APROBAT:

Prin Ordinul nr.103 din 17 aprilie 2024

Președintele interimar al Judecătoriei Strășeni

Sergiu OSOIANU _____

REGULAMENTUL PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA MANUAL ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE JUDECĂTORIA STRĂȘENI

I. INTRODUCERE

Judecătoria Strășeni abilitată prin Lege judecă cauzele în limitele competenței sale. Activitatea instanței judecătorești în domeniul înfăptuirii justiției este condusă de către Președintele instanței și/sau Vicepreședintele care exercită funcțiile președintelui instanței de judecată în cazul absenței acestuia.

Activitatea organizatorică și cea administrativă a instanței judecătorești este asigurată de secretariatul instanței, condus de către un șef numit în funcție de către președintele instanței. Structura Judecătoriei Strășeni include Judecători și Secretariatul instanței constituit din grefă și serviciul administrativ.

Grefa secretariatului include subdiviziunile: asistenți judiciari și grefierii; serviciul sistematizare, monitorizare a practicii judiciare și relații cu publicul; secția evidență și documentare procesuală; serviciul interpreți și traducători.

Serviciul administrativ al secretariatului include: serviciul financiar economic; serviciul resurse umane, serviciul tehnologii informaționale; serviciul expediere; serviciul arhivă; serviciul asigurare tehnico-materială.

Prezentul Regulament stabilește regulile de prelucrare și protecție a datelor cu caracter personal în cadrul sistemelor informaționale gestionate de Judecătoria Strășeni.

Documentele de referință:

- Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a deciziei-cadru 2008/977/JAI a Consiliului;
- Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal;
- Legea nr. 514/1995 cu privire la organizarea judecătorească;
- Legea nr. 158 din 04.07.2008 din cu privire la funcția publică și statutul funcționarului public.
- Legea nr. 544-XII din 20 iulie 1995 cu privire la statutul judecătorului;
- Legea nr. 148 din 09.06.2023 privind accesul la informațiile de interes public;
- Legea nr. 325 din 23.12.2013 privind testarea integrității profesionale;
- Legea nr. 82/2017 privind integritatea;
- Legea nr. 59/2007 privind statutul și organizarea activității grefierilor din instanțele judecătorești;
- Legea nr. 241/2007 privind comunicațiile electronice;
- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
- Legea nr. 467/2018 cu privire la informatizarea și la resursele informaționale de stat;
- Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
- Legea nr. 64/2010 cu privire la libera exprimare;
- Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar;
- Legea nr. 131/2015 privind achizițiile publice;
- Legea nr. 186/2008 securității și sănătății în muncă;
- Hotărârea Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
- Hotărârea Guvernului nr. 822/2012 cu privire la serviciile sistemului de poștă electronică al autorităților administrației publice;
- Decizia CNPDCP nr. 581/2015 cu privire la aprobarea formularului tipizat de informare privind efectuarea supravegherii prin mijloace video;
- Regulamentul CSM nr. 503/17/2014 cu privire la ordinea internă a instanțelor judecătorești;
- Instrucțiunea CSM nr. 142/4/2014 cu privire la activitatea de evidență și documentare procesuală în judecătorii și Curți de apel.

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale au drept scop stabilirea regulilor de implementare a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal.

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

- *prevenirii scurgerii, extragerii, dezvăluirii prin transmiterii a informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;*
- *prevenirii distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele neadmiterea accesului neautorizat terţilor a informaţiei cu accesibilitate limitată;*
- *eficientizarea resurselor informaţionale atât pe suport de hârtie, cât şi în format electronic;*

II. SCOPUL

Scopul prezentului Regulament este de a asigura protejarea şi garantarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal.

Judecătoria Străşeni prelucrează date cu caracter personal în scopul exercitării atribuţiilor prevăzute de lege, ceea ce priveşte desfăşurarea activităţii de judecată precum şi a altor activităţi de natură administrativă (în special, cele vizând resursele umane).

III.CADRUL INSTITUŢIONAL PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN SISTEMUL INFORMAŢIONAL

Judecătoria Străşeni recunoaşte şi respectă dreptul la viaţă intimă, familială şi privată, prelucrarea datelor cu caracter personal desfăşurându-se în conformitate cu prevederile legale în vigoare.

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 menite să asigure confidenţialitatea şi securitatea datelor cu caracter personal, după cum urmează:

Datele cu caracter personal care fac obiectul prelucrării vor fi:

Criptarea datelor- utilizarea algoritmilor de criptare pentru a proteja datele stocate şi transmise. Criptarea poate fi folosită pentru datele în tranzit şi pentru cele în repaus.

Controlul accesului- implementarea unor mecanisme riguroase de control al accesului la date, cu autentificare multi-factorială şi politici de autorizare clare.

Protecţia împotriva ameninţărilor cibernetice- utilizarea unor soluţii de securitate IT, cum ar fi firewall-uri, sisteme de detecţie a intruziunilor, antivirus şi anti-malware.

Actualizări regulate de securitate- păstrarea sistemelor şi a software-ului actualizate cu cele mai recente patch-uri de securitate pentru a remedia vulnerabilităţile cunoscute.

Back-up şi recuperare a datelor - implementarea unui sistem robust de backup pentru a asigura că datele pot fi recuperate în cazul unui incident de securitate sau a unei pierderi accidentale de date.

Politici şi proceduri de securitate- dezvoltarea şi implementarea unor politici şi proceduri de securitate clare şi corespunzătoare pentru angajaţi, inclusiv instruirea lor în privinţa acestora.

Monitorizarea şi auditarea sistemelor -monitorizarea constantă a sistemelor pentru detectarea activităţilor neobişnuite sau a potenţialelor încălcări de securitate, precum şi realizarea de audituri periodice pentru a evalua conformitatea cu politicile de securitate.

Protecţia împotriva pierderii de date -implementarea unor măsuri de prevenire a pierderii de date, cum ar fi sistemele de prevenire a scurgerii de date şi politici de protecţie a datelor.

Securitate fizică - protejarea infrastructurii fizice care găzduieşte datele, cum ar fi centrele de date, prin utilizarea sistemelor de control al accesului, supraveghere video şi alte măsuri de securitate.

Testare şi evaluare a securităţii- realizarea de teste periodice de penetrare şi evaluări a securităţii pentru identificarea şi remedierea potenţialelor vulnerabilităţi.

