**APROBAT**

**prin ordinul Președintelui interimar al**

**Judecătoriei STRĂȘENI**

**nr. 103 din „17” 04 2024**

**Sergiu OSOIANU**

# POLITICA DE SECURITATE

## privind prelucrarea datelor cu caracter personal efectuată de către Judecătoria STRĂȘENI

## I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul entității sunt aplicate principiile prevăzute de **Actele Internaționale:**

- Convenția Consiliului Europei nr.108 pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal,

-Directiva 95/46/CE a Parlamentului European, Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date;

- Declarația Universală a Drepturilor Omului;

-Convenția pentru Apărarea Drepturilor Omului și a Libertăților Fundamentale;

**și a Legislației Naționale:**

- Constituția Republicii Moldova;

- Legea nr.133 din 07 iulie 2011 privind Protecția Datelor cu Caracter Personal;

- Legea nr. 148 din 09.06.2023 privind Accesul la Informație;

- Legea nr. 544-XII din 20 iulie 1995 cu privire la statutul judecătorului;

- Hotărârea 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;

-Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012 și alte acte legislative/normative de profil.

## II. INTRODUCERE

Judecătoria Strășeni are sediul înregistrat în mun. Strășeni, str. Ștefan cel Mare și Sfînt nr. 86, precum și sediul secundar în: or. Călărași, str. Alexandru cel Bun nr.153, Republica Moldova.

Politica de securitate este aprobată de către Președintele interimar al Judecătoriei Strășeni, domnul Sergiu Osoianu, care acționează în baza Legii nr. 514-XIII din 06 iulie 1995 cu privire la organizarea judecătorească.

Prezenta politică de securitate este aprobată, inclusiv, în vederea conformării Judecătoriei Strășeni 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", Legii Republicii Moldova nr.133 din 08.07.2011 "privind Protecția Datelor cu Caracter Personal", Legii nr. 148 din 09.06.2023 privind Accesul la Informațiile de Interes Public.

În ceea ce privește prelucrarea datelor cu caracter personal , protecția persoanelor fizice este un drept fundamental – art. 8 alin. (1) din Carta drepturilor fundamentale a Uniunii Europene („carta") și art. 16 alin. (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. NOȚIUNI GENERALE

Prezenta Politică de securitate:

- stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.

- asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, a dreptului acestora la protecția datelor cu caracter personal.

- se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

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

***terț*** – persoană fizică sau persoană juridică de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator și decât 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 și subdiviziunile ei teritoriale, căreia îi sânt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț. Nu sânt considerate destinatari organele din domeniul apărării naționale, securității statului și ordinii publice, organele de urmărire penală

şi instanţele judecătoreşti cărora li se comunică date cu caracter personal în cadrul exercitării competenţelor stabilite de lege;

***consimțământul subiectului de date cu caracter personal*** – manifestare de voință liberă, specifică, informată şi lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

***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 şi forță 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 performanța la locul de muncă, situația economică, sănătatea, preferințele, interesele, fiabilitatea, comportamentul, locul în care se află persoana respectivă şi deplasările acesteia.

***autentificare*** - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

***control de securitate*** - acțiuni întreprinse de către Judecătoria Străşeni în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale şi/sau registrelor ținute;

***fișiere temporare*** - ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

***identificare*** - atribuirea unui identificator subiecților şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

***integritate*** - certitudinea, ne contradictorialitatea şi actualitatea informației care conține date cu caracter personal, protecția ei de distrugere şi modificare neautorizată;

***mijloace de protecție criptografică a informației care conține date cu caracter personal*** — mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea şi confidențialitatea informației în procesul de prelucrare, depozitare şi 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 şi față de drepturile şi libertățile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

***regulament de securitate a datelor cu caracter personal*** - document, elaborat de către operatorul de date – Judecătoria Străşeni, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sânt expuse acestea;

***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 şi de elaborarea, implementarea şi 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;

***purtător 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 până la momentul pierderii sau distrugerii acestora;

***tehnologie informațională*** - totalitatea metodelor, procedeelor 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 până la momentul opririi acestora;

Scopul prezentei politici este asigurarea protecției drepturilor și libertăților fundamentale ale persoanei fizice în ceea ce privește prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieții intime, familiale și private. De asemenea, acesta presupune întărirea disciplinei muncii, folosirea rațională și eficientă a muncii în cadrul instanței de judecată și nu în ultimul rând respectarea legislației Republicii Moldova.

## IV. OBIECTIVELE POLITICII DE SECURITATE

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de Judecătoria Strășeni, atât în cadrul prelucrării manuale, cît și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul Judecătoriei Strășeni. Baza unei securități IT adecvate o constituie respectarea prezentului 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, sau care pot duce la încălcări ale legislației. Având 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.

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

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

## V. DISPOZIȚII PRIVIND IERARHIA ȘI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE

Operatorul de date cu caracter personal reieșind din specificul activității, prin prezenta Politică de securitate, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

Politica de securitate a datelor cu caracter personal se va revizui cel puțin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității, 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, 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, va fi desemnată persoana 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 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 Preşedintelui Judecătoriei Străşeni 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 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 sânt 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.

## VI. MIJLOACELE SUPUSE PRINCIPIILOR DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

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

Sânt 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:

- suport de hârtie;

- suporturi 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.

## VII.MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN CADRUL JUDECĂTORIEI STRĂŞENI

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

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării 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 atât pe suport de hârtie cât și cel în format electronic.

Măsurile generale de administrare a securității informaționale în cazul neutilizării temporare a purtătorului de informație pe suport de hârtie sau electronic care conțin date preluate din cadrul Judecătoriei Strășeni, aceștia se păstrează în safeuri care se închide.

