoriei Cimişlia.

Prelucrarea informaţiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în safeuri şi dulapuri, care sunt amplasate fizic în Serviciului resurse umane din sediul central al Judecătoriei Cimişlia.

Prelucrarea datelor cu caracter personal de serviciu resurse umane se efectuează pe perioada activităţii angajaţilor Judecătoriei Cimişlia (din momentul emiterii Decretului Preşedintelui Republicii Moldova, Hotărârii CSM, ordinului cu privire la numirea în funcţie publică, din momentul semnării contractului de

muncă până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

La expirarea termenului (în cazul încetării raporturilor de muncă) datele din serviciu resurse umane sunt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor -tip a termenelor de păstrare a acestora în instanțele judecătorești aprobat prin Hotărârea Consiliului Superior al Magistraturii nr. 377/19 din 31 iulie 2018.

Orice utilizare a datelor cu caracter personal în cadrul serviciu în alte scopuri este interzisă.

8. SERVICIUL ARHIVĂ

Sarcinile de bază și atribuțiile Serviciului Arhivă prin prisma respectării datelor cu caracter personal sunt:

- Asigurarea ținerii evidenței, înregistrarea și eliberarea dosarelor și păstrarea documentației;
- Selectarea, prelucrarea și transmiterea dosarelor, documentelor la Arhiva Națională, anual asigură arhivarea și întocmește lista dosarelor și a documentației aflate în arhiva instanției;
- Asigurarea furnizării participanților la proces a informațiilor din dosare și copii de pe materialele dosarelor aflate în arhivă;
- Eliberarea în ordinea stabilită dosarele sau documentele colaboratorilor instanței;
- Ținerea evidența accesului/folosirii documentelor ce se păstrează în arhivă.
- Introducerea informației despre dosarele aflate în arhivă în Programul Integrat de Gestionare a Dosarelor.

Orice utilizare a datelor cu caracter personal în cadrul serviciu în alte scopuri este interzisă.

9. SERVICIUL EXPEDIȚIE

Sarcinile de bază și atribuțiile serviciului expediție prin prisma respectării datelor cu caracter personal sunt:

- Asigurarea securitatea și expedierea corespondenței înregistrate și a altor bunuri sau valori la destinatarii indicați prin intermediul oficiului poștal;
- Transmite, contra semnătură, corespondența înregistrată destinatarului din raza localității în care își are sediul instanța;
- Prelucrarea corespondenței expediate prin sortarea, adresarea, împachetarea, stabilirea costului de expediere, completarea formularelor poștale și predarea lor la oficiul poștal;
- Însoțește după caz, și remite instanțelor ierarhic superioare dosarele supuse căilor extraordinare de atac.

10. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

Judecătoria Cimișlia, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal .

În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în instanță.

Personalul implicat în activitatea de administrare și/sau prelucrare a informațiilor din cadrul Judecătoriei Cimișlia, vor respecta procedura de acces la datele cu caracter personal.

Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al președintelui/vicepreședintelui (managerul

Informațiile furnizate vor fi acordate astfel, în cât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

11. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ AL INSTANȚEI

- Auditul sistemelor informaționale gestionate

a) Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- Data și timpul tentativei intrării/ieșirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

b) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data și timpul tentativelor de obținere a accesului (de executare a operațiunilor);
- denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului, specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
- specificațiile resurselor protejate (identificator, nume logic, nume, fișier, număr etc.);
- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
- rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

- data și timpul modificării competențelor;
- ID-ul administratorului care a efectuat modificările;
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

d) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- data și timpul eliberării;
- denumirea informației și căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- ID-ul utilizatorului, care a solicitat informația.

- Asigurarea protecției contra programelor dăunătoare (virușilor):

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

Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal.

Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

- Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

b) Personalul Judecătoriei Cimișlia informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.

c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate.

- Obligațiile funcționarilor prin prisma respectării confidențialității datelor cu caracter personal.

În ceea ce privește asigurarea securității datelor cu caracter personal, funcționarii au următoarele obligații:

- de a consulta documentele sau dosarele aflate în instanță, având obligația de a respecta secretul de serviciu și de a proteja informațiile confidențiale la care au avut acces în măsura ce ține nemijlocit de activitatea secției;
- de a asigura securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copier;
- de a asigura securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate;
- de a respecta normele deontologice profesionale și legislația în vigoare.