Utilizatorii vor avea acces la informaţiile ce conţin date cu caracter personal conform rolului atribuit în raport cu funcţia deţinută şi competenţele statuate în fişa postului şi/sau alt act.

Intrarea/accesul în sistemul informațional are loc prin: logarea persoanei responsabile, introducerea parolei de conectare, cunoscută doar de către utilizator și schimbată periodic. Parola de intrare/acces urmează că cuprindă cel puțin 8 caractere. La demisionarea persoanei, accesul (cheița de intrare) în sistemul informațional este transmis persoanei responsabile.

La încheierea operațiunilor de prelucrare, datele cu caracter personal se vor stoca în Arhiva Judecătoriei Strășeni și/sau în sistemul informațional de date cu caracter personal al Judecătoriei Strășeni conform Indicatorului documentelor-Tip și a termenelor de păstrare a acestora pentru instanțele judecătorești din Republica Moldova, aprobat prin Hotărârea CSM nr. 377/19 din 31 iulie 2018; explicații privind aplicarea Indicatorului, nomenclatorului intern al arhivei de predare a dosarelor la arhiva raională și regulamentelor/instrucțiunilor privind activitatea arhivei aprobate de operator.

La expirarea termenului de stocare, datele cu caracter personal vor fi distruse în modul stabilit de lege.

IV. PROCEDURA DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Procedura prelucrării datelor cu caracter personal prevede măsuri tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării confidențialității datelor și a informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității executate de angajații Judecătoriei Strășeni.

Prelucrarea datelor cu caracter personal se poate realiza cu sau fără utilizarea de mijloace automatizate în cadrul unor operațiuni ori seturi de operațiuni, fără a fi limitate la acestea, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Colectarea presupune acțiunea de a strânge, a aduna, a primi date cu caracter personal de la persoanele vizate prin intermediul subdiviziunilor Judecătoriei Strășeni.

Înregistrarea presupune consemnarea datelor cu caracter personal într-un sistem de evidență automată ori neautomată, care poate fi registru, fișier automat, bază de date sau orice altă formă de evidentă organizată, structurată ori ad-hoc sau într-un text, înșiruire de date ori document, indiferent de modalitatea în care se înscriu datele.

Organizarea presupune ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuțiilor legale în scopul eficientizării/optimizării activităților de prelucrare a acestora.

Stocarea presupune păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea unor copii de siguranță.

Adaptarea presupune transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate.

Modificarea presupune actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate si actualitate.

Extragerea presupune scoaterea unei parți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separate și distinct de prelucrarea inițială.

Consultarea presupune examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioară.

Utilizarea presupune folosirea datelor cu caracter personal, în totalitate sau în parte, de către și în interiorul Judecătoriei Strășeni, inclusiv prin tipărire, copiere, multiplicare, scanare sau alte procedee similare.

Dezvăluirea presupune acțiunea de a face disponibile datele cu caracter personal către terți prin comunicare, transmitere, diseminare sau în orice alt mod.

Alăturarea presupune acțiunea de adăugare, alipire sau anexare a unor date cu caracter personal la cele deja existente, pe care nu le modifică.

Combinarea presupune îmbinarea, unirea sau asamblarea unor date cu caracter personal separate inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate.

Restricționarea presupune limitarea accesului la datele cu caracter personal pentru o perioadă determinată, pentru scopuri anume determinate.

Ştergerea presupune eliminarea sau înlăturarea, în totalitate sau în parte, a datelor cu caracter personal din evidente sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența ori inexactitatea acestora.

Transformarea presupune operațiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea în scopuri exclusiv statistice.

Distrugerea presupune aducerea la starea de neîntrebuințare, în condițiile legii, definitivă și irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

V. MĂSURI DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE ÎN CADRUL JUDECĂTORIEI STRĂȘENI

Măsurile de protecția 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 purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din cadrul Judecătoriei Strășeni, aceştia se păstrează în safeuri care se încuie.

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

Operatorul asigură securitatea punctelor de primire şi expediere a corespondenței, precum şi 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 instanței sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

Scoaterea şi 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 şi integrității acestora, prin protecție în formă manuală, electronică şi externă.

Cerințe speciale față de marcare: toate informațiile ieşite din instanța, care conțin date cu caracter personal, sunt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară şi 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 şi doar în timpul orelor de program.

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

Birourile nu sunt lăsate niciodată fără supraveghere la ieşirea în exterior, uşa 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 şi documentele ce se conțin în registrul supus lichidării se transmit în arhivă.

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

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

Uşile şi 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 TI 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.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să corespundă necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este interzisă, cu excepția permisiunii speciale a administrației securitate este admisă doar în cazul prezenței unei permisiuni speciale a administrației.

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

În scopul elucidării tentativelor de acces neautorizat, 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:

a) data și timpul tentativei de obținere a accesului (executare a operațiunii),
b) denumirea (identificatorul) aplicației sau procesului, a ID-ului utilizatorului,
c) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
d) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
e) rezultatul tentativei de obținere a accesului - pozitivă sau negativă.

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.

<u>Persoana responsabilă de politica de securitate a datelor cu caracter personal:</u>

a) 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;

b) va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal;

c) va asigura instruirea persoanelor 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.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va informa imediat administrația despre orice caz de încălcare a normelor de securitate și va lua măsuri de restabilire a securității.

În cazul în care operatorul este autoritate publică ori instituție publică, poate fi desemnată o persoană responsabilă cu protecția datelor unică pentru mai multe dintre aceste autorități sau instituții, luând în considerare structura organizatorică și dimensiunea acestora.

Persoana responsabilă de protecția datelor are obligația de a respecta secretul sau confidențialitate privind îndeplinirea sarcinilor, în conformitate cu actele normative.

Persoana responsabilă cu protecția datelor poate îndeplini și alte sarcini și atribuții.

Persoana responsabilă cu protecția datelor are cel puțin următoarele sarcini:

a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrarea datelor cu privire la obligațiile care le revin în temeiul Legii nr. 133 din 08.07.2011 și a altor acte normative;
b) monitorizarea respectării Legii nr. 133 din 08.07.2011 și a altor acte normative referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, precum și atribuirea responsabilităților, inclusiv privind acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare și privind auditurile aferente;
c) oferirea consilierii la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
d) cooperarea cu Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova;
e) asumarea rolului de punct de contact pentru Centrul Național pentru Protecția Datelor cu Caracter Personal privind aspectele legate de prelucrarea datelor, inclusiv consultarea prealabilă, precum și, după caz, consultarea cu privire la alte chestiuni.