La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.

Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.

Accesul fizic la mijloacele de reprezentare a informației preluate din subdiviziuni al instanței este blocat împotriva vizualizării de către persoane neautorizate.

Mijloacele de prelucrare a informațiilor preluate din subdiviziunile al instanței sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din cadrul instanței din/în perimetrul de securitate se înregistrează în registru.

Măsurile de protecție a datelor cu caracter personal, prelucrate în cadrul instanței, se înfăptuiesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

Cerințe speciale față de marcare: toate informațiile ieșite din instanța, care conțin date cu caracter personal, sunt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

Accesul în biroul unde sunt amplasate subdiviziunile instanței este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program.

Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.

Birourile nu sunt lăsate niciodată fără supraveghere la ieșirea în exterior, ușa birourilor se încuie cu lacătul.

Înainte de acordarea accesului fizic, se verifică competențele de acces.

Registrul de monitorizare se păstrează minim un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.

Zilnic, se inspectează perimetrul de securitate al clădirii și al birourilor instanței, din punct de vedere fizic.

Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

Ușile și ferestrele sunt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

Amplasarea subdiviziunilor instanței, răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității instanței, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale,

de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele de evidență a subdiviziunilor instanței, inclusiv posibilitatea deconectării oricărui component TI.

Computerele instanței dispun de UPS-uri, care sunt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaționale.

Securitatea anti incendiară a sistemului instanței este dotat cu echipament anti incendiar și corespunde cerințelor și normelor anti incendiare în vigoare.

Controlul instalării și scoaterii componentelor Tehnologiilor Informaționale se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul instanței.

La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

Măsurile de securitate pentru protecția tehnologiilor informaționale sunt implementate în conformitate cu legislația în vigoare privind protecția datelor cu caracter personal.

## VIII. PROTECȚIA DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE SE EFECTUEAZĂ PRIN URMĂTOARELE METODE:

- preîntâmpinarea 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;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program,
- preîntâmpinarea 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,
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN,
- preîntâmpinarea 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,
- preîntâmpinarea 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 atât pentru utilizatorii interni cât și pentru cei externi.

## IX. PROCEDURILE ORGANIZATORICE ŞI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL JUDECĂTORIEI STRĂŞENI 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 hârtie 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 sânt 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) Este asigurată securitatea şi 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 sânt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
f) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
g) 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 sânt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
b) Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.
c) Perimetrul de securitate a Judecătoriei Străşeni reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal.
d) Perimetrul clădirii sau încăperilor în care sânt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sânt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.
e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
f) Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
h) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii.

### 3. Identificarea şi autentificarea utilizatorilor:

a) Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.
b) Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal

(ID-ul utilizatorului), care nu conține semnalmentele nivelului de accesibilitate al utilizatorului.

c) Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrie 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 primite 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. Identificarea și autentificarea echipamentului.**

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă îndelungată.

**5. Administrarea identificatorilor utilizatorilor:**

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator,
- verificarea autenticității fiecărui utilizator.

**6. 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 sânt prezente indiciile eventualei compromiteri a sistemului sau parolei,
- alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sânt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sânt compuse integral din grupuri de cifre sau litere,
- modificarea parolelor peste intervale de 3 luni,
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

**7. Controlul administrării accesului**

Este efectuat controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

**8. Accesul de la distanță**

a) Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizând-se VPN, criptarea, cifrarea etc.), precum și sânt 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 Judecătoriei Strășeni și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

**9. 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 ale Judecătoriei Strășeni.

**10. Securitatea electroenergetică**

a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe specializate.

b) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

c) Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sânt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

**11. Controlul instalării și scoaterii componentelor T.I.**

a) Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

b) Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire.

**12. Dezvăluirea datelor cu caracter personal**

a) Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidentă, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidentă a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere *(expediere poștală cu aviz recomandat, înmânarea personală, etc.)*.

b) Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor, *(spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.)*sânt interzise.

c) Sânt interzise operațiunile de dezvăluire a datelor cu caracter personal între Judecătoria Strășeni și alte entități care sunt amplasate geografic în stingă Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal.

d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi

reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție 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 protecția datelor cu caracter personal, se permite și se realizează, ținând cont de principiul liberei circulații a datelor.

f) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței contabile, este limitat la strictul necesar pentru realizarea scopurilor declarate.

g) Acces la sistemele informaționale gestionate în cadrul Judecătoriei Strășeni, din partea Procuraturii Generale *(după caz procuraturile teritoriale/specializate)*, Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și 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 circumstanțe care au importanță pentru cauză, *(inclusiv informația stocată în auditul sistemelor informaționale și de evidență)*, 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 și răspândite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație 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 instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Urmează a ține cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. $74^1$ Cod contravențional.

## 13. Drepturile subiecților de date cu caracter personal

a) În cazul în care datele cu caracter personal sânt 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 căror 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 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 externalizare 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 urmând 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 sânt 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 sânt conectate la internet, nu sânt 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 sânt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Judecătoriei Străşeni.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie 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 obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
- data și timpul tentativei de obținere a accesului (executate a operațiunii),
- denumirea (identificatorul) aplicației sau procesului, ID-ul utilizatorului,
- specificațiile resursei 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.

**16. 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.

**17. 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).

**18. 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 Strășeni 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.

d) 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.

**19. Marcarea documentelor**

Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

***MODEL:*** Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr.__-___, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date

poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

**20. 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, semnatari a anexei nr. 1, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. $74^1$ Cod contravențional) și penală (art.art. 177, 178, 180 Cod penal).