12. CONTROL ȘI ÎMBUNĂTĂȚIRE

Persoana responsabilă va organiza anual un audit referitor la protecția datelor cu caracter personal.

Toate subdiviziunile Judecătoriei Cimișlia vor iniția acțiuni corective și preventive pentru a eficientiza procesele referitoare la protecția datelor cu caracter personal.

Toate subdiviziunile Judecătoriei Cimișlia vor asigura identificarea, protocolară și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor cu caracter personal, inclusiv protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

Toate subdiviziunile Judecătoriei Cimișlia vor face periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea echipamentelor și sistemelor de telecomunicații.

13. DISPOZIȚII FINALE

Prezenta Politică poate fi revizuită periodic, în funcție de modificările și completările legislative aplicabile, precum și de nivelul de dezvoltare tehnologică.

Politica este adusă la cunoștința angajaților contra semnătură.

Prezenta Politică intră în vigoare din momentul aprobării de către președintele Judecătoriei Cimișlia.

Întocmit:
Șefă a secretariatului Natalia MICULICI

(anexa nr. 1)
la Politica de securitate
privind protecția datelor cu caracter personal
în cadrul Judecătoriei Cimișlia
APROBAT
prin Ordin nr. 14
din 16.01.2025
Președinte interimar
Veronica CARAPIREA _____
L.Ș.

Atenție !!!

Accesul în perimetrul de securitate a clădirii Judecătoriei Cimișlia 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 nr. 133/2011 privind protecția datelor cu caracter personal, precum și pct. 26 din CERINŢELE faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobat prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010.

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.

(anexa nr. 2)
la Politica de securitate
privind protecția datelor cu caracter personal
în cadrul Judecătoriei Cimișlia
APROBAT
prin Ordin nr. 14
din 16.01.2025
Președinte interimar
Veronica CARAPIREA _____
L.Ș.

DECLARAȚIE

Eu_____, IDNP_____ am fost informat(ă) despre faptul că luarea, sustragerea, degradarea sau distrugerea ilegală a documentelor din dosar este interzisă şi atrage răspundere prevăzută de art. 360 Cod penal al Republiii Moldova.

Mi s-a comunicat despre faptul că studierea dosarelor, conform *Politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestoraîn cadrul sistemelor informaționale gestionate de către Judecătoria Cimișlia* aprobat prin Ordinul preşedintei interimare nr. 14 din 16 ianuarie 2025 *și Regulametul privind supravegherea prin mijloacele video în cadrul Judecătoriei Cimișlia* aprobat prin Ordinul preşedintei interimare nr. 15 din 16 ianuarie 2025, **se efectuează sub supravegherea colaboratorilor instanţei judecătoreşti sau într-o sală amenajată cu supraveghere video iar părăsirea instanţei cu dosare şi transmiterea dosarelor persoanelor terțe este strict interzisă tuturor justițiabililor.**

Totodată, mi s-a adus la cunoştinţă prevederile legale stipulate în Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal şi consecinţele respectării lor.

Data_____ Semnătura_____

(anexa nr. 3)
la Politica de securitate
privind protecția datelor cu caracter personal
în cadrul Judecătoriei Cimișlia
APROBAT
prin Ordin nr. 14
din 16.01.2025
Președinte interimar
Veronica CARAPIREA _____
L.Ș.

JUDECĂTORIA CIMIȘLIA

Republica Moldova, or. Cimișlia, str. C. Stamati, nr. 1
email: jcm@justice.md; Tel.: +373 024 122 364, 067104185

Nr._____ din _____2025

Pentru întocmirea mesajelor electronice:

„Prezentul mesaj constituie o informație confidențială, conține date cu caracter personal și este permisă spre utilizare doar destinatarului. În măsura în care nu sunteți destinatarul vizat, sunteți notificat prin prezenta că orice utilizare, copiere, diseminare sau distribuire a acestei informații este strict interzisă. În situația în care ați recepționat acest mesaj din greșeală, vă rugăm să ne notificați imediat prin răspuns la emailul recepționat și ulterior să ștergeți acest mesaj din sistem."

Pentru utilizarea la întocmirea documentelor:

Atenție! Documentul conține date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în scopul prevăzut de prezentul document și doar în condițiile statuate de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.