VI. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORILOR INFORMAȚIILOR PRELUATE DIN SISTEMELE INFORMAȚIONALE

Toți utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Este interzisă înscrierea parolelor pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acesteia (în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

Parolele urmează a fi modificate de fiecare dată când există suspiciunea compromiterii sistemului sau a parolei. Parolele vechi se păstrează în arhivă, fără a mai fi folosite repetat.

Numărul încercărilor de autentificare la informațiile cu caracter personal trebuie limitat la 3.

În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 01 luni), codurile de identificare și autentificare se revocă sau se suspendă.

În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuiește cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale acestuia.

Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.

Orice incident de securitate se raportează/comunică conducătorului persoanei responsabile și ulterior după ce s-a întreprins acțiuni de cercetare sau documentare și autorității de protecție a datelor cu caracter personal.

Înainte de acordarea accesului la datele cu caracter personal, utilizatorii sunt informați despre faptul că este supus auditării fiecărei accesări a datelor cu caracter personal și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională sau penală.

VII. PRINCIPII DE BAZĂ

La prelucrarea datelor cu caracter personal vor fi respectate principiile:

Legalitate, echitate și transparență – datele cu caracter personal vor fi prelucrate în mod legal, echitabil și transparent față de persoana vizată.

Limitări legate de scop – datele cu caracter personal vor fi colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

Reducerea la minimum a datelor – datele cu caracter personal vor fi adecvate, relevante si limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

Exactitate – datele cu caracter personal vor fi exacte și, în cazul în care este necesar, actualizate.

Limitări legate de stocare – datele cu caracter personal vor fi păstrate într-o formă care permite identificarea persoanei vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

Integritate și confidențialitate – datele cu caracter personal vor fi prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de masuri tehnice sau organizatorice corespunzătoare.

VIII. 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 informații, exceptând cazul în care acesta deține deja informațiile respective:

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

Informații suplimentare, precum:

- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor de acces la date, de intervenție asupra datelor și de opoziție, precum și condițiile în care acestea pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sânt obligatorii sau voluntare, precum și consecințele 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 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.

IX. SISTEMUL INFORMAȚIONAL

Sistemul Informațional Judiciar (SIJ) este constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii aflate în interconexiune, destinat înregistrării, prelucrării, utilizării, păstrării informațiilor cu privire la cererile de chemare în judecată și dosarelor instanțelor de judecată din momentul înregistrării până în momentul arhivării și publicării.
SIJ dispune de mai multe componente cum sunt: Programul Integrat de Gestionare a Dosarelor (PIGD); Soluția Informatică e-Dosar (SI-e-DJ); Portalul Național al Instanțelor de Judecată (PNIJ); Soluția Informatică a ședințelor de judecată (SI a S) videoconferința, înregistrarea audio /video a ședințelor de judecată.

În SIJ personalul Judecătoriei Strășeni prelucrează date cu caracter personal a justițiabililor, persoanelor fizice/și sau reprezentanții persoanelor juridice care au depus spre examinare cereri de chemare în judecată și/sau sunt participanți pe dosarele examinate în cadrul judecătoriilor și instanței de apel, date cu privire la angajații-utilizatori a PIGD.

Tipurile de date cu caracter personal prelucrate în SIJ se referă la: IDNP (preluat din Registrul de stat al populației); Prenume; Nume; Patronimic; Data nașterii; Gen; Minor (Da/Nu); Adresa (preluat din Registrul de stat al populației); Adresa înregistrată în SIJ; Ocupația; Locul de muncă; Educația; Calitatea procesuală; Informații judiciare cu caracter personal (Date cu privire la dosarele în care este și sau a fost implicat, actele judecătorești în care este vizat, informații despre ședința de judecată, înregistrări audio); Loghin (pentru beneficiarii SIJ, utilizatori ai componentei e-Dosar); Adresa IP

(pentru beneficiarii SIJ, utilizatori ai componentei e-Dosar); Telefon fix/mobil, e-mail serviciu/personal; Dreptul de acces în sistem (cu drept de acces în sistem /fără drept de acces în sistem); Statut în sistem (Activ/Inactiv).

X. RESPONSABILITATEA PERSONALULUI INSTANȚEI

Operatorul de date cu caracter personal reieşind din specificul activității, prin prezentul Regulament, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul instanței.

Persoanele responsabile desemnate, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor regulamentului de securitate, se va subordona nemijlocit Preşedintelui (managerul) Judecătoriei Strășeni sau persoanei care îndeplineşte interimatul funcției.

Persoana responsabilă de regulamentul de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilități 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 regulamentul de securitate a datelor cu caracter personal va defini clar responsabilitățile şi procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională şi de funcționare generală, va asigura măsuri tehnice şi 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 şi asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

XI. ATRIBUȚIILE ANGAJAȚILOR JUDECĂTORIEI STRĂȘENI SECRETARIATUL JUDECĂTORIEI

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

- Monitorizarea bazei de date computerizată (Registrului electronic al angajaților, Registrul al funcționarilor publici); privind funcțiile şi personalul autorității publice Judecătoriei Strășeni;
- Asigurarea activității administrativă şi organizatorică a instanței.
- Coordonarea procesului de elaborare a planurilor de activitate şi a programelor de dezvoltare strategică ale instanței.
- Asigurarea gestionarea mijloacelor financiare alocate instanței judecătoreşti.
- Coordonarea procesului de asigurare a instanței judecătoreşti cu personalul, menținerea şi dezvoltarea acestuia

Datele cu caracter personal conținute în cadrul secretariatului Judecătoriei Strășeni se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic.

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 judecătoreşti 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.

XII. GREFA SECRETARIATULUI JUDECĂTORIEI ASISTENTI JUDICIARI şi GREFIERI

Asistenți judiciari şi grefieri prelucrează date cu caracter personal, pe suport de hârtie, în format electronic prin intermediul componentelor SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD); Soluția Informatică e-Dosar (SI-e-DJ); Portalul Național al Instanțelor de Judecată (PNIJ); Soluția informatică a şedințelor de judecată (SI a S) videoconferință, înregistrarea audio /video a şedințelor de judecată, în cadrul proceselor de lucru: Colectarea actelor normative necesare judecătorului şi altă

informație necesară pentru judecarea dosarului distribuit judecătorului; Generalizarea problemelor de drept în dosarele distribuite judecătorului; Verificarea prezenței actelor care urmau a fi prezentate de către participanți; Elaborarea proiectelor de acte judecătorești; Asigurarea accesului la dosar a participanților la proces; Afișarea pe panoul informativ a listelor cauzelor numite spre soluționare; Expedierea citațiilor participanților la proces; Înregistrarea audio a ședințelor de judecată; Asigurarea petrecerii ședințelor prin utilizarea sistemului de videoconferință; Întocmirea procesului-verbal în ședința de judecată; Perfectarea dosarelor după judecare și prezentarea SEDP; Introducerea datelor în PIGD.

Asistenții judiciari și grefierii prelucrează categorii de date cum sunt: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data nașterii și domiciliul; Codul personal de asigurări sociale (CPAS); Date privind locul de muncă și funcția ocupată; Gen; Minor (Da/Nu); Adresa (preluat din RSP); Adresa înregistrată în SIJ; Ocupația; Educația; Calitatea procesuală; Funcție; Telefon fix/mobil, e-mail serviciu/personal; Salariul brut, premii, sporuri, stimulări, suplimente; Numele, prenumele (după caz patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz); Certificate de concediu medical acordat (datele din certificate); certificate/copii ale actelor cu privire la datele personale; Date pentru transferul pe cont bancar plăților salariale și a altor sume datorate cu titlul de indemnizație, compensație, sau alte beneficii după caz; Mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuții, asigurări sociale obligatorii de asistență medicală și socială, alte sume în virtutea legii; Informații judiciare cu caracter personal (date cu privire la dosarele în care este și/sau a fost implicat, actele judecătorești în care este vizat, informații despre ședința de judecată, înregistrări audio).

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Utilizarea datelor cu caracter personal în alte scopuri decît cele prevăzute în activitate; Prelucrarea datelor cu caracter personal în mod accidental sau ilegal. Distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal. Accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod decît cel prevăzut. Acte judecătorești depersonalizate necorespunzător. Anonimizarea datelor efectuată incomplet.

Activități de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Realizarea sistematică a controlului de către managerii operaționali. Asigurarea participării la instruiri organizate în acest sens. Asigurarea depersonalizării prin verificare, realizarea sistematică a controlului de către managerii operaționali. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal.

SECȚIA GENERALIZARE, SISTEMATIZARE, MONITORIZARE A PRACTICII JUDICIARE ȘI RELAȚII CU PUBLICUL

Secția generalizare, sistematizare, monitorizare a practicii judiciare și relații publice (SGSMPJRP) prelucrează date cu caracter personal, pe suport de hîrtie, în format electronic în cadrul proceselor de lucru: Generalizarea practicii judiciare referitoare la anumite categorii de pricini; Întocmirea și analiza statisticii judiciare; Înregistrarea și pregătirea răspunsurilor la petiții; Pregătirea materialelor cu privire la activitatea judecătorului; Asigurarea activității prin intermediul poștei electronice, pagina web a instanței.

Funcționarii publici de conducere și execuție (șef secție, specialiști principali, superiori) din cadrul secției SGSMPJRP prelucrează categorii de date cum sunt: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data nașterii și domiciliul; Date privind locul de muncă și funcția ocupată; Gen; Minor (Da/Nu); Adresa; Ocupația; Educația; Calitatea procesuală; Funcție; Telefon fix/mobil, e-mail serviciu/personal.

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal. Prelucrarea datelor cu caracter personal în mod accidental sau ilegal. Utilizarea datelor cu caracter personal în alte scopuri decît cele prevăzute în activitate. Accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod decît cel prevăzut.

Activități de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Realizarea

sistematică a controlului de către managerii operaționali. Asigurarea participării la instruiri organizate în acest sens.

SECȚIA EVIDENȚĂ ȘI DOCUMENTARE PROCESUALĂ

Secția evidență și documentare procesuală (SEDP) prelucrează date cu caracter personal, pe suport de hîrtie, în format electronic, prin intermediul componentelor SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD); Soluția Informatică e-Dosar (SI-e-DJ), în cadrul proceselor de lucru: Înregistrarea corespondenței instanței de judecată; Efectuarea acțiunilor cu referire la executarea hotărârilor judecătorești; Înregistrarea dosarelor în PIGD și fișa acțiunii; Evidența dosarelor aflate în procedura de examinare; Asigurarea accesului la materialele dosarului; Eliberarea copiilor din materialele dosarului și copiilor înregistrărilor audio a ședințelor de judecată; Întocmirea rapoartelor statistice generate din PIGD; Transmiterea dosarelor și materialelor în arhivă; Expedierea dosarelor examinate în instanțele ierarhic superioare.

Funcționarii publici de conducere și execuție (șef secție, specialiști principali, superiori) din cadrul secției prelucrează următoarele date cu caracter personal: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data nașterii și domiciliul; Date privind locul de muncă și funcția ocupată; Gen; Minor (Da/Nu); Adresa înregistrată în SIJ; Ocupația; Educația; Calitatea procesuală; Funcție; Telefon fix/mobil, e-mail serviciu/personal; Numele, prenumele (după caz patronimicul) persoanelor care se află la întreținerea persoanei (membrii familiei, alte rude și persoane, după caz); Date privind achitarea taxei de stat și taxei de timbru; Informații judiciare cu caracter personal (date cu privire la dosarele în care este și/sau a fost implicat, actele judecătorești în care este vizat, informații despre ședința de judecată, înregistrări audio).

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Prelucrarea datelor cu caracter personal în mod accidental sau ilegal. Distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal. Accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod decît cel prevăzut.

Activități de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Realizarea sistematică a controlului de către managerii operaționali. Asigurarea participării la instruiri privind prelucrarea datelor cu caracter personal.

SERVICIUL INTREPREȚI ȘI TRADUCĂTORI

Serviciul translare (ST) prelucrează date cu caracter personal, pe suport de hîrtie, în cadrul proceselor de lucru: Asigurarea respectării drepturilor participanților la proces și accesul acestora la justiție; Efectuarea traducerii în ședința de judecată pentru persoanele care nu posedă sau nu vorbesc limba de stat; Efectuarea traducerii hotărârilor și altor materiale solicitate de participanții la proces; Confirmarea prin semnătură a caracterului complet și exact al traducerii incluse în procesul verbal al ședinței de judecată la care participă, precum și exactitatea traducerii documentelor care se înmânează persoanelor participante la procesul de judecată.

Funcționarii publici de execuție (specialiști principali, superiori) din cadrul serviciului ST prelucrează categoriile de date cu caracter personal: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data nașterii și domiciliul; Date privind locul de muncă și funcția ocupată; Gen; Minor (Da/Nu); Adresa; Ocupația; Educația; Calitatea procesuală; Informații judiciare cu caracter personal (date cu privire la dosarele în care este și/sau a fost implicat, actele judecătorești în care este vizat, informații despre ședința de judecată, înregistrări audio).

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Utilizarea datelor cu caracter personal în alte scopuri decît cele prevăzute în activitatea sa; Expedierea informației ce conține date cu caracter personal altui destinatar;

Activități de control: Respectarea legislației în vigoare privind protecția datelor cu caracter personal; Realizarea sistematică a controlului de către managerii operaționali. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Participarea la instruiri.

SERVICIUL FINANCIAR – ECONOMIC

Serviciul financiar economic (SFE) prelucrează date cu caracter personal, pe suport de hârtie, în format electronic, în programul contabil 1C, în cadrul proceselor de lucru: Asigurarea organizării corecte a evidenței contabile; Coordonarea utilizării corecte a mijloacelor financiare în corespundere cu alocațiile bugetare aprobate; Asigurarea procesului de elaborare și coordonare a proiectului de buget al instanței judecătorești; Întocmirea și prezentarea în termen a rapoartelor financiare lunare, trimestriale și anuale; Asigurarea inventarierii și evidența bunurilor materiale; Realizarea salarizăriii angajaților; Elaborarea proiectului de buget; Întocmirea documentelor cu privire la contracte.
Funcționarii publici de conducere și execuție (șef contabil, specialist principal) din cadrul serviciului SFE prelucrează categoriile de date cu caracter personal: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data nașterii și domiciliul; Codul personal de asigurări sociale (CPAS); Date privind locul de muncă și funcția ocupată; Gen; Minor (Da/Nu); Adresa; Ocupația; Educația; Funcția; Telefon fix/mobil, e-mail serviciu/personal; Salariul brut, premii, sporuri, stimulări, suplimente; Numele, prenumele (după caz patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, după caz); Certificate de concediu medical acordat (datele din certificate); certificate/copii ale actelor cu privire la datele personale; Date pentru transferul pe cont bancar a plăților salariale și a altor sume datorate cu titlul de indemnizație, compensație, sau alte beneficii după caz; Mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuții, asigurări obligatorii de asistență medicală, contribuții de asigurări sociale de stat obligatorii, alte sume în virtutea legii; Informații judiciare cu caracter personal (date cu privire la achitarea taxei de timbru, alte achitări privind eliberarea copiilor materialelor din dosarul în care este vizat, și taxe pentru eliberarea înregistrări audio a ședinței de judecată)

Sarcinile de bază și atribuțiile SFE prin prisma respectării datelor cu caracter personal sunt:
In cadrul sistemului de evidență contabilă sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- numărul personal de identificare de stat (IDNP);
- locul nașterii;
- nr. de telefon;
- genul;
- datele din buletinul de identitate,
- studiile;
- data nașterii și domiciliul;
- codul personal de asigurări sociale (CPAS);
- datele privind locul de muncă și funcția ocupată;
- mărimea salariului brut și alte premii, sporuri, stimulări, suplimente;
- datele privind situația familială (la cererea solicitantului);
- numele, prenumele (după caz. patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- datele pentru transferul pe contul bancar a plăților salariale și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;
- mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale de stat obligatori, prime de asigurare obligatorie de asistență medicală, și alte sume datorate în virtutea legii sau contractului;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.
- Prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații și care au impact asupra calculării plăților salariale, de exemplu: modificarea gradului de calificare a funcționarilor publici, avansarea în treptele de salarizare, evaluarea performanțelor profesionale ale subdiviziunilor cu acordarea sporului pentru performanță, vechimea în muncă în serviciul public;

- Calcularea salariilor lunare, în conformitate cu legislația 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 angajaților în vederea stabilirii indemnizațiilor corespunzătoare;
- Prelucrarea copiilor ordinelor Președintelui referitoare la personal;
- Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, cotizații judecătorești, impozitul pe venit, etc.;
- Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului;
- Prezentarea trimestrială a rapoartelor la Biroul Național de Statistică privind efectivul de personal și remunerarea muncii acestuia. Anual se prezintă rapoarte privind formarea profesională a angajaților și cheltuielile efectuate în acest scop. Anual se prezintă rapoarte ce reflectă cheltuielile executate pentru întreținerea mijloacelor de transport, TFD 19, precum și cele de întreținere a clădirii instituției(cheltuielile pentru energie electrică și a gazelor naturale, consumul de combustibil), raportul Balanța Energetică. - Prezentarea la Biroul Național de Statistică se prezintă rapoartul privind fluxul de angajări și eliberări ale personalului pe parcursul anului bugetar.
- La Inspectoratul Fiscal se prezintă lunar rapoartele IPC-21,IRM19

a) Prezentarea anuală a raportului IALS21, privind salariul și impozitul pe venit, precum și calcularea primelor de asigurare obligatorie de asistență medicală și calcularea contribuțiilor de asigurări sociale de Stat pentru fiecare angajat în parte.
b) Prezentarea lunară
c) informație privind creanțele cu termen expirat și datoriile cu termen de prescripție expirat formate în instanța (Forma FD -049),ceea ce instituția Judecătoria Strășeni, nu are.
d) raportul operativ privind statele și efectivul de personal din instituție (Forma FD-050).

De asemenea serviciul financiar-economic întocmește și prezintă instituției ierarhic superioare, CSM, trimestrial și anual raportul activității serviciului. Acest raport conține informații despre cheltuielile executate și efective ale instituției în această perioadă de gestiune. Rapoartele financiare sunt întocmite conform Normelor metodologice privind evidența contabilă și raportarea financiară în sistemul bugetar, aprobat prin Ordinul Ministrului Finanțelor nr.216 din 28.12.2015, cu modificările operate ulterior. Totodată, se solicită să se asigure întocmirea și prezentarea rapoartelor financiare în termenele și componența stabilite, să se reflecte integral în evidența contabilă a operațiunilor economice efectuate în perioada de raportare, atât prin sistemul trezorerial, cât și în afara acestuia (după caz), să se verifice raportul financiar cu Fișa executării contului curent (forma FD-037).

- Se întocmesc și se prezintă inclusiv și raportul narativ privind executarea bugetului conform ordinului Ministrului de Finanțe nr.164 din 30 decembrie 2016 cu privire la aprobarea Cerințelor la întocmirea Raportului narativ privind executarea bugetelor în instituțiile bugetare. Rapoartele se prezintă în SI „Raportarea financiară a instituțiilor bugetare" și pe suport de hârtie (imprimat din program). Prelucrarea cererilor și a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reținut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal;
- Eliberarea certificatelor de salariu, la cererea angajaților;

Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate 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/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor 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 evidență contabilă în alte scopuri decât cele menționate mai sus este interzisă.

Datele cu caracter personal conținute în serviciu serviciul financiar economic în cadrul Judecătoriei Strășeni se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic;
- Software - Sistemul de evidență contabilă în sfera bugetară 1C Enterprise, care este instalat la computerul central – „Contabil Șef", computerul aflându-se în biroul 12 din sediul Judecătoriei Strășeni;

Mentenanța programului contabil 1C Enterprise: Este asigurată de către compania SRL „BitGenerator" în baza contractului de valoare mică încheiat pe un termen de 12 luni, privind prestarea serviciilor de deservire între Judecătoria Strășeni și SRL „BitGenerator"cu următoarele atribuții stabilite companiei prestatoare: servicii de automatizare a evidenței contabile prin intermediul Sistemului Informațional Bugetar (SIB) asigurarea perfectării și ajustării sistemului în strictă conformitate cu modificările legislației în vigoare; instalarea versiunilor noi a sistemului;

- consultanță software de bază,
- consultanță software extinsă,
- consultație metodologică.
- Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului;
- Menținerea și actualizarea modelelor;
- Asigurarea copiilor de rezervă, verificarea integrității și la solicitare restabilirea din copiile de rezervă;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului (Linia fierbinte);
- Examinarea solicitărilor parvenite din partea Autorității Publice;
- Examinarea și divulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hârtie este structurată după criteriu "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în biroul 12 din sediul Judecătoriei Strășeni, și în arhiva sin subsolul instanței.

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

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Prelucrarea datelor cu caracter personal în mod accidental sau ilegal. Distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal. Accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod decât cel prevăzut.

Activități de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Realizarea sistematică a controlului de către managerii operaționali. Asigurarea participării la instruiri privind prelucrarea datelor cu caracter personal.

SERVICIUL RESURSE UMANE

Serviciul resurse-umane (SRU) prelucrează date cu caracter personal, pe suport de hîrtie, în format electronic, prin intermediul componentelor SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD), în cadrul proceselor de lucru: Ținerea evidenței angajaților instanței judecătorești; Întocmirea proiectelor de acte administrative ordine/dispoziții; Monitorizarea și acordarea asistenței comisiei de concurs; Evidența dezvoltării profesionale a funcționarilor publici; Gestionarea dosarelor personale; Asigurarea evidenței tuturor concediilor, certificatelor medicale ale personalului, evidenței vechimii în muncă și a treptelor de salarizare, perfectarea și ridicarea semnăturilor electronice avansate calificate a tuturor subiecților declarării averii și a intereselor personale din cadrul Judecătoriei Strășeni; Actualizarea permanentă a Registrului electronic al subiecților declarării averii și a intereselor personale; Organizarea și funcționarea resursei informaționale destinate evidenței integrate și sistematizate a informației aferente raporturilor de muncă/serviciu al angajaților " Registrul electronic al angajaților"; Evidenței poștei electronice @justice.md, completarea fișei personale a angajaților MR-2; Eliberarea Certificatelor / Caracteristicilor angajaților instanței or la cerere a persoanelor

anterior angajate; Încheierea CIM or la necesitate a Acordurilor suplimentare CIM cu angajații (pdtafap, ps, pa), Actualizarea schemei de încadrare, etc.

Funcționarii publici de execuție (specialist principal) din cadrul serviciului SRU prelucrează categoriile de date cu caracter personal: Toate datele menționate în actul de identitate a salariatului (nume, prenume, domiciliu, locul nașterii, data nașterii, IDNP-ul, seria si numărul, data eliberării, sexul, cetățenia, adresa de reședință etc.) întrucât, la angajare actul de identitate al salariatului este solicitat în vederea completării actelor necesare încheierii contractului de muncă; Semnătura salariatului întrucât, la momentul angajării, salariatul semnează contractul de muncă și/sau alte acte; Date privind cazierul judiciar al salariatului, dacă este cazul, a certificatului medical – dacă în fișa postului pentru funcția respectivă, sînt stabilite cerințe speciale de sănătate; Date privind starea civilă; Date privind calitatea de pensionar, dacă este cazul; Date privind asigurări de sănătate și sociale; Date privind studiile, formarea profesională, documente ce atestă experiența profesională (copia carnetului de muncă, certificate privind activitatea profesională desfășurată după data de 1 ianuarie 2019 sau alte documente confirmative); Stagii de perfecționare; Sancțiuni disciplinare; Certificat de integritate - autorității Naționale de Integritate (la necesitate); Certificatul de cazier privind integritatea profesională de la Centrul Național Anticorupție (la necesiatate); Informația referitoare la lipsa sau existența factorilor de risc care pot aduce atingere ordinii de drept, securității statului, ordinii publice de la Serviciul de Informații și Securitate (la necesitate), Date ale membrilor de familie; Date din actele de stare civilă; Date despre evidența militară (livretul militar); Toate datele referitoare la drepturile și obligațiile salariatului întrucât, în contractul de muncă se menționează, în mod obligatoriu, aceste mențiuni; Informații privind modul în care salariatul își exercită funcția (ce măsuri adoptă, ce acte semnează, programul de muncă, prezența sau lipsa de la muncă, numărul concediilor, perioada concediilor etc); Informații privind modul în care salariatul folosește tehnica, alt utilaj, pus la dispoziție pentru activitate; Datele de contact ale salariatului (ex: număr de telefon, nr. fax, adresa e-mail, adresa de reședință etc.); Datele privind veniturile obținute de salariat (sumele plătite, cuantumul acestora, data plății, natura acestora etc, întrucât, pe parcursul desfășurării activității, instanța îi plătește salariatului salariul și/sau alte beneficii); Alte date necesare pentru buna desfășurare a activității, în conformitate cu prevederile legale în vigoare.

Datele personale ale salariaților sunt date furnizate de salariat cu ocazia angajării, completate ulterior cu informații generate de derularea raportului de muncă.

Prelucrarea datelor cu caracter personal de serviciu resurse umane se efectuează pe perioada activității angajaților Judecătoriei Strășeni (din momentul emiterii Decretului Președintelui Republicii Moldova, Hotărârii CSM , ordinului cu privire la numirea în funcție 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 serviciului în alte scopuri este interzisă.

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Utilizarea datelor cu caracter personal în alte scopuri decît cele prevăzute în activitatea sa. Prelucrarea în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Activități de control: Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Participarea la instruiri. Pseudonimizarea și criptarea datelor cu caracter personal. Capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă a sistemelor și serviciilor de prelucrare. Capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică

SERVICIUL ARHIVĂ

Serviciul arhivă (SA) prelucrează date cu caracter personal, pe suport de hîrtie, în format electronic, prin intermediul componentei SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD), în cadrul proceselor de lucru: Evidența dosarelor transmise în arhivă; Furnizarea informațiilor din

dosare şi copiilor de pe materialele dosarelor la solicitarea participanţilor la proces; Elaborarea nomenclatorului dosarelor; Asigurarea selectării, prelucrării şi transmiterii dosarelor, documentelor în Arhiva Naţională.

Personalul din cadrul serviciului SA prelucrează categoriile de date cu caracter personal: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data naşterii şi domiciliul; Adresa; Calitatea procesuală; Telefon fix/mobil, e-mail serviciu/personal; Informaţii judiciare cu caracter personal la eliberarea copiilor materialelor din dosare (date cu privire la participanţii pe dosare în care sunt şi/sau au fost implicaţi).

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

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Prelucrarea datelor cu caracter personal cu încălcarea securităţii datelor cu caracter personal care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

Activităţi de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Aplicarea măsurilor organizatorice de protecţie a informaţiilor ce conţin date cu caracter personal. Realizarea sistematică a controlului de către managerii operaţionali. Asigurarea participării la instruiri privind prelucrarea datelor cu caracter personal.

SERVICIUL EXPEDIŢIE

Serviciul expediţie (SE) prelucrează date cu caracter personal, pe suport de hîrtie, în format electronic, prin intermediul componentelor SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD), în cadrul proceselor de lucru: Realizarea înregistrării corespondenţei de ieşire în registru; Asigurarea securităţii în procesul de expediere a corespondenţei înregistrate şi a altor bunuri sau valori la destinaţie; Asigurarea integrităţii informaţiei şi documentelor primite spre expediere; Furnizarea informaţiei necesare la cererea cetăţenilor în limita competenţei.

Personalul din cadrul serviciului SE prelucrează categoriile de date cu caracter personal: Nume, prenume, patronimic; Numărul personal de identificare de stat (IDNP); Data naşterii şi domiciliul; Adresa; Telefon fix/mobil, e-mail serviciu/personal.

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Utilizarea datelor cu caracter personal în alte scopuri decît cele prevăzute în activitatea subdiviziunii. Expedierea informaţiei ce conţine date cu caracter personal altui destinatar.

Activităţi de control: Respectarea prevederilor legale privind protecţia datelor cu caracter personal; Realizarea sistematică a controlului de către managerii operaţionali. Aplicarea măsurilor organizatorice de protecţie a informaţiilor ce conţin date cu caracter personal. Participarea la instruiri.

SERVICIUL TEHNOLOGII INFORMAŢIONALE (STI)

Serviciul tehnologii informaţionale (STI) prelucrează date cu caracter personal, în format electronic, prin intermediul componentelor SIJ - Programul Integrat de Gestionare a Dosarelor (PIGD); Soluţia Informatică a şedinţelor de judecată (SI a S) videoconferinţa, înregistrarea audio /video a şedinţelor de judecată, în cadrul proceselor de lucru: Asigurarea deservirii tehnicii de calcul din cadrul instanţei; Asigurarea funcţionării paginii web şi a sistemului de poştă electronică a instanţei; Asigurarea conlucrării eficiente cu alte instituţii în vederea funcţionării eficiente a PIGD; Asigurare funcţionării tehnicii de înregistrare audio a şedinţelor de judecată şi arhivarea informaţiei înregistrate; Înaintarea propunerilor pentru modificarea, ajustarea şi îmbunătăţirea programelor instalate şi paginii web a instanţei; Acordarea suportului informaţional şi metodologic angajaţilor instanţei judecătoreşti în domeniul utilizării calculatorului şi echipamentelor electronice; Asigurarea funcţionării sistemului video conferinţă al instanţei judecătoreşti.

Administratorul superior reţea de calculatoare (pdtafap-post de deservire tehnică ce asigură funcţionarea autorităţii publice) din cadrul serviciului STI prelucrează categoriile de date cu caracter personal: Nume, prenume; Date privind locul de muncă şi funcţia ocupată; Adresa; Adresa înregistrată în SIJ; Telefon fix/mobil, e-mail serviciu/personal.

Riscuri posibile în procesul prelucrării datelor cu caracter personal: Prelucrarea datelor cu caracter personal în mod accidental sau ilegal. Distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal. Accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod decît cel prevăzut.

Activități de control: Verificarea corectitudinii aplicării cadrului legal în vigoare. Aplicarea măsurilor organizatorice de protecție a informațiilor ce conțin date cu caracter personal. Realizarea sistematică a controlului de către managerii operaționali. Asigurarea participării la instruiri privind prelucrarea datelor cu caracter personal.

XIII. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

Judecătoria Strășeni, 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 justiție.

Personalul implicat în activitatea de administrare și/sau prelucrare a informațiilor din cadrul Judecătoriei Strășeni, 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 (managerul) autorității publice Judecătoria Strășeni. 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.

XIV. 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 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.

Asigurarea protecţiei contra programelor dăunătoare (virușilor)

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

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).

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 autorităţii publice Judecătoria Străşeni informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

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

Obligaţiile funcţionarilor prin prisma respectării confidenţialităţii datelor cu caracter personal:

În ceea ce priveşte asigurarea securităţii datelor cu caracter personal, funcţionarii au următoarele obligaţii:

- de a consulta documentele sau dosarele aflate în instanţă, având obligaţia de a respecta secretul de serviciu şi de a proteja informaţiile confidenţiale la care au avut acces în măsura ce ţine nemijlocit de activitatea secţiei;
- de a asigura securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copier;
- de a asigura 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;
- de a respecta normele deontologice profesionale şi legislaţia în vigoare.

XV. MOTIVAREA COLECTĂRII ŞI PRELUCRĂRII

Scopul major pentru care Judecătoria Străşeni colectează/prelucrează date cu caracter personal ţine de prelucrarea datelor/informaţiilor pe baza cărora să se poată îndeplini obligaţiile legale şi să poată lua decizii coerente şi corecte în managementul sistemului judiciar.

Furnizarea de date personale, este necesară în vederea derulării/iniţierii de raporturi juridice, cu respectarea prevederilor legale (de exemplu: cele privind relaţia cu angajaţii sau cele privind justiţiabilii pentru examinarea dosarelor, sau cele privind operatorii economici privind asigurarea cu materiale/servicii). În cazul refuzului de a furniza aceste date, instanţa de judecată poate să refuze iniţierea de raporturi juridice, întrucât poate fi pusă în imposibilitatea de a respecta cerinţele reglementărilor legale, ca exemplu în cazul angajaţilor, a prevederilor dreptului muncii şi dreptului fiscal.

De asemenea, instanţa mai colectează şi o serie de informaţii care nu au un caracter obligatoriu (de exemplu: adresa de email, telefon) în vederea îmbunătăţirii modului de comunicare.

Refuzul furnizării şi/sau prelucrării datelor informaţiilor opţionale poate duce la imposibilitatea ca instanţa de judecată să transmită informaţii. (De exemplu: informaţiile cu caracter personal care se colectează şi se prelucrează pentru a respecta prevederile legale relativ la înregistrarea operaţiunilor financiar contabile). Furnizarea informaţiilor din această categorie este obligatorie, refuzul de a le

furniza duce la imposibilitatea de a demara relații juridice între instanța de judecată și respectivele persoane.

XVI. LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Prelucrarea este legală dacă întrunește cel puțin una din următoarele condiții:

Persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specific.

Prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte, sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract.

Prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine instanței de judecată.

Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice.

Prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investită.

XVI. CONDIȚII PRIVIND CONSIMȚĂMÎNTUL

Consimțământul subiectului datelor cu caracter personal nu este cerut în cazurile în care prelucrarea este necesară pentru:

- Executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia;
- Îndeplinirea unei obligații care îi revine operatorului conform legii;
- Protejarea vieții, integrității fizice sau a sănătății subiectului datelor cu caracter personal;
- Executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terțul căruia îi sânt dezvăluite datele cu caracter personal;
- Realizarea unui interes legitim al operatorului sau al terțului căruia îi sânt dezvăluite datele cu caracter personal, cu condiția ca acest interes să nu prejudicieze interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;
- Efectuarea auditului public extern;
- Scopuri statistice, de cercetare istorică sau științifică, cu condiția ca datele cu caracter personal să rămână anonime pe toată durata prelucrării;
- Schimbul de date în condițiile legislației în vigoare.

XVII. DREPTURILE PERSOANELOR ALE CĂROR DATE PERSONALE SUNT COLECTATE ȘI/SAU PRELUCRATE

Drepturile persoanelor vizate în contextul prelucrării datelor cu caracter personal se regăsesc în dispozițiile art.13-22 din Regulamentul (UE) 2016/679 al Parlamentului European și Consiliului Europei din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. Aceste drepturi sunt:

Dreptul de a fi informat – subiecții de date trebuie să poată obține informații despre prelucrarea datelor.

Dreptul de acces al persoanei vizate – subiecții de date trebuie să poată accesa copii ale oricăror date care au fost colectate sau obținute de operatorl de date și sau persoana împuternicită de operator.

Dreptul la rectificare – dacă datele cu caracter personal sunt inexacte, operatorul de date trebuie să le corecteze.

Dreptul de opoziție – după colectarea datelor, subiecții de date pot prezenta obiecții privind modul în care sunt gestionate datele lor și pot opri acțiunile ulterioare.

Dreptul la restricționarea prelucrării – subiecții de date pot solicita ca datele lor să nu fie prelucrate într-un anumit mod sau să oprească prelucrarea lor ulterioară.

Dreptul la ștergere – subiecții de date pot solicita ca datele lor să fie șterse cît mai curînd posibil de către operatorul de date sau de persoana împuternicită de operator.

Dreptul la portabilitatea datelor – subiecții de date au dreptul de a-și accesa datele lor într-un format digital compatibil cu o varietate de dispozitive.

Dreptul la contestare – dacă subiectul de date este nemulțumit de modul în care sunt prelucrate datele sale sau consideră că drepturile sale nu sunt respectate, are dreptul de a depune o plîngere la CNPDCP *cu sediul în mun.Chișinău str. Serghei Lazo nr.48, ((022) 820 801 centru@datepersonale.md).*

XVIII. CONTROL ȘI ÎMBUNĂTĂȚIRE

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

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

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

XIX. DISPOZIȚII FINALE

Prezentul Regulament poate fi revizuit periodic, în funcție de modificările și completările legislative aplicabile, precum și de nivelul de dezvoltare tehnologică. Regulamentul este adus la cunoștința angajaților contra semnătură.

Prezentul Regulament intră în vigoare din momentul aprobării de către Președintele Judecătoriei Strășeni.

Odată cu intrare în vigoare a prezentului regulament, se abrogă cadrul intern cu referire la date cu caracter personal aprobat în anul 2018, după cum urmează: Politica de securitate privind Protecția Datelor cu Caracter Personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Judecătoria Strășeni aprobat la data de 28 mai 2018, Regulamentul privind Prelucrarea Informațiilor ce conțin date cu caracter personal în sistemul resurse umane la Judecătoria Strășeni aprobat la data de 16 octombrie 2018 și Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă aprobat la data de 28 mai 2018.

Întocmit:

Șefa secretariatului
Judecătoriei Strășeni Valentina Prescura